EDPS

European Data Protection Supervisor

Two decades of personal data protection. What next?

EDPS 20th Anniversary

Two decades of personal data protection. What next?

EDPS 20th Anniversary

European Data Protection Supervisor,
Rue Montoyer 30, 1000 Brussels,
Belgium

www.edps.europa.eu • https://20years.edps.europa.eu/en • edps@edps.europa.eu

Follow EDPS on X, LinkedIn, Youtube and Instagram.

Manuscript completed in February 2024.

The European Data Protection Supervisor wishes to express its sincere gratitude to all authors for their contributions.

The European Data Protection Supervisor would also like to thank the EDPS 20th Anniversary Book team of editors: Brendan Van Alsenoy, Julia Hodder, Fenneke Buskermolen, Miriam Čakurdová, Ilektra Makraki and Estelle Burgot, for orchestrating this project.

Luxembourg: Publications Office of the European Union, 2024

Print	ISBN 978-92-9242-823-5	doi:10.2804/209010	QT-05-23-438-EN-C
PDF	ISBN 978-92-9242-824-2	doi:10.2804/652641	QT-05-23-438-EN-N

Two decades of personal data protection. What next?

EDPS 20th Anniversary

2004
2024
EDPS

Table of Contents

01

Introduction

Wojciech Wiewiórowski

Introduction

Wojciech Wiewiórowski (*)

What better way to celebrate a birthday than to invite old and new friends to share a space together?

This year we mark the 20th anniversary of the EDPS as an EU institution. A reason to celebrate, but also a reason to reflect.

There is a specific philosophy behind the different initiatives that celebrate the EDPS' 20th anniversary: we reflect on the richness of the past 20 years in order to prepare for, and embrace, the years ahead of us. This mind-set is also reflected in this commemorative book – a book that sees the development of the EDPS and the development of EU data protection law as closely intertwined.

The legal acts that established the EDPS and the rules it is bound to enforce are themselves part of EU data protection law. In the next chapter, the EDPS' first Supervisor, Peter Hustinx, will describe how the EDPS emerged as a European institution and set up its first activities. His contribution shows how early design choices on how to organise the EDPS' main spheres of activity have left an indelible imprint on how the EDPS functions today.

While the history of the EDPS is first and foremost the history of an institution, it is also the history of the people who have brought the institution to life. The EDPS' Secretary General, Leonardo Cervera Navas, will offer you his personal recollections of the leadership provided by the EDPS' first three Supervisors.

With the entry into force of the Treaty of Lisbon, data protection became an integral part of the EU's constitutional legal order. The implications of this change can hardly be overstated. Hielke Hijmans will share with you the different ways in which Article 16 TFEU has impacted the development of EU data protection law. You will also find many examples of this impact in the remaining chapters of the book.

(*) European Data Protection Supervisor (2019-2024)

The fundamental right to data protection and the fundamental right to respect for private and family life are closely related, but they are not the same. Rosa Barcelo will guide you through the evolution of the legal framework dedicated to protecting privacy in electronic communications, which regulates some of the key privacy issues in the digital age, from confidentiality of electronic communications to online tracking.

The flip side of privacy in electronic communications is data retention. Controversial from the outset, data retention has given rise to a series of landmark rulings of the Court of Justice of the EU ('CJEU'). It has been an honour for the EDPS to have been invited by the CJEU to intervene and share its expertise in these cases. Herke Kranenborg will enlighten you on how the CJEU's case law on this topic has developed over time, as well as offer you a look into the future.

Another series of landmark rulings of the CJEU concerns the regulation of international transfers of personal data. As it is an important vehicle through which EU data protection law influences data processing outside the EU, it is an area to which the EDPS pays close attention. Christopher Kuner will highlight how the EDPS has contributed to the development, application, and interpretation of data transfer regulation.

The EU's General Data Protection Regulation ('GDPR') was finally adopted on the 27th of April, 2016. But the road to adoption was not without difficulty. In an interview, Jan Philipp Albrecht looks back at the goals, challenges and achievements of the GDPR. He also reflects on the relevance of the GDPR in today's digital regulatory landscape, as well as the main challenges for the future.

With the GDPR adopted, it was time to update the data protection rules applicable to EU Union institutions and bodies. Thomas Zerdick will describe how the EUDPR aligns with the GDPR, while also illuminating some of the EUDPR's specificities. After providing examples of how the EDPS has exercised its supervisory powers under the EUDPR, Thomas will reflect on the future of the EUDPR.

During the last 20 years, EU policy in the Area of Freedom, Security and Justice ('AFSJ') has gradually taken shape, and so have the corresponding data protection rules. It is a big chapter in this book because it is such a big part of the EDPS' core activities. Thanks to Fanny Coudert, Teresa Quintel and Juraj Sajfert, you will be able to navigate the highly complex legal landscape that underpins a great deal of the EDPS' supervisory activities. In addition, Diana Alonso Blas will provide you with a practical perspective of how data protection has been implemented in the context of the recently established Eurojust evidence database relating to genocide, crimes against humanity, war crimes and related criminal offences.

When we think about cooperation at the EDPS, we think first of the cooperation with our fellow data protection authorities within the European Economic Area. While the EDPB and the EDPS are two separate institutions, we are closely connected in more ways than one. In 'The making of the European Data Protection Board', Andrea Jelinek and Isabelle Vereecken share a first-hand account of all the hard work that was needed to set up the EDPB, while also offering insight into the vision of two of the EDPB's most fearless leaders.

The EDPS' cooperation activities stretch far beyond our Union's borders. Olivier Matter sets out why international cooperation is imperative by reflecting on the role and milestone achievements of different international fora active in the field of data protection. Just like Olivier, I have no doubt that the EDPS will continue to play its part and try to assume a decisive role for at least another 20 years.

Practical experience in the enforcement of data protection law has led to the realisation that technology not only enables the processing of personal data; it can also contribute to providing safeguards. Massimo Attoresi, Achim Klabunde and Xabier Lareo highlight how the EDPS' strategies and actions have accompanied the evolution of the relationship between technology and data protection since the foundation of the EDPS.

In its Preliminary Opinion of 2014, the EDPS launched a debate in the EU about how enforcement, in particular through interaction of competition and data protection authorities, could adapt to address the challenges of our increasingly digital economy. Christian D'Cunha and Anna Colaps explain how what was once a controversial idea has since become mainstream in discussions concerning the regulation of the digital economy.

The growing need for a Digital Clearinghouse '2.0' is made even more evident by Gabriela Zanfir-Fortuna's contribution on the EU's new digital rulebook. Her chapter shows that regardless of the number, complexity and depth of various legal acts regulating the digital space, data protection law and the authorities entrusted with its enforcement will remain at the core of the protection of fundamental rights.

The relationship between EU data protection law and the recently adopted Artificial Intelligence Act is further explored by Nathalie Smuha. She details how EU data protection law not only 'grounds' and complements the AI Act, it also enables an evaluation and a critique thereof. This Chapter confirms to me once again that effective enforcement of EU data protection will remain of paramount importance in the years to come.

Speaking of effective enforcement: I have been reflecting extensively on how to ensure that the GDPR delivers on its promise of providing strong and coherent protection of the individuals' fundamental right to data protection. Lisette Mustert explains why brave thinking regarding the design of the enforcement system itself is needed and why closer integration is a necessity if we are serious about protecting EU citizens' personal data across the EU.

Last but definitely not least, the EDPS' Honorary Director General, Christopher Docksey, will provide you with insights on some of the most significant trends in the case law of the CJEU following the entry into force of the EU Charter.

Having reflected on major milestones of the past 20 years and what is yet to come, this book offers readers a photographic timeline.

The timeline both visualises the EDPS' own history as the EU's independent data protection authority alongside key moments in the development of EU data protection law.

I warmly encourage you to also read the rich collection of memories of long-standing connections and friends of the EDPS, who have been kind enough to share some personal reflections on their experiences with the EDPS.

The content of this book has made me proud.

Not just because of the high quality of each contribution, for which I am deeply grateful.

I am proud because it reveals what a privilege it is to be a part of the EDPS. Together, we have helped to shape the history of EU data protection.

I can only hope that the EDPS will continue to have the same positive impact in the future.

02

The EDPS' first ten years

Peter J. Hustinx

The EDPS' first ten years

Peter J. Hustinx (*)

This contribution aims to describe how the EDPS emerged as an independent authority at EU level. Developing from a very modest start, the authority was able to exercise considerable influence by concentrating on three main roles – supervision, consultation, and cooperation –and by emphasising that effective data protection should be seen as a condition for success. In this way, the first ten years have provided the basis for how the EDPS is operating today.

1. Introduction

The European Union was rather late in adopting data protection rules for its institutions and bodies and establishing an independent supervisory authority to ensure compliance with such rules. Directive 95/46/EC ([1]) was conceived in the logic of the internal market and addressed to the Member States. However, initial plans ([2]) to do more faced a major obstacle: the lack of a legal basis to provide for binding rules and independent oversight at the level of the Union. In October 1997, as part of the Treaty of Amsterdam ([3]), this resulted in the introduction of a new Article 286 in the EC Treaty, which read as follows:

1. From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.

(*) Mr. Hustinx served as the first EDPS from January 2004 until December 2014. Before that he was President of the Dutch Data Protection Authority (1991-2004) and Chairman of the Article 29 Working Party (1996-2000). Photo credit: International Association of Privacy Professionals (IAPP).

([1]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

([2]) The initial Commission proposal (COM (1990) 314 final SYN 287 and 288) contained a Commission Declaration which inter alia considered that '*the principles contained in [the proposed Directive] … must apply to the institutions and other bodies of the European Communities*'.

([3]) Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, OJ C 340, 10.11.1997, p. 1.

2. Before the date referred to in paragraph 1, the Council, acting in accordance with the procedure referred to in Article 251, shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate.

Although the first paragraph of this provision suggested a direct application of all relevant Community acts, the practical effect of its two paragraphs was that a target date had been set for the Community legislature to lay down all the rules required to comply with the substance of those Community acts. It is interesting to see in retrospect how the establishment of an independent supervisory body, a new element in the institutional landscape, was given special emphasis in this context.

Not by the target date, but almost two years later, on 18 December 2000, the European Parliament and the Council adopted Regulation (EC) 45/2001 ([4]), which can indeed be seen as the implementation at EU level of Directive 95/46/EC and other relevant Community acts existing at the time ([5]). Its main lines were not surprising and stayed quite close to the substance of the relevant directives. However, two important details are worth mentioning at this stage. First, the obligation for each Community institution or body to appoint at least one person as data protection officer ('DPO'), which turned out to be extremely helpful ([6]). Second, the language used to emphasise the principle that the supervisory body should be completely independent and should *'neither seek nor take instructions from anybody'*, on which the Court of Justice partly relied in its first important case on the subject ([7]).

Although the new Regulation entered into force in February 2001, its legal and practical impact once again made a slow start. It took an additional year and a half for a joint decision ([8]) of Parliament, Council and Commission to determine the remuneration of the Supervisor and Assistant Supervisor, some further details of the procedure for their appointment, and their seat in Brussels. Finally,

([4]) Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1.

([5]) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30.1.1998, p. 1, later replaced by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

([6]) See Article 24 of Regulation (EC) 45/2001 and section 3 of this contribution.

([7]) See Article 44 of Regulation (EC) 45/2001 and judgment of the Court of Justice of 9 March 2010, *Commission/Germany*, C-518/07, ECLI:EU:C:2010:125, paragraphs 26 to 29. The EDPS intervened in this case in support of the Commission and was thus able to contribute on important details.

([8]) Decision 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data -Protection Supervisor's duties, OJ L 183, 12.7.2002, p. 1.

another year and a half were required to arrive at a joint decision ([9]) of Parliament and Council to appoint them with immediate effect from the date of publication of that decision: 17 January 2004. As a result, some three years had passed under the Regulation without independent supervision.

2. Building a 'new institution'

The two members ([10]) of the new supervisory body met in Barcelona to start planning for their journey and expressed their intention to start working in the premises of the European Parliament, at least for an initial period to limit resources, as from Monday 2 February 2004. During the first week, they made all necessary arrangements from a protocol room in the Parliament. On the third day, it turned out that the Parliament could provide an empty floor in a nearby office building ([11]) for rent, together with basic office equipment and furniture, and two seconded staff members. This offer was gladly accepted, but the next week it also turned out that the initial draft budget for the new body had never been approved, and due to the time passed was no longer sufficient for the rest of the year.

This meant that the two members and their temporary staff had to concentrate, first of all, at the preparation and adoption of a draft budget for 2004, a draft amending budget for 2004 and an estimate for 2005, including all related interactions with the budgetary levels of the European Commission, the European Parliament and the Council, many of which were initially unfamiliar with the existence and the needs of a newly established supervisory body. In May 2004, a head of unit was seconded by the Commission to set up the Secretariat. Amongst the priorities was the publication of vacancy notices and recruitment of staff as authorised in the organisation chart for the financial year. In June 2004, the EDPS signed an administrative cooperation with the European Commission, the European Parliament, and the Council for an initial period of three years, under which each would provide some well-defined services to ensure both economy and efficiency. By the end of 2004, all staff allowed in the establishment plan had been recruited, and national experts from national or regional data protection authorities had been invited to join the EDPS in 2005 ([12]).

([9]) Decision 2004/55/EC of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty (European Data Protection Supervisor), OJ L 12, 17.1.2004, p. 47.

([10]) The author as Supervisor and Joaquín Bayo Delgado as Assistant Supervisor. See about the EDPS' first five years also: Bayo Delgado, J., 'Setting up a New European Authority' in: Hijmans, H., Kranenborg, H. (eds.), *Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*, Intersentia, Cambridge, 2014, p. 45-47.

([11]) Rue Montoyer 63 in Brussels. In October 2012 the EDPS moved to its present home at Rue Montoyer 30.

([12]) See EDPS Annual Report 2004, issued on 18 March 2005, chapter 2, p. 18-23 for more information. The title of that chapter is used again in this section to indicate that the EDPS, as an independent authority, has many features of an EU institution. See for an early and more detailed analysis: Hijmans, H., 'The European Data Protection Supervisor: The Institutions of the EC controlled by an Independent Authority', *Common Market Law Review,* Vol.43, Kluwer, 2006, p. 1313-1342.

Although a limited number of cases was dealt with during this first building phase, the remaining time available was also used to decide on the main features of the new body: its roles in the Regulation, its mission and values, and the practical consequences of each. At an early stage, we decided to distinguish three main roles – briefly summarised as supervision, consultation, and cooperation – which were used to organise our work. Our first annual report contained a mission statement on that basis, which was kept with only limited variations for many years ([13]). Information on the website and in brochures followed the same approach. This contribution will do the same in the following sections.

Our first annual report contained a series of realistic objectives for the following year, which we also used to measure our own performance ([14]). This practice turned out useful, not only for internal purposes, but also externally, not least in discussions with budget authorities where we could point at a consistent track record. In the same context and more widely, we also emphasised that many EU policies depend on the lawful processing of personal data, and that effective protection of personal data should thus be seen not as a burden, but rather as a condition for success ([15]). Finally, we have often opted for pro-active approaches and pragmatic solutions to ensure that the values of data protection are delivered in practice. The following sections of this contribution will give examples of this approach.

Delivering data protection was not the only new challenge for EU institutions and bodies ('EUIs'). At the same time, they had been confronted with a Regulation on public access to documents ([16]). During our first series of courtesy visits to leading officials in various EUIs, it had become clear that both topics were seen as a challenge, but the combination of the two as an obvious contradiction, or even an impossibility. In addition, as the previous European Ombudsman had been a champion of public access and had actively lobbied against the Data Protection Regulation, the assumption had widely been that the EDPS was either an ally or an enemy, depending on your favourite perspective. The realisation that both topics could be part of 'good administration' had not fully landed yet.

([13]) See EDPS Annual Report 2004, issued on 18 March 2005, p. 9 and 14-15.

([14]) *Ibid*, p. 16-17.

([15]) *Ibid*, p. 16.

([16]) Regulation (EC) 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, p. 43.

During the first year, we therefore invested in a background paper ([17]) explaining how public access to documents and data protection could both be delivered in practice. Moreover, we reached out to the new ombudsman ([18]) in Strasbourg, who accepted to exchange experience and with whom we developed a very productive relationship ([19]).

Our approach to public access and data protection, set out in the background paper, was followed by the Court of First Instance (now the General Court), but on appeal rejected by the Court of Justice, in the *Bavarian Lager* case ([20]). This required an additional EDPS paper ([21]) to explain which part of the initial analysis was no longer valid. The remaining parts continued to serve their purpose and urged all EUIs to develop a proactive approach on the matter, while also advising them on how to react in the absence of such an approach.

The outcome of our efforts during the first building phase was that the EDPS had become more visible at EU level and was ready to perform its different roles.

3. Supervision

As already mentioned, Regulation (EC) 45/2001 contained an obligation for each EUI to appoint at least one person as DPO, with the general task to ensure in an independent manner the internal application of its provisions. By the time the EDPS arrived, the main institutions and a few bodies had already done so. The DPOs had in some cases been active for several years and set up a common network to exchange experiences. This was a welcome point of departure, which we have been able to build on in the following years.

In November 2005, we published and circulated a position paper on the role of DPOs in ensuring effective compliance with the Regulation ([22]). This paper first described the layered approach to guaranteeing data protection in the EUIs, involving – in that order – the EUIs themselves, the controllers, the DPOs and the EDPS. It pointed out that it was the prime task of EUIs to protect personal data, and that the individuals appointed as controllers were acting on behalf of their EUI who bore the responsibility for the respect of the Regulation ([23]).

([17]) EDPS, Public access to documents and data protection, Background Paper, issued in July 2005, with a five-page checklist, and a separate summary, presented in the Parliament's LIBE Committee.

([18]) P. Nikiforos Diamandouros, a former Greek national ombudsman, and political scientist who expressed an interest in the 'Amsterdam school' of political science.

([19]) See Memorandum of Understanding between the European Ombudsman and the European Data Protection Supervisor, OJ C 27, 7.2.2007, p. 21. See also Diamandouros, P.N., 'The Ombudsman and the EDPS: Promoting Transparency, the Protection of Personal Data, and Good Administration' in: Hijmans, H., Kranenborg, H. (eds.), op. cit. (footnote 10), p. 269-278.

([20]) Judgment of the Court of Justice of 29 June 2010, *Commission/Bavarian Lager*, C-28/08 P, ECLI:EU:C:2010:378.

([21]) EDPS, Public access to documents containing personal data after the *Bavarian Lager* ruling, issued on 24 March 2011.

([22]) EDPS Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, issued on 28 November 2005.

([23]) The principle of accountability was thus emphasized at an early stage.

The position paper also explained the role and functions of a DPO within an EUI, the safeguards and conditions ensuring their independence, the requirements for their expertise, and their likely interactions with the EDPS. This served as a useful basis to gradually extend the DPO-network and involve an increasing number of agencies in its activities. In October 2010, the network was mature enough to adopt its own professional standards ([24]). In December 2012, we published the results of a detailed survey involving all EUIs ([25]).

One of the important tasks of a DPO was the notification to the EDPS of processing operations likely to present specific risks to data subjects by virtue of their nature, their scope, or their purposes, such as processing operations relating to health or intended to evaluate personal aspects relating to the data subject. Such notifications with all relevant documents were subject to prior checking by the EDPS and led to an opinion with recommendations within a certain deadline ([26]). As most of those processing operations already existed when the EDPS arrived, this provision gave rise to an extensive practice of prior checking *ex post* ([27]). The recommendations were systematically monitored by the EDPS. The substance of the opinions was also used to develop guidelines for controllers and DPOs on various subjects of interest. Although largely *praeter legem*, this practice turned out to be extremely effective.

Although the list of duties ([28]) of the EDPS started with hearing and investigating complaints, this part of the supervisory role remained relatively limited. This could be seen as a success, given our pro-active approach aiming at ensuring compliance rather than encouraging large numbers of complaints. However, we also developed a detailed internal case manual and guidelines on the EDPS website explaining how to submit an admissible complaint.

In December 2010, we published a policy paper ([29]) setting out how the EDPS monitors, measures and ensures compliance with the Regulation, and explaining the nature of the various enforcement powers, as well as when and how the EDPS would use them. That certainly included the use of systematic visits or inspections, although many of the visits ended in practice with an agreement to comply more fully on certain points within a set deadline.

([24]) Network of Data Protection Officers of the EU institutions and bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, adopted on 14 October 2010. At that stage, some DPOs of other EU bodies, such as Europol and Eurojust, participated as observers in the network.

([25]) EDPS, Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/2001 – Report on the Status of Data Protection Officers, issued on 17 December 2012. In January 2013 this was supplemented by a Survey on the function of Data Protection Coordinators at the European Commission, acting as a valuable internal network for the Commission DPO.

([26]) See Article 27 of Regulation (EC) 45/2001.

([27]) Annual reports suggest that about 900 of such opinions were delivered during the first ten years.

([28]) See Article 46 of Regulation (EC) 45/2001.

([29]) EDPS, Monitoring and Ensuring Compliance with Regulation (EC) 45/2001, Policy paper, issued on 13 December 2010. See also Louveaux, S., 'Ten years of Supervision of the EU Institutions and Bodies', and Laudati, L., 'Ten years of Supervision of the EU Institutions and Bodies: Perspective of a DPO', in: Hijmans, H., Kranenborg, H. (eds.), op. cit. (footnote 10), p. 253-259 and 261-267.

4. Consultation

The second main role was less obvious but also turned out to be quite prominent and impactful as it developed. The Regulation provided in clear terms that the EDPS was also responsible for advising EUIs – either on our own initiative or in response to a consultation – on all matters concerning the processing of personal data ([30]). Moreover, it imposed a duty on the European Commission to consult the EDPS whenever it adopted a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. Our position was that these provisions applied to all legislation with an impact on data protection ([31]). As that legislation could eventually also apply at the national level, this advisory role was both timely and strategic.

In March 2005, alongside with the EDPS Annual Report 2004, we published a policy paper ([32]) setting out this position and extending it in at least two directions. First, we clearly recognised the European Commission's privilege to adopt any legislative proposal with the duty to consult the EDPS, but we indicated our availability to give our informal advice on any draft document at the preparatory stage. Second, we suggested that it would be reasonable to expect that the same would apply to relevant legislation outside the scope of Community law, notably involving matters in the former third pillar of the EU, given their possible impact on data protection. To our satisfaction, these points were accepted and acted on by the European Commission at a gradually increasing scale ([33]).

As part of this policy, informal comments were never published, but formal Opinions and any subsequent comments were published and followed up in European Parliament and Council as the relevant files would require. Quite a few of our recommendations were taken on board by the legislature. From 2007 onwards, we complemented our approach with annual inventories of new proposals expected further to European Commission programmes, with colours showing the priority status of each topic for the EDPS ([34]). In this way, we were in a way 'supervising' and to some extent also influencing legislative activities pro-actively. In June 2014, we took stock of developments in a second

([30]) See Article 41(2) second subparagraph and Article 46(d) of Regulation (EC) 45/2001.

([31]) This approach was confirmed by the Court of Justice when allowing the EDPS to intervene in the PNR case (see further below).

([32]) EDPS, The EDPS as an advisor to the Community Institutions on proposals for legislation and related documents, Policy paper, issued on 18 March 2005.

([33]) Internal instructions were issued by the Commission's Secretary General. Council presidencies followed the same approach in practice, after close interactions with the German presidency in the first semester of 2007. Annual reports suggest that eventually about 170 formal opinions were delivered during the first ten years. One of the most important was the EDPS Opinion on the data reform package, issued on 7 March 2012, contributing to the adoption of the GDPR.

([34]) Red > the EDPS will issue an Opinion (high priority), Yellow > the EDPS may issue an Opinion or react in another formal way.

policy paper ([35]). This second paper also mentioned some related interventions, such as the background papers on public access to documents ([36]), and a more recent contribution on data protection and competition ([37]).

As a sidestep in April 2008, we also offered our availability to advise on relevant EU research and technological development ('RTD') projects, with a link to data protection ([38]). On that basis, we issued several opinions or otherwise contributed to RTD projects. The overall objective of these contributions was to promote and reinforce the application of the principle of *privacy by design*, and to facilitate the implementation of the EU's data protection regulatory framework.

In this context, but as quite a separate matter, our activities before the Court of Justice should also be mentioned. This could in principle involve the EDPS as an acting or defending party in a case, but the Regulation also provided for the power to intervene in actions of others brought before the Court of Justice ([39]). There was some doubt whether this provision was legally sound, as both the Statute of the Court ([40]) and the case law so far had restricted this possibility to EU Member States and institutions such as the European Commission, the European Parliament and the Council, and parties establishing an interest in the matter.

However, when the European Parliament decided, in the first year of our mandate, to appeal against decisions of the Council and the European Commission on the sharing of passenger data on transatlantic flights (PNR-data) with US authorities, we decided to intervene in support of the Parliament on substantive grounds. In these cases, the Court allowed the intervention on the ground that the Regulation was giving effect to Article 286 EC Treaty and could thus deviate from the Court's Statute ([41]). Although our input in these cases did not affect the Court's judgment ([42]), the fact that the intervention had been allowed enhanced the general impact of our advisory role on new legislation. Many other interventions before the various courts have followed since that moment, sometimes with a more visible impact on the outcome of a case ([43]).

([35]) EDPS, The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience, Policy paper, issued on 4 June 2014. By then the policy also covered specific procedures, such as delegated and implementing acts, international agreements, and initiatives of Member States and enhanced cooperation.

([36]) *Ibid*, p.16, see also section 2 and footnote 17.

([37]) EDPS, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Preliminary Opinion, issued on 26 March 2014.

([38]) EDPS, The EDPS and EU Research and Technological Development, Policy paper, issued on 28 April 2008. See also Article 41(2) first subparagraph and Article 46(e) of Regulation (EC) 45/2001.

([39]) See Article 47(1)(i) of Regulation (EC) 45/2001.

([40]) See Article 40 of the Statute of the Court of Justice of the European Union.

([41]) Orders of the Court of Justice of 17 March 2005, *Parliament/Council, Parliament/Commission,* Joined Cases C-317 & 318/04, ECLI:EU:C:2005:189 and ECLI:EU:C:2005:190. See also Hijmans, H., op. cit. (footnote 12), p. 1321-1322.

([42]) Judgment of the Court of Justice of 30 May 2006, *Parliament/Council,* Joined Cases C-317 & 318/04, ECLI:EU:C:2006:346, annulling both decisions for having used an incorrect legal basis.

([43]) E.g. in *Commission/Germany,* see footnote 7.

5. Cooperation

The third main role was even less obvious but turned out to be quite prominent and strategic as well. The Regulation provided that the EDPS had to cooperate with national supervisory authorities of the EU Member States and to participate in the activities of the Article 29 Working Party, as well as cooperate with the supervisory data protection authorities in the former third pillar with a view to improving consistency of their rules and procedures ([44]). 'Improving consistency' in the protection of personal data, in a wider sense, developed into a general mission.

While our bilateral cooperation with national authorities occurred to the extent necessary, our participation in the work of the Article 29 Working Party took place on a more permanent level ([45]). For many years, and in line with the general mission just mentioned above, the EDPS provided both the chair and the secretariat of the Working Party's subgroup on key provisions of Directive 95/46/EC, which prepared a series of opinions on the most important elements of the Directive ([46]). Although advisory in nature, these opinions expressed the common views of all data protection authorities in the EU and therefore had considerable influence, sometimes also visible in the case law of the Court of Justice ([47]).

The former third pillar of the EU covered the cooperation of EU Member States in the field of police and criminal justice. Supervision of the EU bodies in this area, such as Europol and Eurojust, used to be the responsibility of the national data protection authorities at national level, and a joint supervisory body with a common secretariat in the Council, at EU level. A comparable arrangement applied for a long time to the Schengen Information System ('SIS').

In the case of Eurodac, the EDPS has supervised the functioning of the Central Support Unit from the start, while developing a system of coordinated supervision with national data protection authorities. This new model was followed up with the Customs Information System in 2009, the Visa Information System in 2011, with SIS in 2013 and the Internal Market Information System

([44]) See Article 46(f) and (g) of Regulation (EC) 45/2001.

([45]) By the time the EDPS was established, the Supervisor was already one of the most senior members of the Working Party, who had also been its first chairman from 1996 onwards.

([46]) Article 29 Working Party Opinion 4/2007 on the concept of personal data, WP 136, adopted on 20 June 2007; Article 29 Working Party Opinion 1/2010 on the concepts of 'controller' and 'processor', WP 169, adopted on 16 February 2010; Article 29 Working Party Opinion 8/2010 on applicable law, WP 179, adopted on 16 December 2010; Article 29 Working Party Opinion 15/2011 on the definition of consent, WP 187, adopted on 13 July 2011; Article 29 Working Party Opinion 03/2013 on purpose limitation, WP 203, adopted on 2 April 2013; Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, adopted on 9 April 2014. Some of these opinions are still relevant as they influenced the GDPR and/or were endorsed by the EDPB. See also Kohnstamm, J., 'Privacy by debate. The European Data Protection Supervisor's Contribution to Collaboration between National Data Protection Authorities' in: Hijmans, H., Kranenborg, H. (eds.), op. cit. (footnote 10), p. 149-158.

([47]) See e.g. the judgment of the Court of Justice of 20 December 2017, *Nowak*, C-434/16, ECLI:EU:C:2017:994, paragraphs 33 to 35, on the notion of personal data.

in 2014. In each case, the EDPS typically acted as member of a Supervision Coordination Group and provided its secretariat. At a later stage, the EDPS was also entrusted with the supervision of both Europol and Eurojust, while coordinating with national authorities in various ways. The model of coordinated supervision thus reached maturity in a wider area than before ([48]).

At international level, the EDPS has been active in the European Conference of Data Protection Commissioners, with authorities from all Member States of the Council of Europe, and the International Conference of Data Protection and Privacy Commissioners (now known as Global Privacy Assembly) ([49]). However, together with the Council of Europe and the OECD, we also took the initiative for a series of workshops with International Organisations, who are typically not subject to any national or EU law, on how to integrate data protection in their activities ([50]). This cooperation was therefore truly global.

6. Final remarks

Developing from a very modest start, the EDPS was able to exercise considerable influence by concentrating on three main roles – supervision, consultation, and cooperation – and by emphasising that effective data protection should be seen as a condition for success. In this way, the first ten years provided the basis for how the EDPS is operating today.

All this could not have been accomplished without the support of a highly competent and dedicated staff who took part in our mission every step of the way, as well as the leadership of Christopher Docksey, who served as Director during an important part of this period. A good part of the credit is also due to Giovanni Buttarelli, who served as the second Assistant Supervisor from January 2009 until December 2014, when he and Wojciech Wiewiórowski, the current Supervisor, opened a new decade as a new team.

The splendor of the EDPS' 20th anniversary is now partly clouded by Giovanni's untimely passing during his first term as Supervisor, and we still sorely miss his participation at this event. Still, there are many reasons to be satisfied and proud of what has been accomplished, and to wish the EDPS and his entire team a safe and successful journey in the years ahead.

([48]) EDPS, The EDPS as Supervisor of Large-Scale IT Systems and Member of Supervision Coordination Groups, Policy Paper, issued in December 2015.

([49]) See also further the contribution by Matter. O., 'International cooperation: an imperative at the core of EDPS activities', Chapter 13.

([50]) See Hustinx, P., 'Data Protection and international organizations: a dialogue between EU law and international law', *International Data Privacy Law*, 2021, p. 77-80.

03

A tale of three Supervisors

Leonardo Cervera Navas

A tale of three Supervisors

Leonardo Cervera Navas (*)

In this contribution the EDPS' Secretary General, Leonardo Cervera Navas, offers his personal recollections of the leadership provided by the EDPS' first three Supervisors.

1. Personal recollections of three leaders

I worked closely with the three Supervisors who led the EDPS during its first 20 years: Peter Hustinx, Giovanni Buttarelli and Wojciech Wiewiórowski. I think that I know them well because for more than thirteen years now, since I landed at the EDPS from the European Commission, I have attended all Management Board meetings held on a weekly basis.

It is my hope that by sharing my personal recollections, future scholars will be able to better understand how the first three Supervisors, with their different personalities, working styles and values, shaped the EDPS and, more generally, data protection in the EU.

2. Peter Hustinx: be selective to be effective

My first encounter with Peter Hustinx happened eleven years before I joined the EDPS. In fact, I met him during my second day as a probationary EU official at the data protection unit of the European Commission, back in September 1999. I was asked to attend a meeting with a group of representatives of data protection authorities and Peter Hustinx was there as Head of the Dutch Data Protection Authority and Chair of the Article 29 Working Party, the advisory group set up by the Data Protection Directive.

(*) Secretary General of the EDPS.

I cannot recall the exact topic under discussion although I believe it referred to the application of the data protection legislation to the Internet (a novelty at the time, pretty much like Artificial Intelligence these days). Some Commission department disagreed with the data protection authorities about the way the Directive would apply in a specific context. There were several exchanges and when Peter Hustinx took the floor, he caused a great impression on me for two reasons: he spoke very clearly and was both polite and firm. Thanks to his intervention, the Commission representative left the room with a clear understanding of the position of the data protection authorities.

Peter Hustinx worked in the same way all the years he was the Supervisor. Very well organised, he kept dozens of physical folders all around his office with the most important information. I assume that his computer and his thoughts were arranged pretty much with the same methodology. He benefitted also from clear and strong values and a deep sense of pragmatism. One of its favourite mottos was "be selective to be effective" and this way of proceeding, interiorised by most employees at the time, helped tremendously at a time where the resources available were very limited.

His views on data protection were balanced and consistent, away from the dogmatism you could see in some jurisdictions but equally away from excessively liberal views. This balanced approach was very helpful when many things were still under discussion. He set up most of the things that are still in place at the EDPS twenty years later. Perhaps his best contribution to data protection in the EU was the intelligent way in which he persuaded the European Commission to consult the EDPS for every legislative proposal with an impact on data protection. This led to a massive influence in the way data protection evolved in the coming years and contributed to a strong data protection culture in the EU institutions, bodies, offices and agencies.

3. Giovanni Buttarelli: the sky is the limit

My first memories of Giovanni Buttarelli date back to the beginning of the 21st century. He was the Secretary General of the Italian Data Protection Authority, Il Garante. He would accompany his boss, Stefano Rodotá, to the meetings of the Article 29 Working Party in Brussels. He was a very clever and charismatic delegate who would participate in all discussions, often clashing personally and ideologically with Peter Hustinx. They both represented the north and the south of the EU and the slightly different way data protection is perceived due to cultural and legal differences between the Member States.

His arrival to the EDPS as Assistant Supervisor during the second term of Peter Hustinx was a bit stormy. When he became the leader of the institution six years later, he took decisive steps to separate himself from the way things had been

done by his predecessor. The inward, careful and mostly legalistic approach of Peter Hustinx was replaced by the outward, daring and highly mediatic approach of Giovanni Buttarelli.

Thanks to his personal charm, he became very popular in the data protection community worldwide. In one of the international conferences at the time, someone called him 'the George Clooney of data protection' because he was like a movie star in many respects. The sky was the limit for him so he did not adhere to the "be selective to be effective" motto of his predecessor. As he was someone very intuitive and resilient, some level of chaos and a last minute approach suited him just fine.

In October 2018, to reaffirm his undisputed leadership, he organised the 40th International Conference of Data Protection Authorities (later called the Global Privacy Assembly, the 'GPA'). Unfortunately, he was already quite sick and he would pass away few months later, in August 2019. He left us far too soon. Had it not been for his early demise, he could have secured a second mandate that would have probably been very successful as he was a true visionary.

His major contribution was, in my view, his personal involvement in the negotiations that led to the adoption of the GDPR and the setting up of the EDPB. He kept a copy of a newspaper in his office that called him "Mr. GDPR". It is clear that the GDPR had other fathers but he was definitively one of them and his legacy remains intact.

4. Wojciech Wiewiórowski: an empathetic leader

Contrary to Hustinx and Buttarelli, I do not have early memories of Wojciech Wiewiórowski, both because he joined the data protection community a bit later and when I was not attending the meetings of the Article 29 Working Party anymore. In fact, the first time I met him was in 2013 when he was walking down Rue de la Science in Brussels to participate in the selection procedure after which he would become Assistant to the European Data Protection Supervisor. I recognised him from the pictures I had seen on the Internet (as Head of the Polish Data Protection Authority) and stopped him to wish him good luck.

He joined the EDPS in 2014 and I immediately realised that he was a completely different kind of leader. He was not interested in public notoriety like Giovanni but rather in getting a good understanding of how things really work and in getting important things done. The expansive personality and the enormous ambition of Giovanni Buttarelli may have been problematic for any number two in the EDPS but not for Wojciech who gained Giovanni's trust, something that was of paramount importance to keep the organisation afloat when sickness struck the Supervisor.

Wojciech took over as Supervisor in December 2019, as the natural successor, and while he was still reflecting about his priorities for the third mandate of the EDPS, the Covid-19 pandemic turned the world upside down. He became a 'confined' Supervisor, with his staff teleworking from home. His empathetic leadership style was very helpful, not only to reassure EDPS employees, but also for providing the necessary responses to the many data protection challenges posed by the pandemic.

In February 2022, Putin's Russia launched a war of aggression on Ukraine, unleashing worldwide tensions and economic pressures that affected (and continue to affect) the world of data protection. Once again, Wojciech adjusted his plans to focus on what really mattered. Without many headlines but with a clear sense of purpose, his balanced and experienced views reached the global stage (e.g. in the G7 discussions), the European Court of Justice where the EDPS became a regular contributor, or powerful agencies, such as Europol of Frontex where he did not hesitate to take a firm stance when necessary. He grew up in a country ruled by the communist party so he does not need to be reminded about the importance of upholding democracy and fundamental rights.

During his mandate, many digital policies were unfolding in the EU – from the Digital Services Act to the upcoming AI Act – and the number of consultations skyrocketed. Wojciech focused once again on what really mattered and the EU legislator got solid and reliable advice from him. His best contribution to the EDPS and to data protection in the EU has been to ensure continuity and stability in a very difficult period, focusing on what really mattered.

5. A tale to be continued

A pragmatic Supervisor, a visionary Supervisor and an empathetic Supervisor led the EDPS in its first twenty years of existence. Thanks to these leaders, the organisation was effectively set up, gained recognition outside the EU bubble and became a solid and reliable partner for the other EU institutions. The three Supervisors came from the data protection community and were able to exercise their powers and duties with strong independence. Hence their success.

Someone else will continue this tale in the next twenty years. I can only offer a single piece of advice to the readers of the future that I am sure will survive the passage of time: please keep the protection of the human being and its dignity at the centre of this endless march towards integration, human progress and world peace that is the European Union.

04

The constitutional importance of data protection

Prof. Dr. Hielke Hijmans

The constitutional importance of data protection

Prof. Dr. Hielke Hijmans (*)

With the entry into force of the Treaty of Lisbon, data protection became an integral part of the EU constitutional legal order. This contribution explains how the Court of Justice of the European Union ('CJEU') and the EU legislator have given effect to the constitutionally safeguarded fundamental right to data protection. It also explores the essential elements of that right, including the requirement of by control by an independent authority.

1. Introduction

I remember how it all started for me at the EDPS, back in 2004. I showed my interest, triggered by the fact that I had read about the appointment of Peter Hustinx as Supervisor. I knew him vaguely from my period at the Ministry of Justice in The Hague in the second half of the nineties, when I was dealing with law and the Internet.

I met Peter and the also freshly-nominated Assistant Supervisor Joaquín Bayo Delgado at Rue Montoyer 63. A remarkable interview, with positive outcome, in a setting with offices, desks and computers – but no actual staff to protect personal data.

When I joined the EDPS on 1 October of that year, as one of the first staff members of the EDPS, the reactions – especially in circles of EU lawyers – were not super, to say the least: "What happened to you? Could you not find something else? We thought you were doing well in your professional life and now this?"

Data protection was a niche subject, not yet developed in the constitutional framework of the Union. There was Directive 95/46 ([1]), with an internal market

(*) President of the Litigation Chamber and Member Executive Board of the. Belgian Data Protection Authority. Professor (part time) at the Vrije Universiteit Brussel. This article only reflects the personal views of the author, and not those of the Belgian Data Protection Authority or its Litigation Chamber.

([1]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

legal base and the Court of Justice had just published its first two judgments, *Österreichischer Rundfunk and others* ([2]) and *Lindqvist* ([3]). Hence, data protection existed within EU law, but mentioning the word 'constitutional' as a characteristic of data protection would definitely be exaggerated.

This all changed quite rapidly. The Treaty establishing a Constitution for Europe ([4]) was signed on 29 October 2004, a few weeks after my arrival at the EDPS. Its Article 50 dealt with data protection; however, the treaty was rejected in referenda by French and Dutch voters in May and June 2005.

Nevertheless, much of the substance of the draft Constitutional Treaty remained unchanged in the Lisbon Treaty that entered into force on 1 December 2009. The aforementioned Article 50 was transformed into Article 16 TFEU, and the Charter of the Fundamental Rights of the Union became a binding instrument, with Treaty Status. As we all know, the Charter contains an Article 8 on Protection of personal data.

From December 2009, it was thus justified to refer to the constitutional *existence* of data protection, in the legal order of the Union. Data protection gained its constitutional *importance* in the years that followed, with the seminal judgments of the Court of Justice of the European Union ('CJEU'), in *Google Spain and Google* ([5]), *Digital Rights Ireland* ([6]) and *Schrems* ([7]). The constitutional importance of data protection became clearer when the EU legislator gave full effect to Article 16 TFEU, notably by adopting the General Data Protection Regulation ('GDPR') ([8]) and not to forget, in this *Festschrift* for the EDPS, the Regulation on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies ('EUDPR') ([9]).

Hence, the CJEU and the EU legislator gave effect to the constitutionally safeguarded fundamental right to data protection. Control by an independent authority forms part of this fundamental right of the individual.

The GDPR provides for a decentralised enforcement model, leaving the core of the enforcement with national administrative authorities. To be precise, this is not a *fully* decentralised model, since the GDPR contains a number of compensating mechanisms, to ensure that these national authorities operate in a harmonised manner, and are ultimately bound by the (majority) views of their peers, united in a European body, the European Data Protection Board ('EDPB').

([2]) Judgment of the Court of Justice of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294.

([3]) Judgment of the Court of Justice of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

([4]) Draft Treaty establishing a Constitution for Europe, OJ C 169, 18.7.2003, p. 1.

([5]) Judgment of the Court of Justice of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317.

([6]) Judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Seitlinger and others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

([7]) Judgment of the Court of Justice of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.

([8]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

([9]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

Also the enforcement model gives constitutional importance to data protection ([10]). In earlier work, I referred to the "in between status" of data protection authorities, since they operate in between the national and European jurisdictions ([11]). The model is a novelty under EU law, aiming at reconciling national enforcement of fundamental rights close to the citizen (sometimes referred to as the principle of 'proximity' ([12])) with the need for harmonised and effective enforcement which should lead to a level playing field in the EU.

These are the three constitutional aspects covered in this contribution: the protection of the fundamental right, the control by an independent authority and the delimitation between EU and national competences.

But before this, I start with the observation that, in the 2010s, data protection was no longer the niche subject. It had become a serious subject for practitioners of EU law.

2. The Court's case law: data protection triggering the constitutional development of the Union

It is safe to say that the inclusion of a binding Charter of Fundamental Rights in the Treaty framework of the Union was one of the main constitutional changes resulting from the Lisbon Treaty.

It is also safe to say that data protection triggered the real effect of this inclusion, starting with three seminal cases of the Court of Justice in this area.

The importance of *Google Spain and Google* lies *inter alia* in the fact that the CJEU recognised the right of a (Spanish) citizen to have links to his name removed from a search engine, a right that was made more prominent in the GDPR as 'the right to be forgotten' ([13]).

A lot has been written about *Google Spain and Google* ([14]), but let me specify why the judgment has importance from a constitutional perspective, as a trigger for taking fundamental rights seriously in the EU legal order.

First, the judgment ensured that the fundamental rights in the Charter are effectively safeguarded, including a balancing between the different Charter-rights which should take place.

([10]) See e.g. Brito Bastos, F. and Pałka, P., 'Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?' *European Constitutional Law Review*, Vol. 19, No. 3, 2023, p. 487-517.

([11]) Hijmans, H., *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*, Springer, 2016.

([12]) The notion of proximity was mainly put forward during the negotiations in Council on the GDPR, see various documents of Institutional File 2012/0011 (COD).

([13]) See Kranenborg, H., in: Kuner, C., Bygrave, L., Docksey, C. (eds.), *The EU General Data Protection Regulation: A Commentary*, Oxford University Press, New York, 2020, p. 475-484.

([14]) *Ibid*, literature mentioned on p. 483-484.

Second, the obligations under the Charter also apply in horizontal relations, where the obligations of private entities are defined in a broad manner. The obligations to guarantee fundamental rights protection obviously apply to entities that disseminate information (publishers), but equally to entities that facilitate the access to this information (such as search engines) ([15]).

Third, the Court widely interprets the territorial scope of EU law and the Charter, by reasoning that the processing of personal data carried out by an entity outside of the EU should not '*escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure*.' ([16]) Therefore, the Court construes a direct link between the Spanish establishment of Google and its headquarters in the United States, the actual data controller.

Fourth and final, the Court specifies that effective fundamental rights' protection requires a balancing between fundamental rights, *in casu*, on the one hand, the rights to privacy and data protection of Articles 7 of the Charter and, on the other hand, the freedom of expression and information guaranteed by Article 11 of the Charter ([17]).

This balancing is primarily the task of the search engines, which are provided by the Court with this social responsibility. In earlier work, I underlined that this approach strengthens ([18]) the fundamental rights protection, but does not necessarily guarantee democratic legitimacy.

One could add that this approach is a first recognition of the reality of the strong market powers of online platforms, and as a result the dependence of governments. The platforms are instrumental in ensuring the effectiveness of legal instruments. This approach became more predominant in later years. Good examples are the obligations under the Digital Services Act for very large online platforms and search engines. Since these platforms and search engines pose particular risks in the dissemination of illegal content and societal harms, they should comply with strict legal obligations ([19]).

Digital Rights Ireland ([20]) is the second case which demonstrates the constitutional importance of data protection for EU law. It was the first case where a directive under EU law was declared invalid. As the Court states: '*it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the*

([15]) Judgment of the Court of Justice of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraphs 32 to 41.

([16]) *Google Spain and Google*, see footnote 15, paragraph 58.

([17]) *Google Spain and Google*, see footnote 15, paragraph 76. The freedom of expression is not explicitly mentioned there; the Court clarifies this in its Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraphs 56 to 57.

([18]) Hijmans, H. op. cit. (footnote 11), Chapter 5.13.

([19]) Articles 33-43 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1.

([20]) Judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Seitlinger and others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter' ([21]). In other words, the Charter imposes limits on the powers of the EU legislator. When a legislative measure is adopted, the EU legislator should respect the Charter. This requirement even applies to a legislative measure which was adopted before the Charter has become binding. Just to recall, the data retention directive 2006/24 ([22]) was adopted in 2006, and the Charter became binding in 2009.

The constitutional importance of this judgment also lies, first, in the fact that it attempts to define the essence of the fundamental rights to data protection, and, second, in a qualification of breaches. An interference with fundamental rights can be particularly serious, but '*not such as to adversely affect the essence of those rights*' ([23]).

Finally, the Court made clear that the unlimited retention of communications data of all citizens amounted to such a serious infringement of Charter rights that it can never be justified([24]). As the Court ruled, '*the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*' ([25]). This line of thinking was later on confirmed and specified in further case law ([26]).

The third seminal case is *Schrems* ([27]), currently often referred to as 'Schrems I', in which the adequacy decision of the Commission, known as Safe Harbour ([28]), was declared invalid, because it did not comply with the requirements stemming from Directive 95/46 read in the light of the Charter. From a constitutional point of view, the importance of the judgment lies in the following elements.

First, the assessment of instruments of EU law under the Charter may also extend to external instruments, and may include the assessment of fundamental rights protection in a third country ([29]). After all, according to the Court, the adequacy decision enabled interference with fundamental rights, founded on national security and public interest requirements or on domestic legislation of the United States ([30]).

([21]) *Digital Rights Ireland and Seitlinger and others*, see footnote 20, paragraph 69.

([22]) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54.

([23]) *Digital Rights Ireland and Seitlinger and others*, see footnote 20, paragraph 39.

([24]) *Digital Rights Ireland and Seitlinger and others*, see footnote 20, paragraphs 57 to 61.

([25]) *Digital Rights Ireland and Seitlinger and others*, see footnote 20, paragraph 37.

([26]) A good example is the Judgment of the Court of Justice of 6 October 2020, *La Quadrature du Net and others*, C-511/18, ECLI:EU:C:2020:791. See also further the contribution by Kranenborg, H., 'The EDPS and the never-ending story of data retention', Chapter 6.

([27]) *Schrems*, see footnote 7.

([28]) Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7.

([29]) See also further the contribution by Kuner, C., 'International Data Transfers and the EDPS: Current Accomplishments and Future Challenges', Chapter 7.

([30]) *Schrems*, see footnote 7, paragraph 87.

Second, for the first time, the Court establishes that the essence of fundamental rights under the Charter was compromised, in particular Articles 7 (private life) and 47 (the right to effective judicial protection) thereof ([31]).

Third, the judgment addresses the enforcement model, with wider constitutional consequences. The Commission may use its implementing powers as provided under EU law to adopt a decision, but not in a way in which it denies a national supervisory authority the exercise of its powers, where a complainant before it puts forward matters that may call into question whether the Commission's decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals ([32]). Hence, powers granted to national authorities in the area of fundamental rights should be respected, also by an EU Institution.

3. To what extent does the GDPR trigger the constitutional development of the Union?

A regulation under Article 288 of the Treaty on the Functioning of the European Union ('TFEU') has general application and is binding in its entirety and directly applicable in all Member States. The GDPR is such a regulation. However, is it really binding in its entirety and directly applicable?

As the EDPS Opinion on the data protection reform package from 7 March 2012 ([33]) explains, there are many provisions allowing or providing for national law to play a role. The GDPR coexists in many respects with national law and national administrative procedure.

One could argue that the GDPR has elements of a directive, because many of its provisions leave to the national authorities the choice of form and methods, thus triggering the development of a hybrid between the instruments of regulation and directive ([34]).

Let me say a few words on enforcement. I already mentioned the constitutional embedding of the national enforcement authorities under EU law. The authorities, however, operate under national procedural law, whilst they have to coordinate their actions, in the context of the cooperation- and consistency mechanisms of Chapter VII of the GDPR. This is not evident: the principles of effective enforcement of EU law and of sincere cooperation should be reconciled with the procedural autonomy of the Member States.

([31]) See Brkan, M., 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core', *European Constitutional Law Review*, Vol. 14, 2018, p. 352-355.

([32]) *Schrems*, see footnote 7, paragraphs 102 and 103.

([33]) EDPS Opinion on the data protection reform package, issued on 7 March 2012, paragraphs 50-70.

([34]) Article 288 of the Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47 provides that '*A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods*'.

It is at this point where the Proposal for a Regulation laying down additional procedural rules relating to the enforcement of the GDPR ([35]) kicks in. This proposal is based on the view that important differences in national administrative procedures and interpretations of concepts in the GDPR cooperation mechanism hinder the smooth and effective functioning of the GDPR enforcement in cross border cases. According to the Commission, the '*Proposal ensures an appropriate balance between meeting the objective of ensuring the smooth functioning of cross-border enforcement of the GDPR while not unduly interfering with national legal systems*' ([36]).

To give a few examples of the interference with national legal systems:

- Article 3 of the Proposal specifies how to deal with a complaint, including the use of a complaint form with mandatory elements, according to a format laid down at EU level.
- According to Article 5, a complaint may be resolved by amicable settlement between the complainant and the parties under investigation, also in Member States where such a notion does not exist under national law.

The Proposal for a Regulation laying down additional procedural rules is an example of the constitutional importance of data protection: the objective of ensuring the smooth functioning of cross-border enforcement of the GDPR interferes by definition with national legal systems.

4. Constitutional law developing data protection

On the one hand, data protection is no longer a niche subject, if only because it has a big influence on the (constitutional) development of EU law. I explained that in the previous section.

On the other hand, data protection itself developed enormously thanks to its constitutional embedding in EU law. Of course, informatisation and the grown value of data play an equally big – or even bigger – role, but that is an angle I leave to others.

Let me go back to 2004. At the beginning of this article I noted that a reference to 'constitutional' in the context of data protection would be exaggerated in 2004 when the EDPS started its activities. This holds truth for EU law. However, the preamble of Directive 95/46 refers to the fundamental rights recognised in the constitution and laws of the Member States and in the European Convention

([35]) Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM(2023) 348 final. See also Mustert, L., 'The Commission Proposal for a New GDPR Procedural Regulation: Effective and Protected Enforcement Ensured?', *EDPL Review*, Vol. 9, No. 4, 2023, p. 454-464.

([36]) COM (2023) 348 final, p. 5-6.

for the Protection of Human Rights and Fundamental Freedoms ('ECHR') ([37]). In *Österreichischer Rundfunk and others* ([38]), the CJEU rules that the *'provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures*'. In *Lindqvist* ([39]), the Court refers more in general to the fundamental rights protected by the Community legal order.

The Lisbon Treaty has three direct consequences. First, whereas in *Österreichischer Rundfunk and others* the CJEU ruled that not all processing of personal data falls within the scope of fundamental rights, this is no longer the case. Second, the supervision has become a constitutional concern. Third, data protection falls by definition within the scope of EU law, with an in practice complete competence for the EU legislator. Article 16 TFEU provides that the EU legislator adopts *the* rules on data protection.

4.1. Constitutional importance, recognising rights and freedoms

Under Article 16(1) TFEU and Article 8(1) Charter 'Everyone has the right to the protection of personal data concerning *them* (TFEU) or *him or her* (Charter)'.

The TFEU mandates the ordinary legislator of the Union to establish rules to give effect to the right, whereas the Charter mentions the main elements of the right, that should in any event be included in those rules. Arguably, these elements could be considered the essence of the right.

Both the TFEU and the Charter lay down the mandatory control of independent authorities (TFEU) or of 'an' independent authority (Charter).

A constitutional right has an essence that cannot be touched ([40]). The term 'essence' is sometimes explained as the 'very substance' of a right ([41]), or with the German term 'Wesensgehalt' stemming from Article 19 of the Constitution of the Federal Republic of Germany ([42]). Essence is sometimes mentioned as the limit of limits ([43]).

([37]) Recital 1 of Directive 95/46/EC.

([38]) Judgment of the Court of Justice of 20 May 2003, *Österreichischer Rundfunk and others*, C-465/00, ECLI:EU:C:2003:294, paragraph 68.

([39]) Judgment of the Court of Justice of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraphs 87 and 90.

([40]) On the essence of the fundamental right to data protection, see González Fuster, G., *Study on the essence of the fundamental rights to privacy and to protection of personal data (EDPS 2021/0932)*.

([41]) Explanation of Article 52 of the Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391.

([42]) Translated into 'essence' in the English translation of the Basic Law for the Federal Republic of Germany, provided by the Federal Ministry of Justice and the Federal Office of Justice – www.gesetze-im-internet.de.

([43]) Tridimas, T. and Gentile, G., 'The Essence of Rights: An Unreliable Boundary?', *German Law Journal*, Vol. 20, p. 794, King's College London Law School Research Paper No. 2019-37. See also Brkan, M., op. cit. (footnote 31).

Whereas the Court has at several occasions mentioned the essence of the right to data protection, it has not ruled that this essence has been compromised ([44]), whereas it has established in *Schrems* that the essence of two other rights of the Charter was compromised, in the context of data protection: the right to respect for private and family life (Article 7 of the Charter) and the right to an effective remedy (Article 47 of the Charter).

This leaves some room for interpretation.

First, if one takes the view that the right does not equal the right to informational self-determination, but is a claim based to fairness. The processing of personal data as such cannot be considered to be a limitation of the right to data protection. I take that view, in line with a.o. Peter Hustinx ([45]).

This also means that the elements of the right to data protection mentioned in the Charter (mainly: fairness and purpose specification, consent or another legal basis, right to access and right to rectification) can be specified. However, these elements cannot be deprived of their basic substance. For example, EU or national legislation cannot provide that in certain areas individuals have no right to access whatsoever.

Second, as the Court observed, '*The establishment in Member States of independent supervisory authorities is thus an essential component of the protection of individuals with regard to the processing of personal data*' ([46]). This would mean that the absence of such an authority in certain domains would compromise the essence. This is for instance the case in the area of the common foreign and security policy, where the Council should adopt rules on data protection under Article 39 of the Treaty on European Union, but it did not, or in case of processing operations of courts acting in their judicial capacity, where no appropriate procedure is foreseen. Indeed, the data protection authorities are not competent following Article 55(3) GDPR ([47]).

Third, the right to data protection clearly has a procedural component, as the connection with Article 47 of the Charter shows. But, equally, the rights of access and rectification, as said included in Article 8(2) of the Charter are procedural rights.

An important procedural right is the right to lodge a complaint with a supervisory authority, which is specified in Article 77 GDPR. Arguably, this right for an individual to complain and to have his complaint handled is even part of the essence. As the recent *Schufa* judgment illustrates:

([44]) González Fuster, G., op. cit. (footnote 40) Table I, p. 29.

([45]) Hijmans, H., op. cit. 11, Chapter 2.11, and literature mentioned there.

([46]) Judgment of the Court of Justice of 8 April 2014, *Commission/Hungary*, C-288/12, ECLI:EU:C:2014:237, paragraph 48.

([47]) And the similar Article 45(2) of the Law Enforcement Directive (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89).

- Each supervisory authority is required on its territory to handle complaints and is required to examine the nature of that complaint as necessary. The supervisory authority must deal with such a complaint with all due diligence.
- Where, following its investigation, such an authority finds an infringement of the provisions of that regulation, it is required to react appropriately in order to remedy the shortcoming found.
- The complaints procedure, which is not similar to that of a petition, is designed as a mechanism capable of effectively safeguarding the rights and interests of data subjects ([48]).

4.2. Enforcement

The enforcement bodies have constitutional status, provided to them under Article 8(3) Charter and Article 16(2) TFEU. As specified by the CJEU, *'the supervisory authorities' primary responsibility is to monitor the application of the GDPR and to ensure its enforcement'* ([49]). The responsibility directly follows from EU Constitutional law. In that perspective, it is their constitutional mandate to ensure the respect of EU data protection law. Recital (2) of the GDPR refers to the need for protection of individuals, irrespective of their nationality and residence, as well as '*to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons*'.

How to ensure this constitutional mandate with a pan European component, where authorities operate within the national administrations and their decisions are subject to control by national courts?

This links to the various demands to modify the system towards more centralised enforcement ([50]).

As we know, the model of the enforcement of the GDPR already contains centralised elements, most predominantly with the role of the EDPB in the provisions of consistency (articles 63-67 GDPR). The question raises whether this is enough, or whether, as Bastos and Palka seem to claim, centralised GDPR enforcement is a constitutional necessity ([51]). They refer to Gentile and Lynskey ([52]) who identified four flaws of the current mechanism with a composite

([48]) Judgment of the Court of Justice of 7 December 2023, *SCHUFA Holding (Libération de reliquat de dette)*, Joined Cases C-26/22 and C-64/22, ECLI:EU:C:2023:958, extracts from paragraphs 56 to 58.

([49]) Judgment of Court of Justice of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraph 108.

([50]) As Politico reported on 22 January 2024, even Commissioner Reynders alludes that '*Europe's privacy law could be partially enforced from Brussels in the future, much like how competition law has been enforced for longer, and how digital platforms are overseen under the EU's new Digital Services Act and Digital Markets Act*'.

([51]) Brito Bastos, F. and Przemysław, P., op. cit. (footnote 10).

([52]) Gentile, G., and Lynskey, O., 'Deficient by Design? The Transnational Enforcement of the GDPR', *International & Comparative Law Quarterly*, Vol.71, Issue 4, 2022, p. 799 – 830.

administration: ambiguities and divergences in oversight, inequality of DPAs with a predominant role for the Lead Supervisory Authority, lack of procedural fairness and an unequal application of the law.

I limit myself in this article to the observation that in view of the constitutional basis of data protection authorities, where the enforcement concerns EU wide concerns, like for instance for the big platforms, a central authority might best be placed to deal with these concerns. A preference for centralisation is justifiable; I would not call it a necessity.

For the time being, however, it is more useful to aim for a more practical and feasible solution, i.e. addressing the flaws of the current system, by making progress in the work on the Proposal for a Regulation laying down additional procedural rules relating to the enforcement of the GDPR ([53]).

4.3. Constitutional importance, redefining the interaction between the EU and the Member States

Article 16 TFEU also redefines the competences of the Member States in the area of data protection. Data protection has become an EU competence, with no room for national law, unless specifically mandated in an EU Law instrument ([54]). An interesting example in this respect is Article 6 GDPR. National law can specify the legal grounds for processing in Article 6(1)(c) (legal obligation of the controller) or 6(1)(e) (public interest or exercise of official authority).

The national legislator, however, is not fully free when it adopts such a law. It should comply with the qualitative requirements under Article 6(3) GDPR. Moreover, the national legislator does not have any competence to adopt rules on one of the other legal grounds of Article 6. It cannot define what – in a specific context – constitutes a legitimate interest. As already clarified under Directive 95/46, national law cannot impose additional requirements to the EU conditions for legitimate interest ([55]). More recently, the Court confirmed that national law cannot definitively prescribe the result of the balancing of the rights and interests at issue ([56]).

This is a reality which is not always evident for all actors in the field, for instance because the protection of fundamental rights has always been a national competence, whereas in this specific area of fundamental rights – as a main rule – more strict national rules cannot be imposed.

([53]) COM(2023) 348 final. See also Mustert, L., op. cit. (footnote 35).

([54]) Hijmans, H., op. cit. (footnote 11), Chapter 4.3.2.

([55]) Judgment of the Court of Justice of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 39.

([56]) Judgment of the Court of Justice of 7 December 2023, *SCHUFA Holding (Scoring)*, C-634/21, ECLI:EU:C:2023:957, paragraph 70.

Also, the EU legislator struggles with this reality, as exemplified by Article 85 GDPR, which requires the Member States to reconcile data protection with the freedom of expression and information. Article 85(2) provides for at first sight almost unlimited exceptions, which seem difficult to combine with the – in practice – exclusive EU competence under Article 16 TFEU.

5. Epilogue

This article discusses the constitutional importance of data protection in EU law over the last 20 years. It takes stock of the situation in 2024. We find ourselves in a dynamic environment where technology, but also legal instruments relevant for data protection rapidly change.

The second *Schufa* judgment underlined the importance of human intervention in a context of artificial intelligence ([57]). More widely, the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) ([58]) and the subsequent legislative procedure in Council and Parliament demonstrate the need for reassessing the constitutional nature of data protection. Not only is the proposal (also) based on Article 16 TFEU, it equally illustrates that a starting point for data protection that the '*processing of personal data should be designed to serve mankind*' ([59]) requires further thinking, also in the perspective of human dignity. I recall Article 1 of the Charter: Human dignity is inviolable. It must be respected and protected.

As far as the constitutional position of data protection authorities is concerned, the new legal instruments under the EU digital package; such as the Digital Markets Act ([60]) and the Digital Services Act ([61]), require new thinking, based on the principle of sincere cooperation between data protection authorities and other competent authorities, as explained in the Court's *Meta* judgment ([62]).

([57]) *SCHUFA Holding (Scoring)*, see footnote *56*, paragraph 73.

([58]) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM(2021) 206 final.

([59]) Recital 4 of GDPR.

([60]) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1.

([61]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1.

([62]) Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraphs 53 to 63.

05

The ePrivacy Directive: then and now

Rosa Barcelo

The ePrivacy Directive: then and now

Rosa Barcelo (*)(**)

The ePrivacy Directive regulates some of the key privacy issues in the digital age, from confidentiality of electronic communications to online tracking. Since its adoption in 2002, the Directive has undergone changes with tremendous impact on individuals' privacy. This article discusses the main provisions of the Directive and focuses on two milestones in the Directive's development: the change to opt-in consent for online tracking in 2009, and the broadening of the confidentiality of communications rules of 2020 to cover instant messaging, emails, internet calling (through the adoption of the European Electronic Communications Code). The article also discusses how these changes to the Directive's scope impact the providers' ability to screen communications to combat the dissemination of online child sexual abuse material and the ongoing legal work being done to address this issue. The article's final section looks at the proposed ePrivacy Regulation.

1. A snapshot of the 2002 ePrivacy Directive

The ePrivacy Directive was adopted in 2002 ([1]), but most of its provisions originate from an earlier Directive on the same topic adopted in 1997 ([2]). The Directive sets forth rules aiming at the protection of privacy and personal data of users of electronic communications. In doing so, it particularizes and complements

(*) Rosa Barcelo is a partner at the law firm McDermott Will & Emery, based in Brussels. She specialises in Data Privacy and Cybersecurity. Rosa Barcelo worked as legal officer at the EDPS from 2006 to 2011 and at the European Commission (DG CNECT- Cybersecurity and Digital Privacy Unit) from 2011 to 2018.

(**) The author would like to thank her colleague Ania Ciesielska for her unevaluable support in the drafting of this article, in particular for her underlying research, comments and suggestions, which have greatly contributed to improve it.

([1]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37. The unofficial consolidated version of the 2002 ePrivacy Directive, as amended by 2009 Directive, is available on EUR-Lex.

([2]) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 024, 30.01.1998, p. 1.

the Data Protection Directive ([3]) (replaced subsequently by the General Data Protection Regulation, GDPR ([4])). It also implements the rights to privacy and to protection of personal data set out in Articles 7 and 8 of the Charter of Fundamental Rights of the EU ([5]) and ensures the free movement of data processed in the electronic communications sector. Moreover, it provides for the protection of the legitimate interests of subscribers who are legal persons.

Given that the Directive regulates privacy in the electronic communications sector, it relies on and cross-refers to the definitions contained in electronic communications legislation. With respect to the definition of consent, the Directive cross-refers to the GDPR. As EU Member States have transposed the provisions of the Directive into their legal orders, some divergences at national level exist ([6]).

1.1. Main content

While the core of the Directive is the protection of confidentiality of electronic communications, its provisions extend to many topics that can be explained in the following three groups.

The first group is about confidentiality of communications and of information in terminal equipment. It contains the rules on confidentiality of electronic communications and related traffic data (Articles 5, 6). Essentially, such rules require users' consent to listen, tap, store, or otherwise intercept communications or related traffic data in publicly available electronic communications networks. Traffic data must be erased or made anonymous when they are no longer needed for the conveyance of a communication or for billing. Similarly, location data other than traffic data can be processed where they are made anonymous, or with users' consent for the provision of a value-added service (Article 9). The Directive requires prior consent to access and/or store information in users' equipment, as it is deemed to be part of their private sphere (Article 5(3)) ([7]). Security requirements and notification of a personal data breach related to content and traffic data complete this first group.

([3]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

([4]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

([5]) Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391.

([6]) See notably two studies prepared for the European Commission DG Communications Networks, Content & Technology: (1) *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation (SMART 2013/0071)*, and (2) *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector (SMART 2016/0080)*.

([7]) Recital 24 provides that *'[t]erminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms*.

The second group includes the rules on direct marketing communications (Article 13), which require prior opt-in consent to use automatic calling machines or electronic mail for the purposes of direct marketing ('opt-in' rule) ([8]). An exception to this rule enables sellers to market similar products or services to their existing customers by electronic mail.

The third group includes several rules specific to the electronic communications sector, which in different ways, seek to protect the privacy of users of electronic communications. An example is the right to prevent the presentation of the calling line identification if users want to protect their anonymity (Article 8), or the right to stop automatic call forwarding by a third party and therefore prevent unwanted interferences (Article 11).

1.2. ePrivacy from 2002 to today

Since its 2002 adoption, the Directive has undergone several important changes, which have increased the initial protection of privacy and personal data. Some of them were the result of an initiative targeted at amending the provisions of the Directive directly (i.e., the amendments made by Directive 2009/136/EC ([9])). Some others were the result of repealing and replacing the acts cross-referred to by the ePrivacy Directive (i.e., the Data Protection Directive repealed and replaced by the GDPR; and the Framework Directive ([10]) – repealed and replaced by the EECC).

A. Direct changes

In 2009, the electronic communications framework was amended, to address competitive issues concerning broadband providers and the provision of spectrum, among others. Being part of that framework, the ePrivacy Directive was also reviewed. As further developed below, the most notorious 2009 amendment was the switch from opt-out to opt-in to access and/or store information in users' equipment, which had an enormous impact for users and companies involved in online tracking.

([8]) With respect to direct marketing calls carried out by regular calls, the Directive leaves it up to Member States to decide whether to impose a prior consent requirement (i.e., opt-in) or a right to object (i.e., opt-out). Opt-out solutions require organizations to check first whether an individual has registered on an opposition list or signed up to a 'Robinson list', and allow them to place marketing calls only to individuals who do not figure on such lists.

([9]) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, p. 11. This Directive was adopted as part of the amendments to the EU telecoms package, and specifically, it amended the Universal Services Directive and the ePrivacy Directive.

([10]) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, p. 33.

B. Indirect changes

On 25 May 2018, due to the GDPR becoming applicable and its Article 94(2), the references to the repealed Data Protection Directive were to be construed as references to the GDPR. This meant that the consent in the ePrivacy context (to which Article 2(f) referred to) changed and became the same as under Article 4(11) of the GDPR. All consents required under the ePrivacy Directive (e.g., consent for storing/accessing cookies, consent for sending direct marketing emails, or to process traffic data) had to fulfill the conditions of the GDPR.

On 21 December 2020, the EECC became applicable, repealing and replacing the directives of the EU telecoms framework. The ePrivacy Directive was not modified or repealed by the EECC. However, Article 2 of the Directive cross-refers to the definitions of electronic communications services contained in the EU telecoms framework. As the EECC's new definition of the electronic communications services included number-independent electronic communications services, this meant that services such as Voice over Internet Protocol, instant messaging applications and web-based email services ('Over-the-Top service providers' or 'OTTs') were brought within the scope of application of the ePrivacy Directive, indirectly modifying the original Directive. Then, in 2021, the Interim Regulation ([11]) derogated temporarily the confidentiality provisions of the ePrivacy Directive from applying to these new service providers.

C. Proposed change of the rules

Meanwhile, in 2017 the Commission had adopted the proposal for a Regulation on Privacy and Electronic Communications ('proposed ePrivacy Regulation') ([12]). The proposal's objective was to align the ePrivacy rules with the new general rulebook – the GDPR – and provide a level playing field for all market players, including OTTs. To date, the proposed ePrivacy Regulation is still undergoing the legislative process.

1.3. Is ePrivacy needed in a GDPR reality?

After the GDPR was adopted, some questioned the need for the ePrivacy rules. Some of the ePrivacy Directive's provisions seek to protect personal data in the electronic communications sector, which means content, traffic and location data. Such rules are more specific and granular than their counterparts in the GDPR. Some argue that the general principles of the GDPR would suffice,

([11]) Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, OJ L 274, 30.7.2021, p. 41.

([12]) European Commission's Proposal of 10 January 2017 for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 010 final.

complemented as needed by regulatory guidance. Having a separate legal framework may provide some additional legal certainty and harmonization, but it is not absolutely needed.

The EDPS and the Article 29 Working Party ('WP29') (and the European Commission) have disagreed with these views. While the GDPR protects personal data, the ePrivacy rules aim at protecting *also* the confidentiality of electronic communications, as well as the integrity of one's device, independently of processing any personal data. These protections implement a different fundamental right, the right to private and family life, home and communications (referred to as 'privacy'). These protections would not be afforded by the GDPR alone. This view was also shared by the WP29 ([13]).

The same is true in relation to the protection of the legitimate interests of legal persons, which are covered under the ePrivacy Directive, but not the GDPR.

The EDPS has also shared the view that sectoral rules are necessary, as reliance merely on Article 7 of the Charter of Fundamental Rights of the EU to put in practice the principle of confidentiality of electronic communications would not ensure legal certainty ([14]). Hence, there is a need for secondary legislation setting forth clear and specific rules to that end. Further, the EDPS noted that the EU privacy and data protection framework would be incomplete without such rules: *'While the GDPR (…) is a great achievement, we need a specific legal tool to protect the right to private life guaranteed by Article 7 of the Charter of Fundamental Rights, of which confidentiality of communications is an essential component'* ([15]).

2. A closer look at the 2009 update

The 2009 amendments to the ePrivacy Directive, still in force today, were adopted through Directive 2009/136/EC. Other than the amendment to the cookie consent rule explained below (Section 3), most of the amendments provided for enhanced privacy protection that was saluted by the privacy community, including the EDPS and the WP29, without manifest rejection by providers of electronic communications services. Examples include the introduction of enhanced security obligations and a personal data breach notification requirement (Articles 4(1a) and (3) respectively), the reinforcement of the competent authorities' powers and the penalties (Article 15a) and the possibility for any natural or legal person adversely affected by unsolicited communications to bring legal proceedings before courts (Article 13(6)).

([13]) Article 29 Working Party Opinion 1/2017 on the Proposed Regulation for the ePrivacy Regulation (Directive 2002/58/EC), WP 247, adopted on 4 April 2017, p. 3, paragraph 2.

([14]) EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), issued on 24 April 2017, p. 7, paragraph 1.

([15]) *Ibid*, Executive Summary, p. 3.

Regarding the mandatory breach notification, the Commission was empowered to adopt implementing measures regarding the circumstances, format and procedures, which it did through a Data Breach Commission Regulation ([16]).

The EDPS was actively involved in the development of the personal data breach notification requirement. While the European Commission had initially proposed leaving to comitology the development of the data breach requirements, the EDPS supported European Parliament's amendments (which were finally adopted), developing the breach provisions in the Directive itself. On the scope of the data breach notification, while the European Commission and the Council aimed to limit its scope of application to providers of electronic communications services, the European Parliament (with the EDPS and WP29's support) were in favour of expanding it to providers of information society services. In his second opinion on the review of the ePrivacy Directive ([17]), the EDPS advocated and substantiated why this notification should be expanded to such providers. While eventually, the broad mandatory breach notification was not included in the 2009 amendments to the ePrivacy Directive, it laid solid foundations for adding such mandatory notification system to the General Data Protection Regulation a few years later.

3. Article 5(3): the new standard for online tracking

The key amendment of the 2009 review is certainly the new Article 5(3), currently known as the 'cookie consent rule' and Directive 2009/136/EC introducing it as 'the Cookie Consent Directive'. The amendment requires consent to storing information or gaining access to information already stored on terminal equipment (such as storing a cookie, or reading a cookie already stored, on a computer). The requirement changed the opt-out rule (i.e., offer the user the right to refuse) of the 2002 ePrivacy Directive to an opt-in rule, i.e., obtain user's consent (unless one of the two exceptions applied – which remained the same). This change is an important step forward in terms of protecting privacy online. It empowers users to make informed choices as to whether to accept online trackers, which until that point were rather hidden, thus leading to invisible online tracking.

Given websites' widespread use of cookies and other tracking technologies to obtain users' information for different purposes (analytics, targeted advertising), every website or application became (and remains today) impacted by this provision. Up until the adoption of the cookie consent rule, the market practice was to provide cookie information and the right to refuse in websites' privacy

([16]) Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L 173, 26.6.2013, p. 2.

([17]) EDPS Second Opinion on the review of Directive 2002/58/EC, issued on 9 January 2009.

policies. After the cookie consent rule became applicable, this has been replaced by cookie consent banners, cookie preference centers and further information has been increasingly provided in dedicated cookie policies.

Interestingly, this change was not included in the European Commission's proposal ([18]), but was later proposed by the European Parliament ([19]). This may explain why the EDPS and WP29's initial opinions did not comment on it.

As for the European Parliament, its amendment proposed not only to reverse the opt-out rule with the opt-in, but also that '*browser settings constitute prior consent*'. Given that most browsers accepted cookies by default, the consent requirement would probably have had little or no effect since everyone would be deemed to be consenting to cookies (as it is well known that settings are seldom changed).

However, the European Parliament's amendments regarding browser settings did not make it to the final version of the law ([20]). Several factors may have contributed to it. One of them worth highlighting may be the revelation, at the time when the ePrivacy amendments were discussed, of Flash cookies (sometimes called zombie cookies or super cookies) and their quite widespread use ([21]). Thanks to their tracking identifiers, Flash cookies would persist even if a user cleared their browser cookies (i.e., HTTP tracking cookies). This may have prompted the need to give more transparency and control to users as to whether they wanted to have cookies in the first place and removed the possibility for browsers settings to signify consent.

The privacy community (including the EDPS and the WP29) may have formally and informally supported its adoption and pleaded for the removal of the reference to browser settings as a tool to signify consent. Indeed, in its Opinion on the proposals amending the ePrivacy Directive, the WP29 strongly objected

---

([18]) European Commission's proposal for Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, COM(2007) 0698 final.

([19]) European Parliament legislative resolution of 24 September 2008 on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p.37 and Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation), OJ L 364, 9.12.2004, p. 1. The Parliament's relevant amendments are in bold: '*Member States shall ensure that the storing of information, or gaining access to information already stored, in the terminal equipment of a subscriber or user, either directly or indirectly by means of any kind of storage medium, is prohibited unless the subscriber or user concerned has given his/her prior consent, taking into account that browser settings constitute prior consent, and is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing and is offered the right to refuse such processing by the data controller. (..).*'

([20]) While the reference to browser settings constituting consent disappeared from the operative provision of Directive 2009/136/EC, a trace of it was left in Recital 66, which provided that '*Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.*'

([21]) See, e.g., Soltani, A., Canty, S., Mayo, Q., Thomas, L., Hoofnagle, C. J., *Flash Cookies and Privacy*, *SSRN*, 2009.

to the Parliament's amendment in that regard ([22]). Finally, the fact that the ePrivacy Directive review and adoption was taking place at the same time as the rest of the review of the entire EU telecom package, with many other challenging issues on the table of the co-legislators, may explain why the cookie consent rule was smoothly approved.

After the adoption of Article 5(3), industry showed strong dissatisfaction. It was argued that prior analysis of its practical and economic effects, which may not have been obvious to legislators, had not taken place.

3.1. Interpretative guidance and CJEU judgements

Article 5(3) aims to protect the confidentiality of the information contained in terminal equipment, for example, against viruses, stealing of information and tracking for a variety of purposes, including offering targeted advertisement. This is well explained in Recitals from 2002 ([23]), when the standard was opt-out. However, the 2009 adoption of the cookie consent rule was hardly accompanied by any Recital interpreting how the cookie consent would regulate online tracking and what it would mean in practice ([24]).

After its adoption, some criticized the ability of Article 5(3) to regulate online tracking, its intrinsic limits to achieve this goal and the lack of answers to some issues. The EDPS, the WP29, the EDPB and national authorities have remedied its shortages with abundant clarifications and interpretative guidance on its application to cookies ([25]), digital fingerprinting ([26]), connected vehicles ([27]), and to other technologies ([28]).

([22]) Article 29 Working Party Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), W159, adopted on 10 February 2009, p. 10, paragraph 1: *'The Working Party strongly objects to the amendment 128 adopted by the Parliament, stating that default browser settings would be a means to provide prior consent'*.

([23]) *(24) '(…) So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.'*

(25) 'However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. (…).'

([24]) See Recital 66 Directive 2009/136/EC.

([25]) Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption, WP 194, adopted on 7 June 2012.

([26]) Article 29 Working Party Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224, adopted on 25 November 2014.

([27]) EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, adopted on 9 March 2021.

([28]) Article 29 Working Party Opinion 2/2010 on Online Behavioral Advertising, WP 171, adopted on 22 June 2010; EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, adopted on 14 February 2023; or EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, adopted for public consultation on 14 November 2023.

Case law has also helped. For example, in October 2019, in its judgment in the case *Planet49* ([29]), the Court of Justice of the EU ('CJEU') clarified that a pre-selected checkbox, which the user would have to deselect to refuse his or her consent, does not constitute a legally valid consent. This judgment had an important effect on websites, some of which had to correct their practices in this regard.

3.2. Genuine choice in the era of online tracking proliferation?

The proliferation of online tracking and forceful enforcement of the rules has meant that cookie consent banners have become a reality for already many years. Market practices have been and continue to be shaped by enforcement ([30]) – in some cases triggered by complaints filed by privacy campaigners ([31]). Over the years, market practices have led to a relatively high granularity of choices in cookie consent banners. There seems to be more acceptance amongst industry of the need to empower users to be able to make informed and genuine choices. At the same time, it is common to read that there is a certain cookie fatigue, including among users. This has and continues to trigger attempts to find ways to empower individuals, without endangering the user interface. For example, in the explanatory memorandum to the proposal for the ePrivacy Regulation, the Commission noted that '*the consent rule to protect the confidentiality of terminal equipment failed to reach its objectives as end-users face requests to accept tracking cookies without understanding their meaning*' ([32]). Similarly, the EDPS noted that '*Article 5(3) of the ePrivacy Directive, as currently applied, has failed to live up to its potential to provide a genuine opportunity to choose, and to give control to the individuals. Instead, consent mechanisms have been developed by businesses and other organisations with the objective of arguably meeting the bare legal requirements for compliance under the ePrivacy Directive but failing to give users a genuine choice and control over what is happening to their data*' ([33]). To help fix this problem, the proposed ePrivacy Regulation added an exemption from obtaining consent in case of cookies and other technologies used for web audience measuring purposes (Article 8(1)(d)) and a possibility to express consent through settings of a software application such as browser (Article 9(2)), provided that such consent is legally valid.

([29]) Judgment of the Court of Justice of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, point 1 of the operative part of the judgment.

([30]) For instance, the French Data Protection Authority has been known for its consistent enforcement of the cookie consent rules, as transposed into the French legal order, accompanied by significant fines.

([31]) See e.g., EDPB, Report of the work undertaken by the Cookie Banner Taskforce, adopted on 17 January 2023.

([32]) COM(2017) 10 final, p. 5.

([33]) EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), issued on 24 April 2017, p. 17, paragraph 1.

In 2023, the European Commission launched a 'Cookie Pledge', i.e., a reflection process on how to better empower consumers to make effective choices regarding tracking-based advertising models. This has led to formulating high-level draft principles, adherence to which would be voluntary, to address the current shortcomings ([34]).

While the question may seem to focus on cookies, it is also valid in relation to other similar technologies. Indeed, as technology and market practices continue to evolve, so will regulatory guidance (see, e.g., the EDPB Guidelines on technical scope of Article 5(3)) and jurisprudence, which, by their nature, have a reactive effect.

4. Broadening the confidentiality rules to OTTs

As explained in Section 1.2, when the EECC was adopted with a new definition of electronic communications services encompassing OTTs, this extended Directive's scope of application to such services. This means that OTTs are now bound by the rules on confidentiality of electronic communications and related traffic data, restrictions on the use of location data, designed back in 2002 for traditional telecommunications operators. Potentially, OTTs could find themselves subject to data retention obligations, if national laws would provide so, in line with Article 15 of the ePrivacy Directive.

The broadening of the scope to OTTs was one of the main objectives of the proposed ePrivacy Regulation (see Section 5). Interestingly, while the Proposal was making its way through the legislative process, the inclusion of OTTs happened independently of the proposed ePrivacy Regulation.

4.1. Are the rules enforced vis-à-vis OTTs?

Some of the major OTTs such as instant messaging or email services have adapted their data processing practices in compliance with the ePrivacy Directive. In some cases, this is visible from publicly available privacy notices stating that traffic data generated by such services are handled in line with the requirements of the ePrivacy Directive.

Whether the ePrivacy rules are being effectively enforced by competent national authorities is uncertain. No cases of enforcement of the electronic communications confidentiality rules with respect to OTTs have been publicly reported. Surprisingly, other than in relation to legislative initiatives on combating the dissemination of online child sexual abuse materials, the EDPS or EDPB have not issued statements welcoming the application of the ePrivacy Directive to OTTs (even though both supported it in the context of the proposed ePrivacy Regulation).

([34]) European Commission's page dedicated to the Cookie Pledge. At the time of writing this article, the European Commission aimed to present the final version of the principles in April 2024.

The authorities' silence may be due to the fact that not all data protection authorities are entrusted with the supervision and enforcement of the ePrivacy rules. Indeed, under the ePrivacy Directive, it is up to EU Member States to designate the competent authorities. Some Member States have designated telecoms regulators, and it may be that the ePrivacy rules are not an enforcement priority for them. This may be somehow surprising, as covering OTTs by the principle of the confidentiality of communications was one of the key purposes of the proposed ePrivacy Regulation, and endorsed by the privacy community. On the other end of the spectrum, law enforcement authorities of some Member States appear to be using the national legislation (setting forth exceptions pursuant to Article 15(1) of the ePrivacy Directive) to require OTTs to retain communications data, just like some require traditional telecoms operators to do.

4.2. Interim Regulation

A. Why was it needed?

Some OTTs voluntarily use technologies such as PhotoDNA to scan electronic communications in order to detect, report and remove online child sexual abuse materials ('CSAM') from their services. Up until 20 December 2020, such scanning was covered by the GDPR – insofar as personal data were concerned – and OTTs could rely on the legitimate interests legal basis. When the EECC entered into application on 21 December 2020, OTTs had to abide by the ePrivacy Directive's confidentiality rules, which does not include a legitimate interests legal basis. Instead, the Directive essentially requires users' consent to conduct such scanning. Relying on consent would obviously devoid the activity of its purpose. Another potential possibility was to rely on national law adopted pursuant to Article 15(1) of the Directive (if there was any), that would enable OTTs to carry out such processing (subject to appropriate safeguards, and where that national law would apply to the communication at hand). At the EU level, there was no such measure available.

B. Temporary derogation from OTTs' confidentiality requirements

As the protection of children is one of the Union's priorities, EU co-legislator adopted in July 2021 the Interim Regulation to address this issue temporarily, pending the adoption of a dedicated fully-fledged regulation at EU level. The Interim Regulation aims to enable OTTs to continue their voluntary activities with respect to detecting, reporting and removing online CSAM from their services, provided that they comply with the GDPR as far as the processing of personal data is concerned and they meet a number of specific conditions set forth by the Interim Regulation. Given the critical importance of the issue, as well as the implications on confidentiality of communications, the EDPS has published an Opinion with recommended necessary safeguards to be added

to the Interim Regulation ([35]). The temporary derogation from conforming with the ePrivacy Directive's provisions regarding the confidentiality of electronic communications (including traffic and location data) expires on 3 August 2024. However, given that the EU co-legislator has not adopted yet the fully-fledged regulation (see Section 4.3 below), the European Commission has proposed to extend the Interim Regulation's derogation until 3 August 2026 ([36]). The legislative process on this proposed Regulation is ongoing, with co-legislators proposing different timelines. In that context, the EDPS has reiterated its views in an Opinion ([37]).

4.3. The proposed CSAM Regulation

In May 2022, the Commission adopted a proposal for a Regulation to prevent and combat online CSAM (the proposed CSAM Regulation) ([38]).

This long-term legislation is expected to replace the Interim Regulation. The proposed CSAM Regulation lays down a framework for providers falling within its scope (which includes OTTs) to address online CSAM and solicitation of children for sexual purposes in the internal market. Among others, it requires providers to carry out assessments to identify and minimize the risk of their services being used for the purpose of online CSAM and solicitation. The proposed CSAM Regulation provides for national courts or independent authorities to issue detection orders, requiring providers to put in place scanning technologies to detect CSAM and solicitation.

The proposed CSAM Regulation has raised important issues connected to the principle of confidentiality of communications. While the scope of this article does not permit to delve into the details, below we note some of key issues discussed in the context of the legislative process. At the time of writing, the proposal continues its way through the legislative process and it is uncertain how these issues will be addressed.

A. Scanning on a voluntary basis

First, whether OTTs should be allowed to continue scanning electronic communications on a voluntary basis. To do so, they would need to have a legal basis under the ePrivacy Directive ([39]) to engage in voluntary detection. Under

([35]) EDPS Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, issued on 10 November 2020.

([36]) European Commission's Proposal of 30 November 2023 for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/1232 of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC for the purpose of combating online child sexual abuse, COM(2023) 777 final.

([37]) EDPS Opinion 8/2024 on the Proposal for a Regulation amending Regulation (EU) 2021/1232 on a temporary derogation from certain ePrivacy provisions for combating CSAM, issued on 24 January 2024.

([38]) European Commission's Proposal of 11 May 2022 for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final.

([39]) Or be allowed to derogate from complying with the confidentiality rules, such as in the Interim Regulation.

the proposed CSAM Regulation, scanning is only envisaged with a detection order. The CSAM Proposal repeals the Interim Regulation, which provides for a derogation from complying with the ePrivacy Directive to enable voluntary scanning. This means that other than under the circumstances foreseen by the proposed CSAM Regulation (when a detection order exists), scanning would not be allowed (as the ePrivacy Directive does not provide for a legal basis). Against this backdrop, some stakeholders have advocated for voluntary detection to remain lawful (and hence for the proposed CSAM Regulation to confirm that they can derogate from the ePrivacy Directive and rely on the legal bases of the GDPR). On the other hand, the EDPB and EDPS support the Commission's conclusion that the consequences of the deployment of voluntary detection measures are too far-reaching and serious to leave the decision on whether to implement such measures to the service providers ([40]).

B. End-to-end encryption

Probably one of the most controversial aspects of the proposed CSAM Regulation are the implications of detection orders for end-to-end encryption ('E2EE'). The Proposal is technologically neutral as to the choice of the technologies to be operated to comply with detection orders. However, stakeholders, including data protection authorities and some OTTs, have voiced their concerns that detection orders would undermine E2EE, which is deemed critical to protect confidentiality of electronic communications.

5. The Proposed ePrivacy Regulation

As mentioned, on 10 January 2017, the Commission adopted the proposed ePrivacy Regulation. Seven years after its adoption, the proposed ePrivacy Regulation remains in the legislative process. The European Parliament's plenary voted in October 2017 and agreed to enter into the interinstitutional negotiations with the Council, based on the LIBE Committee's amendments to the proposed ePrivacy Regulation, while the Council adopted its position in 2021. Since then, co-legislators have not been able to find common ground and adopt the regulation.

This section takes a brief look (glimpses at) the consequences of the adoption of the ePrivacy Regulation in relation to confidentiality of electronic communications and in relation to the cookie consent provision.

([40]) EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, issued on 28 July 2022. See also the Summary report of the EDPS Seminar on the CSAM proposal: "The Point of No Return?", issued on 10 November 2023.

5.1. Confidentiality of electronic communications

One of the main aims of the proposed ePrivacy Regulation was to expand its scope of application to OTTs, providing privacy protection regardless of the means of communications used and ensuring a level playing field for all providers offering electronic communications. The explanatory memorandum of the proposed ePrivacy Regulation refers to the increased use of internet-based services enabling interpersonal communications such as Voice over IP, instant messaging and web-based email services, instead of traditional communications services. The Proposal explains that one of its main objectives is to ensure that the principle of confidentiality applies to current and future means of electronic communications, including the ones described above (i.e., the Proposal is technologically neutral). While such services had to abide by the general data protection rules (the GDPR) insofar as they processed personal data, they were not subject to the confidentiality rules, and could process traffic and location data for any legitimate purpose and without user's consent (provided that they relied on another legal basis of Article 6(1) GDPR and, in case of special categories of personal data, complied with Article 9(2) GDPR).

Given that this outcome already happened through the adoption of the EECC, the consequences of the adoption of the ePrivacy Regulation could, from this perspective, appear quite limited. However, the proposed ePrivacy Regulation would present at least two advantages vis-à-vis the current situation on this aspect, further described below.

A. Rules tailored to OTTs

Compared to the Directive, the new rules would be more adapted to their application to OTTs. As an example, the Directive is almost entirely silent in relation to content of (written) communications. This made sense at the time of its adoption in 2002, when traditional telecommunication operators were used mainly for oral communications (other than for the use of SMS messages). Hence, the Directive was mainly focused on traffic data related to calls, not to messages. Therefore, the application of the Directive to instant messaging, emails and similar written communication leaves many open questions in relation to content data. Compared to the rules set by the Directive, the proposed ePrivacy Regulation, including under the European Parliament and Council amended versions, provides explicit rules on the processing of electronic communications content, thus giving more clarity as to their application to content of communications.

B. More effective enforcement

The proposed ePrivacy Regulation would vastly improve the effectiveness of the application of the Directive upon OTTs by virtue of its enforcement framework and penalties (this applies also in relation to the Parliament and Council versions). Indeed, it designates data protection authorities as competent

authorities to enforce the ePrivacy rules, with the consistency and cooperation mechanisms of the GDPR applying *mutatis mutandis*. As the Directive leaves it up to Member States to designate the competent national authorities entrusted with the enforcement of the Directive, the enforcement landscape across the EU is fragmented. Infringements of the Directive cannot be investigated and agreed under the GDPR consistency and cooperation mechanisms. Regarding infringements, the proposed ePrivacy Regulation provides for the same level of fines as the GDPR. This would significantly improve the current situation, where the level of fines is left to Member States and is vastly lower than the fines under the GDPR.

5.2. Cookie consent rules

The proposed ePrivacy Regulation largely retains the current Directive requirement to obtain consent to set or read information such as cookies and similar technologies (as it retains the two main well-established exceptions to this requirement).

Vis-à-vis the current Directive, the proposed ePrivacy Regulation presents some novelties and adaptations. First, it extends the list of exceptions to the consent rule in various ways. For example, first party analytics cookies would be allowed without consent, in line with prior guidance from the EDPS ([41]). The Council's general approach ([42]) further expands the exceptions to cookies that are necessary for security purposes and those necessary for software updates. Second, the Commission proposal, Parliament's proposed amendments and Council's general approach all have (different) rules which, in different ways, give users the ability to control the use of certain types of cookies by whitelisting one or several providers/cookies. The goal pursued by this rule is to limit the cookie consent fatigue, without disempowering users in relation to their ability to control whether they want cookies. This goal is currently still fully relevant: there is still a need to streamline the way individuals consent to cookies and other technologies. Recently the Commission started developing other approaches, such as the Cookie Pledge aiming to achieve the same goal (See Section 3.2).

However, some of the purposes of the proposed ePrivacy Regulation in relation to cookies have been somehow addressed through other means, including by jurisprudence or guidance. For example, in Recital 20aaaa, Council's mandate for the negotiations with the European Parliament regarding the proposed ePrivacy Regulation provides that cookie walls are permissible provided that the user has a real choice ([43]), i.e., can choose between different services on the basis of clear, precise and user-friendly information about the purposes of cookies or similar techniques. Since then, some data protection authorities have

([41]) Preliminary EDPS Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC), issued on 22 July 2016, p. 17.
([42]) Council's mandate for negotiations with the European Parliament, document no. 6087/21, adopted on 10 February 2021.
([43]) *Ibid.*

ruled or given guidance setting forth the conditions under which cookie walls would be valid. For example, the French CNIL provided four points to consider when assessing the legality of cookie walls (whether there is alternative access to content, the price of that access, paid access without cookie placement and potential embedded consent overrides) ([44]). Meanwhile, in the case involving Meta Platforms Inc., Meta Platforms Ireland, and Facebook Deutschland (Meta), the CJEU ruled that users must be free to refuse consent (in the case of free online services), without being obliged to refrain entirely from using the service. And the judgement adds that *in such case, 'those users are to be offered (by the provider), if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations*". While this applied to social media services, arguably the same rationale could possibly be applied in relation to cookie walls.

6. Conclusion

The ePrivacy Directive remains key for the protection of confidentiality of electronic communications. Its 2009 update was a response to the advent of new privacy-intrusive technologies and played a crucial role in enhancing individuals' privacy and integrity of their devices. The subsequent legislative developments – the GDPR in 2018 and the EECC in 2020 –further strengthened these protections. With respect to the integrity of one's device, guidance of the EDPB, the WP29 and individual competent national authorities, together with CJEU judgments, have been crucial in filling the gaps. While the proposed ePrivacy Regulation has not been adopted and new technology continue to advance and market practices to evolve, such guidance and jurisprudence will likely continue to serve this role.

The Directive remains a very powerful tool. At the same time, its full potential cannot match that of the level of the GDPR, due to its low level of fines and enforcement set up, lacking 'teeth' and a proper cooperation and consistency mechanisms. Other areas for improvement include solving the cookie consent fatigue and providing a clearer framework for the processing of content and traffic data by OTTs, including in relation to online CSAM.

([44]) CNIL, Cookie walls: la CNIL publie des premiers critères d'évaluation, 16 May 2022.

06

The EDPS and the never-ending story of data retention

Prof. dr. Herke Kranenborg

The EDPS and the never-ending story of data retention

Prof. dr. Herke Kranenborg (*)

The two decades during which the issue of data retention has been discussed at EU level, shows the difficulty and sensitivity of the debate on how to achieve a proper balance between privacy and security in the modern digital society. The EU Court of Justice ('CJEU') took a firm stance in the debate, causing uproar in the EU Member States. Despite the fierce criticism from the law enforcement side, the CJEU stood by its position, thereby acknowledging the importance and great value of the Charter of Fundamental Rights.

From the moment the matter reached EU level, the EDPS made an important contribution to the debates, which eventually led to the invalidation of the infamous Data Retention Directive by the CJEU in 2016. But also after the invalidation, the EDPS continued to provide critical input, in particular during the hearings before the CJEU for which he was invited multiple times and in which national measures of data retention were debated.

1. Introduction

When discussing the matter of 'data retention', one can be assured of lively debates. Data retention classically refers to measures that require the retention of telecommunications data by telecom operators for possible access and use by law enforcement and national security authorities. Such a preventive measure, concerning all users, has always been a controversial issue. In a way, the issue serves as a proxy for a more fundamental debate about how to achieve a proper balance between privacy and security in the modern digital society.

(*) Herke Kranenborg is a member of the Legal Service of the European Commission and professor in European Privacy and Data Protection Law at Maastricht University. This contribution is written on a personal title.

It goes without saying that telecommunications data can offer crucial evidence in the fight against crime or can be crucial for measures protecting national security. On the other hand, such data, even if limited to so-called 'metadata' and not including the content of communications, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained ([1]). These opposing interests must be reconciled. How far can governmental interference with the rights of individuals go, to the benefit of maintaining law and order and of ensuring the security of the state?

From the moment the issue reached the level of the European Union, the EDPS played an active role in this debate.

2. Data retention as matter of EU law

The discussion on data retention, as a preventive law enforcement measure, was pushed to the level of the European Union in April 2005, when several EU Member States, on the basis of the former third pillar of the Union, proposed a Framework Decision intending to harmonise national data retention measures ([2]). It required EU Member States to put in place generalised and indiscriminate retention schemes as regards the metadata of subscribers generated by the telecom providers. To be noted, the majority of EU Member States did not have such rules in place.

After the terrorist attacks in London in July 2005, urgent action was requested from the EU. In September 2005, the European Commission proposed a parallel draft Directive on data retention, based on the former first pillar of the EU, which meant that the instrument was subject to the ordinary legislative procedure, including the European Parliament and the Council. Although both proposals prescribed a generalised and indiscriminate retention of metadata, the European Commission proposal was more limited compared to the draft Framework Decision, in particular in terms of retention period ([3]).Within less than six months, which is extremely fast for a legislative procedure involving the two co-legislators, Directive 2006/24 ('the Data Retention Directive') was adopted ([4]). The proposed Framework Decision never saw the light.

([1]) See judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Seitlinger and others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 27. The notion of 'metadata' refers to data *about* the communication, it excludes the content of the communication. So, it refers to information about who, when, where (location data) and how (with which device) communication was made.

([2]) Council of the EU, Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism, 7833/05, 14 April 2005.

([3]) The proposed Data Retention Directive (COM(2005) 438 final, Article 7) introduced a maximum retention period of one year (in the final directive it was extended to two years). The draft Framework Decision (Article 4(2)) allowed for a retention period of up to 4 years.

([4]) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54.

Immediately after its adoption, the Data Retention Directive was brought before the EU Court of Justice ('CJEU') for annulment ([5]). Although one would perhaps expect this was done for reasons of incompatibility with the rights to privacy and data protection, that was not the case. The action for annulment was instigated by Ireland that had preferred the adoption of the Framework Decision. Ireland, supported by the Slovak Republic, considered that the Data Retention Directive had a wrongful legal basis in the basic treaties. Instead of the first pillar legal basis (internal market), Ireland argued it should have been based on the third pillar legal basis (police and judicial cooperation). Early 2009, the CJEU dismissed the action for annulment, considering that the Data Retention Directive did not contain any substantive rules on access and use of the retained data by competent authorities, and only concerned the harmonisation of the obligations put on telecom operators. Therefore, it was correctly based on the first pillar legal basis for the establishment of the internal market. As we will see, the absence of such rules was precisely why, only five years later, the CJEU declared the Directive invalid after all. The game changer for the CJEU in that respect most likely was the entry into force of the Lisbon Treaty later in 2009, which abolished the pillar structure, included a new self-standing legal basis for the adoption of data protection rules and put the Charter of Fundamental Rights at the same level as the two founding treaties.

After having survived its first legal attack, the Data Retention Directive could continue to have its effects within the EU. As a directive, it had to be transposed into Member States' law. However, not all Member States were able to do so in time, or even at all. In some Member States, this was due to objections in national parliaments as to the intrusive nature of the measure regarding the fundamental rights of citizens ([6]). The lack of transposition led to several infringement procedures instigated by the European Commission, with one Member State, Sweden, finally being ordered by the CJEU to pay a fine of 3 million Euro ([7]). But, even after proper transposition, some Member States ran into trouble because their constitutional courts declared the national law invalid for being contrary to the fundamental rights contained in the national constitution ([8]).

Against this background, the European Commission, in 2010, had to evaluate the application of the Data Retention Directive, as required by the Data Retention Directive itself ([9]).

([5]) See judgment of the Court of Justice of 10 February 2009, *Ireland/Parliament and Council*, C-301/06, ECLI:EU:C:2009:68. See on this ruling also Docksey C., 'The European Court of Justice and the Decade of Surveillance', in Hijmans, H., and Kranenborg, H.R. (eds.), *Data Protection Anno 2014: How to Restore Trust. Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014),* Intersentia, Cambridge, 2014.

([6]) See e.g. judgment of the Court of Justice of 29 July 2010, *Commission/Austria*, C-189/09, ECLI:EU:C:2010:455, in which the CJEU rejected the argument of the Austrian government that the lack of transposition could be justified by the fundamental rights concerns in the national legislative process.

([7]) See judgment of the Court of Justice of 4 February 2010, *Commission/Sweden*, C-185/09, ECLI:EU:C:2010:59.

([8]) This was the case in Germany and Romania.

([9]) See Article 14 of the Data Retention Directive.

3. The EDPS: one of the main critics of the Data Retention Directive

During a conference organised by the European Commission in December 2010, as part of preparing the evaluation report, the EDPS (at the time: Peter Hustinx) called the evaluation the 'moment of truth' for the Data Retention Directive. The EDPS stated that he considered the Directive '*the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects*' ([10]).

With this statement, which later resonated in the doctrinal and public debates about the matter, the pressure mounted on the European Commission to use the evaluation to also establish whether the necessity of the instrument of data retention as provided for by the Directive had been proven in practice. The inclusion of that assessment in the evaluation was not self-evident, since the Data Retention Directive did not explicitly require such assessment, despite the fact that the EDPS had insisted on including it in its opinion on the proposal for the Directive in 2005 ([11]). With his speech, the EDPS still achieved the desired result.

In its report, the European Commission stated that the evaluation had demonstrated that data retention was 'a valuable tool' for criminal justice systems and for law enforcement in the EU ([12]). However, the European Commission also concluded that there was still a lack of harmonisation and announced amendments to the Directive. These amendments were to follow an impact assessment, which, according to the European Commission, would provide an opportunity to assess data retention in the EU against the tests of necessity and proportionality.

Despite the attempt of the Commission to reassure the critics of the Data Retention Directive and to move the debate on necessity and proportionality to the future, the EDPS was firm in his opinion on the evaluation report ([13]). The EDPS concluded that the necessity of data retention as provided for in the Data Retention Directive had not been sufficiently demonstrated ([14]). He called upon the European Commission to consider the repeal of the Directive ([15]). With these statements, the EDPS followed-up on his opinion from 2005 on the proposal for the Directive, in which he had already expressed doubts as to the necessity and

([10]) EDPS Speech on the "moment of truth" for the Data Retention Directive: EDPS demands clear evidence of necessity, 3 December 2010.

([11]) See EDPS Opinion on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services, issued on 26 September 2005, paragraphs 72-77.

([12]) See Report from the Commission of 18 April 2011 to the Council and the European Union on the evaluation of the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, p. 1.

([13]) See EDPS Opinion on the Evaluation Report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), issued on 31 May 2011.

([14]) *Ibid*, paragraph 85.

([15]) *Ibid*, paragraph 86.

proportionality of the data retention measure and had stated that it had to be demonstrated 'in its full extent' ([16]). The European Commission did not answer the call for repeal of the EDPS, which meant the Directive remained in place.

4. The CJEU invalidates the Data Retention Directive after all

Meanwhile, in a case instigated before an Irish court by the NGO Digital Rights Ireland, as well as in a case brought by 11 130 applicants before an Austrian court, questions were raised about the validity of the Data Retention Directive. Since only the CJEU can decide on the validity of Union acts, the questions were referred to the CJEU, who joined the two cases. It led to the seminal *Digital Rights Ireland* ruling in 2014 in which the CJEU declared the Data Retention Directive invalid ([17]). According to the CJEU, the Directive exceeded the limits imposed by the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter ([18]). Although not mentioned in the ruling, the EDPS attended the hearing in the case, upon the invitation of the CJEU. In its statements ([19]), the EDPS had repeated that the Data Retention Directive did not comply with the requirements stemming from the Charter.

The CJEU considered the interference with the rights laid down in Articles 7 and 8 of the Charter 'particularly serious' ([20]). Although the essence of both rights (see the requirements of Article 52(1) of the Charter) was not affected by the measure, and the fight against serious crime, according to the CJEU, constituted an objective of general interest, the measure did not meet the requirement of proportionality. Ironically, the CJEU, like the European Commission in its evaluation report of 2011, refers to data retention as 'a valuable tool' for law enforcement ([21]). However, that remark is made in the context of assessing the suitability of the measure, before the CJEU in fact turned to assessing the (strict) necessity of the measure.

([16]) See EDPS Opinion on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services, issued on 26 September 2005, paragraph 75.

([17]) *Digital Rights Ireland and Seitlinger and others*, see footnote 1.

([18]) *Digital Rights Ireland and Seitlinger and others*, see footnote 1, paragraph 69.

([19]) EDPS pleading at the hearing of the Court in Joined Cases C-239/12 and C-594/12 (Digital Rights and Others), 9 July 2013.

([20]) *Digital Rights Ireland and Seitlinger and others*, see footnote 1, paragraph 37.

([21]) *Digital Rights Ireland and Seitlinger and others*, see footnote 1, paragraph 43.

As regards the necessity, the CJEU took issue with the generalised and indiscriminate nature of the measure, and the lack of a link between the data retained and the objective pursued ([22]). Moreover, the CJEU denounced the general absence of limits and conditions for the access of the competent national authorities to the retained data[23]. Indeed, what saved the Data Retention Directive from being annulled right after its adoption (see above) still led to its invalidation in 2016. As to the procedural conditions for access, the CJEU underlined, in particular, the requirement of prior review carried out by a court or by an independent administrative authority ([24]).

The ruling meant the end of the Data Retention Directive, but not the end of the story. On the contrary. Member States were obviously no longer obliged to have a data retention measure in place, and the fine for Sweden was refunded. However, there were still several Member States that kept their transposition laws on data retention in place.

At this point, it is important to know that the Data Retention Directive in fact harmonised the possibility for Member States, provided by Article 15(1) of the e-Privacy Directive ([25]), to adopt legislative measures to restrict the scope of certain of the provisions of the e-Privacy Directive. Before the Data Retention Directive was adopted, this provision constituted the basis for data retention measures that were in place in several EU Member States. With the invalidation of the Data Retention Directive, the possibility of having national data retention measures in place on the basis of Article 15(1) of the e-Privacy Directive revived. However, these national measures still had to meet the requirements laid down in Article 15(1), which resemble those laid down in Article 52(1) of the Charter. Since the CJEU had based itself on Articles 7, 8 and 52(1) of the Charter when invalidating the Data Retention Directive in *Digital Rights Ireland*, the question quickly rose as to whether the consideration of the CJEU, in particular on the conditions for access by competent authorities to the retained data, were also applicable to the national measures on data retention still in place.

([22]) *Digital Rights Ireland and Seitlinger and others*, see footnote 171, paragraphs 57 to 59, although the phrase 'generalised and indiscriminate' is used only in later rulings.

([23]) *Digital Rights Ireland and Seitlinger and others*, see footnote 1, paragraphs 60 to 62.

([24]) *Digital Rights Ireland and Seitlinger and others*, see footnote 1, paragraph 62.

([25]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, p. 11.

5. The CJEU sets out conditions for national data retention measures (I)

In its ruling in *Tele2 Sverige*, the CJEU answered the above question positively: also Member State legislation on data retention must meet the substantive and procedural requirements as set out in the *Digital Rights Ireland* ruling. This followed from Article 15(1) of the e-Privacy Directive read in the light of the Charter. The CJEU actually spelled out these requirements in greater detail ([26]). However, the ruling was more controversial, at least from the Member States' law enforcement perspective, on three other points.

First, the CJEU clarified the relation between the exclusion of law enforcement activities from the scope of the e-Privacy Directive in Article 1(3) and the possibility to restrict certain rights and obligations of the Directive for the same purpose of law enforcement under Article 15(1). EU Member States had argued that data retention measures, even put on telecom providers, since it was for the purpose of law enforcement, did not fall within the scope of the e-Privacy Directive. The CJEU decided differently, since such an approach would make Article 15(1) redundant. Therefore, once a national measure requires the processing of personal data by providers, it falls within the scope of the e-Privacy Directive and must, when it restricts rights and obligations in the Directive, fulfil the conditions of Article 15(1). In its later ruling in *La Quadrature du Net*, the CJEU applied the same logic to activities for national security purposes: only measures, which are directly implemented by national security authorities, so without imposing processing obligations on providers, fall outside the scope of the Directive ([27]).

Second, the CJEU considered that, given the particularly serious interference in the fundamental rights of subscribers when metadata is retained which allows for a profile to be established of the individual concerned, can only be justified by the objective of fighting 'serious crime' ([28]). The notion of 'serious crime' occurred in the Data Retention Directive, but cannot be found in Article 15(1) of the e-Privacy Directive. Therefore, in the context of data retention, this notion has its basis purely in the case law of the CJEU.

Third, and this is perhaps the most debated element of the ruling: the CJEU closed the debate on whether retention of the personal data and access to the retained data should be assessed on compliance with the requirements of Article 15(1) of the e-Privacy Directive, separately or jointly. In other words: in order to assess the lawfulness of a retention obligation, should one also take

([26]) Judgment of the Court of Justice of 21 December 2016, *Tele2 Sverige and others*, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 115 and further.

([27]) Judgment of the Court of Justice of 6 October 2020, *La Quadrature du Net and others*, Joined Cases C-511, 512 & 520/18, ECLI:EU:C:2020:791, paragraph 103. See also judgment of the Court of Justice of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790.

([28]) *Tele2 Sverige*, see footnote 26, paragraphs 100 to 102.

into account how access is organised (a 'holistic' approach), or should one first assess whether retention in itself is lawful, before turning to the rules on access (a 'staged' approach). In the *Digital Rights Ireland* ruling it was not entirely clear whether, according to the CJEU, generalised and indiscriminate retention was, as such, excluded under Union law, or whether it could still be justified, provided there were strict rules on access in place. The latter would only work, if one would follow the holistic approach.

The main argument for defending a holistic approach was that it is only at the moment of access that the seriousness of the interference materialises. Retained data can *allow* establishing a profile, which would be a serious interference with the rights of individuals, but if the rules on access in fact prohibit authorities from doing so, such interference will (or at least: should) not materialise. One would perhaps think the holistic approach was only put forward by the Member States, who mostly took a law enforcement perspective. However, in the *Tele2 Sverige* case, the European Commission argued in favour of such an approach, which was followed by the Advocate-General ([29]). And perhaps more surprising, in later cases, also the EDPS took this approach (see below). Be that as it may, the CJEU clearly choose for a staged approach, since, as clarified more clearly by the CJEU in later case law: '*the mere retention of such data … entails a risk of abuse and unlawful access*' ([30]).

The CJEU took the staged approach and concluded that generalised and indiscriminate retention as such was not acceptable under Union law. In an attempt to be constructive, the CJEU continued with explaining what *could* be acceptable, namely so-called 'targeted' retention, which implies that there is a connection between the data to be retained and the objective pursued ([31]). As regard the public and the situations that may potentially be affected, according to the CJEU, the national measure must be based on '*objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offence, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security*' ([32]).

Many EU Member States were displeased with the ruling in *Tele2 Sverige*. One of the main points of criticism was that the alternative measure of 'targeted' retention as a preventive measure did not work in practice, and that the limitation to the fight against serious crime was too strict. New preliminary rulings reached the CJEU, in some cases openly asking the CJEU to reconsider its case law, leading to heated debates in the Court room.

([29]) *Tele2 Sverige*, see footnote 26, paragraph 66 and Opinion of Advocate General Saugmandsgaard Øe of 19 July 2016, *Tele2 Sverige*, ECLI:EU:C:572, point 192 and further.

([30]) *La Quadrature du Net and others*, see footnote 27, paragraph 119.

([31]) *Tele2 Sverige*, see footnote 26, paragraphs 108 to110.

([32]) *Tele2 Sverige*, see footnote 26, paragraph 111.

6. The CJEU sets out conditions for national data retention measures (II)

A French and two Belgian preliminary references were joined in the case known as *La Quadrature du Net* ([33]). No less than fifteen Member States, as well as Norway, submitted their views. Main points of discussion were whether the assessment of the generalised and indiscriminate retention in *Tele2 Sverige* would be different if the objective pursued would constitute safeguarding national security, and whether such retention should still not be allowed for certain purposes of law enforcement. As for the latter, during at times a grim hearing, the Member States tried to convince the CJEU about the necessity of having such a retention measure in place by providing examples of successful prosecutions of serious crimes in which the retained information constituted the crucial evidence.

In a very rich ruling, the CJEU, after considering that the e-Privacy Directive also applies to measures requiring processing by telecom providers for national security purposes (see above), recalled the basic requirement that '*the retention of personal data must always meet objective criteria which establish a connection between the data to be retained and the objective pursued*' ([34]). The CJEU subsequently considered that a generalised and indiscriminate retention measure could be allowed for the purpose of safeguarding national security, due to the importance of the objective. However, such a retention measure may be ordered only for a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat, which is shown to be '*genuine and present* or f*oreseeable*' ([35]). The existence of such a threat, according to the CJEU, is in itself capable of establishing the connection between the data and the objective pursued ([36]).

Although this could be seen as a victory for the Member States that wanted to have the measure of generalised and indiscriminate data retention at their disposal, it is limited to the objective of safeguarding national security. Despite the almost unifocal position of the fifteen Member States, and the examples put forward, the CJEU did not change its position taken in *Tele2 Sverige* as regards retention measures for law enforcement purposes. The CJEU repeated that generalised and discriminate retention of metadata is not acceptable for the purposes of law enforcement and that only targeted retention for the purpose of fighting serious crime could pass the test ([37]). Remarkably, the

([33]) *La Quadrature du Net and others*, see footnote 27.

([34]) *La Quadrature du Net and others*, see footnote 27, paragraph 133.

([35]) *La Quadrature du Net and others*, see footnote 27, paragraph 137.

([36]) The CJEU formulated some further conditions, *La Quadrature du Net and others*, see footnote 27, paragraphs 138 to 139.

([37]) *La Quadrature du Net and others*, see footnote 27, paragraphs 141 and 146.

EDPS, who was again invited to the hearing, urged the CJEU to adopt a 'holistic' approach instead of the 'staged' approach, as explained above ([38]). However, it did not convince the CJEU.

Although the CJEU did not revise *Tele2 Sverige*, the *La Quadrature du Net* ruling contained some more explanation on how the CJEU considers *targeted* retention could be achieved ([39]). Moreover, the CJEU addressed several more specific or alternative retention measures. The CJEU considered that generalised and indiscriminate retention of IP addresses relating to the source of communication for fighting serious crime could be allowed, subject to strict conditions and safeguards. The CJEU considered it justified because for crimes committed online, the IP address is often the only means of investigation ([40]). The generalised and indiscriminate retention of the civil identity of users could also be allowed. Due to the limited nature of the interference, such data could, according to the CJEU, also be retained for fighting crimes that are not qualified as serious ([41]). The CJEU furthermore looked at the measure of 'expedited retention', which is the possibility of a competent authority to order providers to undertake the expedited retention of traffic and location data at their disposal for a specified period of time. Such a measure can be allowed for the fight against serious crime, according to the CJEU, and does not need to be limited to the data of persons specifically suspected of having committed a criminal offence. It may also be extended to data relating to persons other than those who are suspected, provided that that data can shed light on such an offence ([42]).

The measure of expedited retention, also known as 'quick freeze' or 'quick freeze plus', has always played a role in the debates around generalised and indiscriminate data retention. It was brought forward by opponents of generalised and indiscriminate retention as an alternative, less intrusive measure. However, the law enforcement sector did not consider it a proper alternative, as it does not guarantee the availability of data pre-emptively. In its opinion on the European Commission's evaluation report on the Data Retention Directive, the EDPS expressed its disappointment about the commitment of the Commission to examine whether quick freeze could complement data retention instead of replacing it ([43]).

([38]) EDPS Pleading at the joint hearing of the Court in Case C-623/17 (Privacy International) with Joined Cases C-511/18 and C-512/18 (La Quadrature du Net and Others) and Case C-520/18 (Ordre des barreauxfrancophones et germanophone and Others), 9-10 September 2019.

([39]) *La Quadrature du Net and others*, see footnote 27, paragraphs 148 to 150.

([40]) *La Quadrature du Net and others*, see footnote 27, paragraph 154.

([41]) *La Quadrature du Net and others*, see footnote 27, paragraph 157.

([42]) *La Quadrature du Net and others*, see footnote 27, paragraph 165.

([43]) EDPS Opinion on the Evaluation Report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), issued on 31 May 2011, paragraph 57.

7. The CJEU sets out conditions for national data retention measures (III)

In *La Quadrature du Net*, the CJEU built on its ruling in *Tele2 Sverige* and explained in quite great detail what the Member States could still do in terms of data retention. However, in the absence of a dramatic change of position of the CJEU, many Member States were still not satisfied. The dissatisfaction led to yet another round before the CJEU, with many of the same actors (including the EDPS) saying many of the same things.

This time, an Irish reference and two German preliminary references reached the Court ([44]). The Irish case (*G.D.*) was a rather hopeless attempt to try to convince the CJEU again to revise its position. The German cases (*SpaceNet*) offered a bit more prospect for the Member States. At issue in the latter cases was a German measure of generalised and indiscriminate retention, but for a very limited period of time (4 and 10 weeks) and limited to the purpose of fighting *particularly serious* crimes. The question was whether those two elements, which lead to a more restrictive retention measure than the one at issue in the previous cases, could perhaps convince the CJEU to allow this form of retention, even though it was not 'targeted'. It did not.

One would think that the matter would be settled after the rulings of the CJEU in *Digital Rights Ireland*, *Tele2 Sverige*, *La Quadrature du Net*, *G.D.* and *SpaceNet* (all decided in Grand Chamber). The opposite is true. Although the fundamental debate about whether or not generalised retention of telecom data for law enforcement purposes is allowed, might have been settled (for the time being, see below), there appeared to be still enough left to discuss about. This concerned specific elements of the previous rulings, or the implications of these rulings for retention measures in other contexts, for example with regard to banking data([45]).

And, as a matter of fact, there is still one major ruling in the making in which one element of the *La Quadrature du Net* ruling is contested ([46]). The case concerns the French Hadopi law, which put in place measures to counter intellectual property right infringements. One of the questions at issue is whether it should be possible to use the IP address relating to the source of communications for crimes which are committed online and for which the IP address is the only means to start an investigation, but which do not qualify as 'serious', as the CJEU required in *La Quadrature du Net*. After AG Szpunar

([44]) Judgment of the Court of Justice of 5 April 2022, *Commissioner of An Garda Síochána*, C-140/20, ECLI:EU:C:2022:258 and judgment of the Court of Justice of 20 September 2022, *SpaceNet*, Joined Cases C-793/19 and C-794/19, ECLI:EU:C:2022:702.

([45]) See, amongst others, judgment of the Court of Justice of 2 March 2021, *Prokuratuur*, C-746/18, ECLI:EU:C:2021:152, judgment of 22 September 2022, *VD*, Joined Cases C-339/20 and C-397/20, ECLI:EU:C:2022:703, judgment of 16 February 2023, *HYA*, C-349/21, ECLI:EU:C:2023:102, and judgment of the Court of Justice of 7 September 2023, *A.G.*, C-162/22, ECLI:EU:C:2023:631.

([46]) See pending Case *La Quadrature du Net (II)*, C-470/21.

suggested a 'readjustment' of the *La Quadrature du Net* ruling to that effect, the oral procedure was reopened, and the case was transferred from the Grand Chamber to the full Court ([47]). In his second opinion in the case, the AG underlined that, if his approach would be followed, it would not be a matter of 'reconsidering' the CJEU's case law, but of accepting a 'more nuanced solution' in very limited circumstances ([48]).

8. A look at the future

In January 2017, the European Commission adopted a proposal for an e-Privacy Regulation, replacing the current e-Privacy Directive, which has to be aligned with the GDPR ([49]). At the moment of writing, the co-legislators were still discussing the proposal, without much prospect of an agreement in the near future. The issue of data retention, albeit certainly not the only one, is a matter, which causes difficulties in the legislative process.

The European Commission proposal takes a neutral approach on the issue of data retention in the sense that it does not bring about any substantive changes to the current setup in the e-Privacy Directive ([50]). In his opinion on the proposal, the EDPS did not have many comments on the subject matter. He underlined that EU Member States have to respect the case law of the CJEU on data retention ([51]).

However, the proposal offered several EU Member States the possibility to provide a legislative reaction to the case law of the CJEU. In the General Approach of the Council, which was adopted only in February 2021, *all* activities for the purpose of safeguarding national security were excluded from the scope of the new Regulation ([52]). In addition, the objective of safeguarding national security was removed from the provision that allows for the restriction of certain rights and obligations (the equivalent to Article 15(1) e-Privacy Directive). In particular, the latter change would take away an important element in the CJEU's reasoning in *La Quadrature de Net* when it considered that Article 15(1) would be redundant if national measures that regulate the activities of private entities for national security purposes would fall outside the scope of the e-Privacy Directive (see above). With these proposed changes, *any* activity for the purpose of safeguarding national security would fall outside the scope of the new e-Privacy Regulation.

([47]) See Opinion of Advocate General Szpunar of 27 October 2022, *La Quadrature du Net (II)*, C-470/21, ECLI:EU:C:2022:838, point 82. See also EDPS Pleading at the hearing of the Court in case C-470/21 (La Quadrature du Net e.a.), 14 May 2023.

([48]) See Opinion of Advocate General Szpunar of 28 September 2023, *La Quadrature du Net (II)*, C-470/21, ECLI:EU:C:2023:711, point 88.

([49]) COM(2017) 10 final.

([50]) In essence, the new Article 11 takes the same approach as Article 15(1) of the e-Privacy Directive.

([51]) See EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), issued on 24 April 2017, p. 21-22.

([52]) See the Council Mandate of 10 February 2021 for negotiations with the European Parliament.

In doing so, Member States hope that the CJEU would no longer be able to express itself on national security measures. However, it is unlikely the European Parliament will accept this approach ([53]). In any event, it is questionable whether the Member States would actually achieve their purpose with these changes. If the measure falls outside the scope of the e-Privacy Regulation, it still falls under the GDPR, which does not exclude the objective of national security from the restriction clause (see Article 23 GDPR) ([54]). Article 23 GDPR must necessarily also be interpreted in the light of the Charter, which will lead to similar considerations. In fact, in *La Quadrature du Net*, the CJEU already applied its considerations under the e-Privacy Directive *mutatis mutandis* to its assessment under the GDPR ([55]).

Another attempt by the EU Member States to change the legislative framework on which the CJEU based its data retention rulings, is to include a positive ground for processing of metadata in the e-Privacy Regulation, instead of allowing a retention measure only as a restriction of rights and obligations ([56]). The change intends to react to the CJEU's consideration that with a measure of generalised and indiscriminate retention, the exception becomes the rule ([57]). Again, it is questionable whether the EU Member States will achieve what they intend; also a positive ground for processing must comply with the requirements of Article 52(1) of the Charter. See in that respect the CJEU's case law on national laws that form the basis of processing within the meaning of Article 6(1)(c) and (e), and Article 6(3) of the GDPR. Article 6(3), which requires such a law to be proportionate to the legitimate aim pursued, is *'an expression of the requirements arising from Article 52(1) of the Charter'*, according to the CJEU ([58]).

([53]) The European Parliament does not propose any substantive amendments on this point as regards the Commission proposal, see Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 20 October 2017.

([54]) See to that effect also the EDPB Statement 03/2021 on the ePrivacy Regulation, adopted on 9 March 2021, p. 1-2.

([55]) *La Quadrature du Net and others*, see footnote 27, paragraphs 208 to 211.

([56]) See Article 7(4) of the Council Mandate, op. cit. (footnote 52).

([57]) *Tele2 Sverige*, see footnote 26, paragraph 89.

([58]) See judgement of the Court of Justice of 1 August 2022, *O.T.*, C-184/20, ECLI:EU:C:2022:601, paragraph 69.

9. Conclusion

The two decades during which the issue of data retention has been discussed shows the difficulty and sensitivity of the debate on how to achieve a proper balance between privacy and security in the modern digital society. The CJEU took a firm stance in the debate, causing uproar in the Member States. Despite the fierce criticism from the law enforcement side, the CJEU stood by its position, thereby acknowledging the importance and great value of the Charter of Fundamental Rights.

The EDPS, who had just been established in 2005, has from the outset been one of the strongest critics of the Data Retention Directive. The EDPS made an important contribution to the debates which eventually led to the invalidation of the Directive in *Digital Rights Ireland*. Also after the ruling, the EDPS continued to express a critical view on the matter, in particular during the hearings for the Court of Justice for which he was invited multiple times and in which national measures of data retention were debated.

Although surely critical, when looking at his interventions, one can also see how the EDPS tried to convince the CJEU to depart from its rather dogmatic approach when disqualifying generalised and indiscriminate retention as such and move towards a more holistic approach. So far, it has not convinced the CJEU. However, since the story is never ending, the digital society is continuously changing, and the matter is known for its unexpected bends and turns, one may never know. In any event, it is clear that the EDPS will continue to follow the matter closely and make its always valuable contribution.

07

International data transfers and the EDPS: current accomplishments and future challenges

Dr. Christopher Kuner

International data transfers and the EDPS: current accomplishments and future challenges

Dr. Christopher Kuner (*)

Regulation of international data transfers is one of the main vehicles through which EU data protection law interacts with and influences data processing outside EU borders. Since beginning its work 20 years ago, the EDPS has made a significant contribution to the development, application, and interpretation of data transfer regulation. It will continue to play an important role as the EU faces growing challenges to protect data transfers in coming years.

1. Introduction

Regulating transfers of personal data outside EU borders is one of the main ways that European Union ('EU') data protection law interacts with and influences data processing in the wider world. For example, third countries emulate EU data transfer regulation in their own laws; data controllers, EU bodies, and data protection authorities ('DPAs') evaluate the protection provided by foreign law when data are transferred; and companies in third countries implement EU standards in processing data transferred to them ([1]).

(*) Affiliated Professor of Data Protection Law, University of Copenhagen; Associate, Centre for European Legal Studies, University of Cambridge; Visiting Fellow, European Centre on Privacy and Cybersecurity, Maastricht University; Co-editor, *The EU General Data Protection Regulation: A Commentary* (Oxford University Press); Member, European Commission Multistakeholder Expert Group on the GDPR; Senior Privacy Counsel, Wilson Sonsini Goodrich & Rosati, Brussels. The author is grateful to Joanna Jużak for her excellent research assistance.

([1]) Regarding the global influence of EU data protection law, see Bradford, A., *The Brussels Effect*, ed. Oxford University Press, New York, 2020, p. 131-156 (Kindle edition); Kuner, C., 'The Internet and the Global Reach of EU Law', *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, ed. by Cremona, M., and Scott, J. Oxford University Press, Oxford, 2019, p. 112-145.

The European Data Protection Supervisor ('EDPS') has made an important contribution to developing, applying, and interpreting EU data transfer regulation. As an independent data protection authority ('DPA') and a member of the European Data Protection Board ('EDPB'), it enforces data protection law with respect to the EU institutions, intervenes in cases before the Court of Justice of the EU ('CJEU'), produces guidance, and furthers international cooperation. Much of this work has involved international data transfers.

As risks for data transfers increase, EU data transfer regulation faces growing challenges to ensure its continued relevance. This will require the EU to address important strategic issues and pressing legal questions, in which the EDPS can play an important role.

2. Compliance, enforcement, and investigation

The tasks of the EDPS are enumerated in Regulation (EU) 2018/1725 (the 'EUDPR') that established it ([2]). The EDPS is responsible for monitoring and enforcing application of the EUDPR by EU institutions, bodies, offices, and agencies ([3]), including compliance with the rules on international transfers of personal data ([4]).

The EUDPR also grants the EDPS specific powers with regard to data transfers by the EU institutions, such as adopting its own standard data protection clauses ([5]); authorising the use of appropriate safeguards, such as legally binding instruments between public authorities and standard data protection clauses adopted by the European Commission (the 'Commission') or the EDPS ([6]); receiving information from EU institutions and bodies about data transfers based on appropriate safeguards or derogations ([7]); and cooperating with the Commission and the EDPB to further international cooperation in the protection of personal data ([8]). In order to carry out these tasks, the EDPS may order the suspension of data transfers from an EU institution to a recipient in a third country or to an international organisation ([9]).

([2]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39 (referred to as the 'EUDPR').

([3]) Article 57(1)(a) EUDPR.

([4]) Chapter V EUDPR.

([5]) Article 48(2)(c) and Article 58(3)(d) EUDPR.

([6]) Article 48(3) and Article 58(3)(e-f) EUDPR.

([7]) Article 48(5) and Article 50(6) EUDPR.

([8]) Article 51 EUDPR.

([9]) Article 58(2)(j) EUDPR.

The EDPS also plays a leading role in work on data transfers done by the EDPB under the EU General Data Protection Regulation (the 'GDPR') ([10]). This includes issuing guidelines, recommendations, and best practices ([11]), and opining on proposed Commission adequacy decisions ([12]), among other things.

The EDPS has issued many decisions concerning data transfers ([13]), which have often involved situations and technologies that are relevant outside the context of the EU institutions. For example, in 2020 it investigated the institutions' use of Microsoft products and services, and found a number of areas of non-compliance, including a lack of control over the location of data processing and what data were transferred out of the European Economic Area ('EEA') ([14]). In addition, in 2022 the EDPS reprimanded the European Parliament (the Parliament) for the use of Google Analytics that resulted in improper transfers of personal data to the US ([15]).

3. Interventions before the CJEU

3.1. Introduction

Intervention in cases before the CJEU is an important way by which the EDPS becomes involved in issues concerning international data transfers. Thus far there have been four cases in which the CJEU interpreted the EU rules on international transfers ([16]). The first such case was *Lindqvist* ([17]), decided in 2003 under the EU Data Protection Directive 95/46/EC (the 'Directive 95/46/EC', which was the predecessor of the GDPR) ([18]), in which the CJEU found that placing material on a server located in the EU that was accessible worldwide via the internet did not constitute an international data transfer. As the EDPS

([10]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1 (referred to as the 'GDPR'), Article 68(3).

([11]) See, e.g., Article 70(1)(i) and Article 70(1)(j) GDPR.

([12]) Article 70(1)(s) GDPR.

([13]) EDPS, Authorisation Decisions for Transfer.

([14]) EDPS, Public Paper on the Outcome of own-initiative investigations into EU institutions' use of Microsoft products and services, issued on 2 July 2020.

([15]) EDPS, Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament, issued on 5 January 2022.

([16]) Other judgments of the CJEU have involved situations where personal data were being transferred internationally, but they did not result in the Court interpreting EU rules on data transfers, and are not discussed here.

([17]) Judgment of the Court of Justice of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

([18]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31 (no longer in force) (referred to as the Directive 95/46/EC).

only began operations in 2004 ([19]), it was not involved in that case. Also, in 2020 the Grand Chamber of the CJEU issued its judgment in *Facebook Ireland and Schrems*, in which it invalidated the Commission's Privacy Shield adequacy decision covering data transfers to the US because of deficiencies in the decision in light of characteristics of the US legal system ([20]); however, the EDPS did not intervene in that case.

Under Article 58(4) of the EUDPR, the EDPS has a right to intervene in *'actions brought before the CJEU'* concerning the processing of personal data. As the CJEU has decided, the right of the EDPS to intervene extends to all matters concerning the processing of personal data, not just to those where personal data has been processed by EU institutions or bodies ([21]). Based on this right, the EDPS requests leave to intervene, and the CJEU assesses the admissibility and the merits of the application and then issues an order in the relevant case to grant or decline it. Under Article 24 of its Statute ([22]), the CJEU can also invite the EDPS to intervene before it, particularly in proceedings where the EDPS cannot intervene on its own (i.e., when the proceedings are not *'actions'* brought before the CJEU). Thus, the EDPS has intervened in cases involving data transfers that go beyond data processing in the EU institutions.

In addition, other EU legislation may also allow for intervention before the CJEU by the EDPS ([23]), which has occurred on numerous occasions ([24]), though not involving data transfers. The EDPS may also refer a case to the CJEU, but has not yet done so ([25]). Decisions of the EDPS may be challenged before the CJEU ([26]), but thus far such challenges have not produced any cases dealing with data transfers.

The two data transfer cases in which the EDPS intervened before the CJEU will now be discussed.

([19]) See EDPS, Our role as a supervisor.

([20]) Judgment of the Court of Justice of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559.

([21]) Order of the Court of Justice of 17 March 2005, *Parliament/Council*, C-317/04, ECLI:EU:C:2005:189.

([22]) Protocol (No 3) on the Statute of the Court of Justice of the European Union, OJ C 202, 7.6.2016, p. 210.

([23]) See Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 11.5.2016, p. 53; Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, p. 1; Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018, p. 138.

([24]) See EDPS, Court Cases.

([25]) *Ibid.*

([26]) *Ibid.*

3.2. Case C-362/14, *Schrems*

This case involved several complaints brought against Facebook before the Irish Data Protection Commissioner, concerning, among other things, its membership in the EU–US Safe Harbour arrangement. The Safe Harbour was based on a Commission decision finding that the arrangement provided an adequate level of protection for transfers of personal data to US companies that were members of it.

In its judgment ([27]) responding to questions put to it by the Irish High Court, the Grand Chamber of the CJEU ruled that the term *'an adequate level of protection'* under Directive 95/46/EC requires a third country to ensure a level of protection of fundamental rights and freedoms essentially equivalent to that of EU law read in the light of the Charter of Fundamental Rights ('the Charter') ([28]). It noted that the Safe Harbour decision of the Commission did not contain sufficient findings explaining how the US ensures an adequate level of protection, and that under it, the applicability of the principles could be limited to meet, for example, national security, public interest or law enforcement requirements, which in effect gave US law primacy over EU fundamental rights. Moreover, the Safe Harbour decision did not contain any finding concerning limitations on the powers of public authorities (such as law enforcement authorities) in the US to interfere with fundamental rights. It found that US legislation compromised the essence of the fundamental right to respect for private life under Article 7 of the Charter and the essence of the fundamental right to effective judicial protection enshrined in Article 47 of the Charter. Thus, the Commission's Safe Harbour adequacy decision was held invalid.

The *Schrems* judgment demonstrates that the CJEU views the concept of an international data transfer in terms of requiring a high level of protection based on EU fundamental rights standards. As President of the CJEU Koen Lenaerts has stated, the judgment is also *'a landmark case'* in EU procedural law, '*because it has made clear that the preliminary reference for controlling the validity of an act of the Union is not only without limit in time… but also may be reviewed in terms of the legal framework existing at the date of the Court's judgment'* ([29]).

The EDPS was invited by the CJEU to intervene in the case ([30]). Several of the points made by the EDPS in its intervention were mentioned by the Court in its judgment. These included, in particular, the need for personal data to be subject

([27]) Judgment of the Court of Justice of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650. See Kuner, C., 'Article 46', The EU General Protection Regulation: A Commentary, Update of Selected Articles, Oxford University Press, Oxford, May 2021, p. 170-172.

([28]) Charter of Fundamental Rights of the European Union, OJ C 83, 30.3.2010, p. 389.

([29]) Lenaerts, K., 'The EU General Data Protection Regulation Five Months On', speech by CJEU President Koen Lenaerts at the 40th International Conference of Data Protection and Privacy Commissioners (25 October 2018), YouTube, between 27'07" and 30'35".

([30]) See EDPS pleading at the hearing of the Court of Justice in Case C-362/14 (Schrems v Data Protection Commissioner), 24 March 2015.

to the control of an independent DPA ([31]); the fact that supervision by a DPA is an *'essential component'* of the fundamental right to data protection ([32]); and the conclusion that the Safe Harbour did not respect the essence of the right to respect for private life under the Charter ([33]).

Schrems can be regarded as a seminal judgment for EU data protection law in general and for data transfer regulation in particular. The fact that the Court invited the EDPS to intervene and took its intervention into account in the judgment shows that the Court looks to it for guidance on data transfer issues.

3.3. Opinion 1/15

This case was initiated by the European Parliament, which sought an opinion from the CJEU on whether a proposed agreement for the processing and transfer of airline passenger name record ('PNR') data between the EU and Canada was legally valid, and in particular whether the envisaged agreement was compatible with Article 16 of the TFEU ([34]) and the Charter. Having invited the EDPS to intervene, the Grand Chamber of the CJEU in its *Opinion 1/15* ([35]) found that the draft agreement could not be concluded in its current form, as it violated the Charter and was enacted under the wrong legal basis.

The Court held that transfers of personal data may be legalised by an international agreement, which must meet the *Schrems* standard of essential equivalence with EU law. After having examined the protections provided by the Canadian legal system, it ruled that the transfer of PNR data to Canada and the rules foreseen in the draft agreement would entail an interference with the fundamental rights to respect for private life under Article 7 and the protection of personal data under Article 8 of the Charter. The Court adopted several of the arguments made by the EDPS in its intervention, such as that the processing of PNR data represented a serious interference with fundamental rights ([36]); that precision in describing data processing is important in determining whether a violation of fundamental rights exists ([37]); and that an international agreement must comply with the standards of the Charter ([38]).

([31]) EDPS pleading at the hearing of the Court of Justice in Case C-362/14, see footnote 30, p. 3, and *Schrems*, see footnote 27, paragraph 58.

([32]) EDPS pleading at the hearing of the Court of Justice in Case C-362/14, see footnote 30, p. 5, and *Schrems*, see footnote 27, paragraph 41.

([33]) EDPS pleading at the hearing of the Court of Justice in Case C-362/14, see footnote 30, p. 2, and *Schrems*, see footnote 27, paragraph 94.

([34]) Consolidated Version of the Treaty on the Functioning of the European Union (TFEU), OJ C 326, 26.10.2012, p. 47.

([35]) Opinion 1/15 of the Court of Justice of 26 July 2017, *EU-Canada PNR Agreement*, C-1/15, ECLI:EU:C:2017:592. See regarding the case, Kuner, C., 'International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15 (EU-Canada PNR)', *Common Market Law Review*, Vol. 55, No. 3, Wolters Kluwer, Leiden, 2018, p. 857-882.

([36]) See EDPS pleading at the hearing of the Court of Justice in Opinion 1/15 (*EU-Canada PNR agreement*), 5 April 2016, p. 5, and *Opinion 1/15*, see footnote 35, point 128.

([37]) EDPS pleading at the hearing of the Court of Justice in Opinion 1/15, see footnote 36, p. 6, and *Opinion 1/15*, see footnote 35, point 157.

([38]) EDPS pleading at the hearing of the Court of Justice in Opinion 1/15, see footnote 36, p. 2, and *Opinion 1/15*, see footnote 35, point 214.

Opinion 1/15 reaffirms the high standard of data protection and fundamental rights protection for international data transfers set out in *Schrems*, while extending it to data transfers based on an international agreement. It facilitates the use of international agreements for data transfers by clarifying that they may meet the requirements of being a '*law*' under the Charter, while at the same time setting strict conditions for their use.

In *Opinion 1/15* the Court once again adopted a number of the EDPS' arguments. This reaffirms the influence of its voice on data transfer issues also seen in *Schrems*.

4. Guidance

The EDPS is also tasked with promoting the awareness of Union institutions and bodies of their obligations under the EUDPR ([39]), advising them on legislative and administrative measures relating to data protection ([40]), and monitoring relevant developments having an impact on data protection ([41]). In line with these mandates, the EDPS may advise data controllers ([42]) and issue opinions on data protection topics ([43]), which it has done with regard to matters pertaining to international data transfers.

For example, the EDPB issued guidance on the implications of the CJEU's judgment in *Facebook Ireland and Schrems* mentioned earlier that invalidated the EU-US Privacy Shield ([44]), and the EDPS did the same for the EU institutions by issuing a strategy document on complying with the judgment ([45]). The EDPS document aims to ensure and monitor compliance of the EU institutions with the judgment's pronouncements concerning data transfers, and includes a plan containing both short-term and medium-term actions. These include ordering the EU institutions to map on-going contracts, procurement procedures, and other types of cooperation involving data transfers, and then report to the EDPS about them; providing guidance on data transfers to the US and other third countries; and asking EU institutions to carry out case-by-case transfer impact assessments.

([39]) Article 57(1)(c) EUDPR.
([40]) Article 57(1)(g) EUDPR.
([41]) Article 57(1)(h) EUDPR.
([42]) Article 58(3)(b) EUDPR.
([43]) Article 58(3)(c) EUDPR.
([44]) See, e.g., EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, issued on 18 June 2021, version 2.0.
([45]) EDPB Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling, issued on 29 October 2020.

5. Furthering international cooperation

The EDPS has the mandate to engage third countries and international organisations in discussions and activities to further international cooperation for the protection of personal data ([46]). The European Data Protection Supervisor has stated that he views such cooperation as a part of its strategic objective to foster '*global partnerships in the field of data protection*' ([47]).

Such cooperation is particularly important with regard to complex data transfer issues, such as how bodies set up by treaty under public international law (known as international organisations or IOs) can comply with the GDPR's requirement that both data transfers to them and onward transfers of EU data from them be conducted in compliance with it ([48]). Data transfers are particularly significant for IOs, since the nature of their work requires them to transfer personal data across borders in order to fulfil their mandates.

For several years, the EDPS has worked with IOs to facilitate their discussion of data protection and data transfer issues. Beginning in 2005, the EDPS has organized annual workshops dedicated to data protection within IOs, which aim to bring together '*International Organisations to share experiences and best practices in the field of privacy and data protection*', and allows them to '*discuss the most recent regulatory developments at international level and analyse their implications*' ([49]).

6. Conclusion

The regulation of international data transfers presents challenges that the EU will have to confront in coming years, only a few of which can be discussed here. These concern in particular the EU's institutional structure; the need to address pressing strategic and legal issues; clarifying the conditions for use of international agreements; and better defining the territorial limits of data transfer regulation.

([46]) Article 51 EUDPR.

([47]) Wiewiórowski, W., 'Working with international organisations to lead the way in data protection', *EDPS Blog*, 24 June 2019.

([48]) See Article 44 GDPR. For a full discussion of the issues concerning data transfers to and from IOs, see Kuner, C., 'International Organizations and the EU General Data Protection Regulation: Exploring the Interaction between EU Law and International Law', *International Organizations Law Review*, Vol. 16, No. 1, Brill/Nijhoff, Leiden, 2019, p. 158-191. See also EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), issued on 12 November 2019, version 2.1, p. 23.

([49]) EDPS, International Organisations Workshop on Data Protection 2023; see also further the contribution by Matter, O., 'International cooperation: an imperative at the core of EDPS activities', Chapter 13.

6.1. Institutional issues

There is a complex institutional framework for the regulation of data transfers in EU law. The Commission is responsible for proposing primary legislation, conducting international negotiations for the EU, and enacting secondary legislation (such as decisions on adequacy and approval of standard contractual clauses), which powers are subject to few institutional constraints. Taking adequacy decisions as an example, the EDPB must be consulted about them ([50]), but its opinion is non-binding, and there is no requirement for the Parliament to approve adequacy decisions. While the Council opines on delegated and implementing acts proposed by the Commission ([51]), and the Parliament can request opinions from the CJEU (as in *Option 1/15*) as well as issue political statements, neither institution has much involvement in the details of data transfer regulation. The EDPB adopts guidance and opinions and coordinates cross-border enforcement of the GDPR, but the usefulness of its work is limited by the need to seek consensus among DPAs from all 27 EU Member States, which is one reason why its action on data transfers has been criticized as slow and ineffective ([52]).

The EDPS fills the need for an entity dealing with data transfers that is independent, European in structure and outlook, and dedicated to upholding high standards of data protection. Its position allows it to stand apart from political pressures, and to take a strategic view of data transfer issues. As a single entity, it can also be nimbler in addressing data transfer issues than more heterogeneous institutions like the Commission and the EDPB. For example, probably no other EU entity could have facilitated discussions between international organisations as the EDPS has done.

The EDPS should build on its strengths to become a centre of excellence for data transfer issues. By reaching out to experts from academia, non-governmental organisations, and elsewhere beyond the EU institutional structure, it could incorporate valuable outside expertise into its work, while also contributing to greater openness in dealing with data transfer issues (see below); the past work of the EDPS advisory group on digital ethics could serve as a model in this regard ([53]).

([50]) Article 70(1)(s) GDPR.

([51]) Article 93 GDPR.

([52]) See noyb, 23 years of illegal data transfers due to inactive DPAs and new EU-US deals, 14 August 2023.

([53]) See EDPS Ethics Advisory Group, Report 2018, Towards a Digital Ethics.

6.2. Strategic issues

The EU has focused disproportionately on data transfers to US companies and law enforcement authorities, and neglected other important strategic issues, such as how EU data transferred to authoritarian and non-democratic countries can be protected ([54]). In addition, despite the Coronavirus pandemic and the migration crisis, the EU has done little to facilitate data transfers carried out for important reasons of public interest such as providing international humanitarian aid ([55]) and combatting global pandemics ([56]). The EDPS has already called for a pan-European approach to data sharing in pandemics ([57]), and its experience as a DPA responsible for supervising public institutions could help it develop initiatives to facilitate data transfers for public interest purposes.

There is also a pressing need to develop more of the legal bases for data transfers foreseen in EU law. For instance, codes of conduct and certification mechanisms ([58]) could be an effective way to protect large-scale data transfers by intrusive technologies such as artificial intelligence, but this would require that the lengthy process for their approval be shortened and that questions about their legal effect be answered.

6.3. Data transfers and international agreements

International agreements can be used as a legal basis for data transfers in either an informal or a formal sense. Informally, the Commission issues adequacy decisions covering data protection in third countries, which strictly speaking are unilateral acts of the Commission. However, in practice the Commission always holds detailed discussions with a third country before issuing an adequacy decision, resulting in an informal commitment to bring its legal standards in line with those of the EU, which can be regarded as an '*agreement in principle*' ([59]).

([54]) Data transfers to such countries were not even mentioned in the Commission's 2017 Communication on global data transfers. See Communication from the Commission to the European Parliament and the Council, Exchanging and Protection Personal Data in a Globalised World, COM(2017) 7 final.

([55]) See Brussels Privacy Hub and International Committee of the Red Cross, Handbook on Data Protection in Humanitarian Aid, ICRC Publishing, Geneva, 2020, p. 73-81.

([56]) See Docksey, C., and Kuner, C., The Coronavirus Crisis and EU Adequacy Decisions for Data Transfers, *European Law Blog*, 3 April 2020.

([57]) See, e.g., Wiewiórowski, W., EU Digital Solidarity: a call for a pan-European approach against the pandemic, 6 April 2020.

([58]) See Article 46 GDPR.

([59]) See, e.g., The White House, Remarks by President Biden and European Commission President Ursula von der Leyen in Joint Press Statement, 25 March 2022, in which von der Leyen stated that the EU and the US had reached an 'agreement in principle on a new framework for transatlantic data flows' that ultimately resulted in a new adequacy decision being issued by the Commission. Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data under the EU-US Data Privacy Framework, C/2023/4745, OJ L 231, 20.9.2023, p. 118–229.

The secretive nature of such negotiations, together with the fact that adequacy decisions are based on legal studies that are never made public, illustrates the lack of transparency surrounding much data transfer regulation.

In *Opinion 1/15*, the CJEU found that international agreements may provide a formal legal basis for data transfers, as long as they meet the requirements of the Charter. However, EU law does not specify the protections for data transfers that an international agreement should contain ([60]), which leaves many questions open. The EU institutions should work to define the standards for international data sharing agreements, which must both maintain a high level of protection and allow enough flexibility so as not to make third countries reluctant to enter into them in the first place.

6.4. Defining territorial limits

The EU institutions and the DPAs have often reacted to the growing volume of international data transfers by adopting documentation requirements of increasing complexity. Examples of this approach can be seen in EDPB guidance requiring parties to prepare data maps and impact assessments covering both data transfers ([61]) and situations when data are processed outside the EU but a data transfer is not technically deemed to occur ([62]). Attempting to compensate for the risks posed by such situations through documentation requirements cannot provide complete protection for data processed abroad, and is a poor substitute for directly addressing the question of what the territorial limits of EU data transfer regulation and EU data protection law should be.

The EU's insistence that foreign legal systems be essentially equivalent to EU law seems an example of the attitude that Weiler has criticised as '*withdrawing into one's own constitutional cocoon, isolating the international context and deciding the case exclusively by reference to internal constitutional precepts*' ([63]). That a different approach is possible, even in a member of the European legal family famed for its protection of fundamental rights, is shown by the position of the German Federal Constitutional Court, which has held that under German constitutional law, '*it is … not necessary that the receiving state have rules on the processing of personal data that are comparable to those within the German legal order …*', and that German law '*recognises and generally respects the autonomy and diversity of legal orders, including in the context of data sharing*' ([64]).

([60]) For instance, the GDPR merely states in Recital 102 that international agreements must include '*appropriate safeguards for the data subjects*'.

([61]) See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 18 June 2021, p. 3.

([62]) See EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, adopted on 12 November 2019, p. 15.

([63]) Weiler, J., 'Editorial', *Blog of the European Journal of International Law*, Vol. 19, No. 5, 13 January 2009.

([64]) BVerfG, Order of the First Senate of 20 April 2016 – 1 BvR 966/09, ECLI:DE:BVerfG:2016:rs20160420.1bvr096609, paragraph 334. The translation has been slightly corrected by the author.

The EU should also adopt a clearer and more consistent methodology for evaluating whether foreign legal standards provide protection essentially equivalent to that of EU law. Interpreting foreign law poses daunting methodological challenges ([65]), and the EU institutions and the DPAs should make better use of the lessons of comparative law to evaluate foreign data protection standards more consistently and rigorously. The fact that two Commission adequacy decisions were invalidated and a draft international agreement was found wanting by the CJEU demonstrates that the EU's current methods leave much to be desired.

It will ultimately be necessary for the EU to clarify how far international data transfers can be conditioned on the adoption by third countries of standards essentially equivalent to its own. This question exemplifies the challenges facing EU data transfer regulation in coming years, and the need for the EU institutions to work together to confront them, an effort in which the EDPS can play a crucial role.

([65]) See, e.g., Samuel, G., *An Introduction to Comparative Law Theory and Method*, Hart Publishing, Oxford and Portland, 2014 (Kindle edition).

08

Why we have the GDPR: an interview with Jan Philipp Albrecht

Jan Philipp Albrecht

Why we have the GDPR: an interview with Jan Philipp Albrecht

Jan Philipp Albrecht (*)

In an interview, Jan Philipp Albrecht looks back at the goals, challenges and achievements of the General Data Protection Regulation. He offers a first-hand account of his experience in negotiating the GDPR, as well as the role of the EDPS during the legislative process. Jan Philipp Albrecht also reflects on the relevance of the GDPR in today's digital regulatory landscape and main challenges for the future.

1. ***When you decided to become rapporteur for the GDPR, what were you hoping to achieve?***

   My main objective was to make sure that the fundamental right to data protection, which was enshrined not only in the Treaty but also in the Charter of Fundamental Rights, had a comprehensive set of rules in order to protect it.

   The Lisbon Treaty meant that the Charter of Fundamental rights became legally binding. While the 1995 Data Protection Directive was a very important cornerstone at the time, we still we had very different implementations across the Member States. We needed to ensure the fundamental right to data protection had the same level of protection across the European Union.

   The next important objective was to create a single market, a digital single market. For most companies, cross-border activities were already standard at that time. However, many of these companies struggled with very different sets of standards across Member States. This brought us to a point where the protection of a fundamental right was becoming in contradiction with the goal of achieving a single market, which was a disadvantage for companies.

(*) Member of the European Parliament 2009 –2018.

Therefore, we needed to achieve both goals at the same time and this was the reason for having a regulation instead of a directive. We had already debated this before I became rapporteur on the file: both the European Parliament and Council of the European Union had already taken a position on the initial Communication of the European Commission. In each these documents, it was already clear that there was a common objective to make this regulation happen in the best way possible.

2. ***The legislative process that led to the adoption of the GDPR was not always easy, but still you made it. How 'lucky' are we to have the GDPR we have today?***

   It was a heavy struggle. It took hard work by many people in the different Institutions and in Member States' governments to bring this across the line.

   It was also a dialogue, a process of getting everyone convinced of the need to protect the fundamental right to data protection on the one hand, but also to have a single set of rules for the Single Market on the other hand.

   In the end, we managed to pass the idea that we could be stronger in the world together as a European Union. We could be bold as Europeans and have an impact on the creation of global standards.

   I think that it was a successful result and energy well spent by many people. We still harvest the fruits of those efforts today, as we are able to pass other legislation, such as the Digital Service Act or the AI Act. I do not think those regulations would be possible at all if there had not first been this struggle on the data protection regulation.

3. ***It is well known that there was a lot of lobbying against your initial draft report – which broke a record at the time in terms of the number of amendments received. Why was this the case?***

   When you enter into a fundamentally political sphere to effectively establish a new kind of fundamental right, there is always resistance to that. It is also understandable, because it was not so clear to everyone that we needed further rules.

   Of course, many also feared regulation because we already had a number of rules, but for several reasons, these rules were never strictly enforced. They were a kind of 'paper tiger' in many respects, because they could be circumvented in different jurisdictions of the European market. Another reason was that those rules had no real sanction mechanisms. There were some fees, but it was far cheaper to pay the fees than to actually comply with the requests that came with them.

We wanted to see data protection standards enforced, even if it was not easy to do so. Many companies reacted to it and many interests groups reacted to it, perhaps because they also built their business model around these standards not being enforced.

On the other hand, were many business representatives advocating for this regulation as they saw that it was necessary to enforce these rules better. Otherwise, consumers would also lose trust in the quickly developing digital markets and new technologies.

Imagine if we would not have a strong and reliable data protection standards today: people would turn their back to technological developments such as artificial intelligence. Certain companies already realised back then and they were allies to help bring this forward, also as a chance for the European market and for European businesses to be front Runners and to have a competitive advantage in this field in the future.

At the same time, many civil rights groups were making it very clear that digitilisation needed more and better standards for the protection of privacy and other fundamental rights. Data protection standards needed to be brought forward in a better way and more modern way, given the ongoing massive surveillance as demonstrated by the Snowden revelations in 2013 (after the GDPR had already been proposed). These revelations further supported the argument that we needed to have a better regulation in order to obtain more transparency on where our data goes and for what it is used for.

4. ***How would you describe the role of the EDPS during the legislative process?***

The European Data Protection Supervisor was of course one of the first stakeholders in this whole reform debate. We had already received inputs and advice from the EDPS before the regulation was proposed, by having exchanges on the needs for reform and on the different legal acts in place. Because it was a complex field of regulation where we had different sets of rules on privacy-related matters, and in some of the places, we still have these very different sets of rules. The EDPS was very important for us also as European Parliament to support us in approaching a more unified framework for data protection. It helped bringing forward the right ideas for modernising these different sets of rules.

During the legislative process, the EDPS was also a constant guest in our meetings of the rapporteurs and shadow rapporteurs and of the working groups we had on different subjects. The EDPS was the main point of reference for expertise at the European level, even more as we did not have the European Data Protection Board at the time.

I am very thankful for the role of the EDPS in promoting coherence and consistency in Europe, also between the data protection authorities. I would like to explicitly thank Peter Hustinx and Giovanni Buttarelli, who really did a tremendous effort to clear the ground for this new era, where we have the European Data Protection Board which brings together all the data protection authorities. They did it also by stepping a little bit over their mandate of looking at the EU institutions, by really looking at Europe as a whole. By doing that, they really helped to create this new framework.

5. ***During the negotiations, many lobbyists referred to "big data", arguing that this technology was at odds with the basic principles of data protection. Do you think that the GDPR's approach is still relevant in today's age of artificial intelligence?***

   It is really important to understand that data protection and the fundamental right to data protection is both technologically neutral and principle based. We have basic principles, developed since the '60s and '70s; that no personal should data used without a clear purpose and the processing should always limited to that purpose. There should be transparency about what the purpose is and which data categories are processes, so the logic behind the processing needs to be transparent. Finally, there should be accountability, because data protection is not something which you can just outsource, you need to incorporate it into your own behaviour.

   All these principles confirm that what matters is the protection of the humans involved, not the protection of the data. Data security is an important part, but in the end, it is about the protection of the human involved and human self-determination. If in the end we do not know which personal data about us are being processed, we have no idea on what consequences personal behaviour could have. This concern also stems from our experiences with autocratic regimes for example. It is always important to understand these principles and the history behind them and how they apply new technologies.

   Data protection and also the GDPR do not really impose a specific way to do things. Some of the criticism which came up during the negotiation were that the regulation is too detailed or everything is complicated. It is not! In the end, it is very simple, principle-based regulation, but you need to take some time to understand it and then apply it to new technologies.

6. ***The GDPR is a landmark piece of EU legislation, something to be proud of. Looking back, however, is there anything you regret in terms of the agreed text? Or something you would now do differently?***

   It was obvious from the beginning that there will be many things which would still require further review or even change in the future. For example, those fields which are not addressed by the GDPR, such as the ePrivacy

Directive, which is still not replaced by an own regulation (which is really a pity). I really think that it would be better to incorporate the standards for telecommunications devices and networks into the framework of the data protection regulation in some form.

In addition, there are areas such as health, social security and employment which were not fully regulated by the GDPR. In addition, even in the police and judicial field, we can see that there could be more coherence on the way in which we apply data protection principles. Coming back to that basic architecture of different data protection laws, it would be better if we could get more integration in this area – not only European integration but also substantive integration of these different legal acts. That is also important because for citizens and also for companies it is sometimes hard to understand why there are so many different rules and in some areas also very different Member State rules.

On substance, I also think that there are important points which need to be looked at. We had the aim of making it easier for people to understand the information about how their personal data are being processed. This information is still very often written by lawyers for lawyers, and you need stakeholder and interest groups to make sure that all people are able to understand the rules and act our rights. It would be better for everyone if this could be also somehow be 'pinned down' using easy understandable symbols.

For example, when we are on the street in the traffic, we have traffic signs. Everyone can understand those signs. Of course everybody needs to learn about those signs and what they mean, but it is easily understandable. Why can't we have that also in the digital environment of our lives today, where everything and every moment is somehow digital? I think that the use of symbols has a big potential going forward, in particular with regards to new technologies based on automated processing.

7. What are your thoughts about the GDPR's 'one-stop shop' enforcement model?

One of the biggest achievements of the GDPR is to have a unified application of data protection rules across the European market. Not just in the legal formulation of the rules, but also in the interpretation by data protection authorities.

With the European Data Protection Board (which convenes the different data protection authorities), we have the tools to get coherence, to get common interpretations, to also even get common measures, and to reach agreements not only in consensus but also by majority. That was a very important change that we achieved in the European Parliament, to avoid situations where we have to wait for everyone to agree to take a decision.

Data protection authorities are independent from governments and parliaments, but they are not independent from each other. They need to arrive at a consistent interpretation. This means that in order to act, they need to also be able to sometimes take decisions by majority.

I think that we made the right decision, but I also think that there could be a bit more courage. We need to get a little bit away of the 'diplomatic' past of our European family and get into a dialogue and a discussion, but also decisions.

Because for all the people out there, for the citizens but also for the companies who are developing new technologies, we need to get certainty about what is the right interpretation. It cannot be in the end up to the sole individual to calculate the best interpretation of a law, there is to be guidance and clear indications. This is also necessary for the legitimacy of the law, because people need to also see that this comes with a clear indication: 'what do I need to do with this law?'

8. ***What do you see as the main challenges for data protection for the future?***

I think that one of the biggest challenge is transparency and in particular meaningful transparency.

I am very pleased that the GDPR clearly indicates that the logic behind automated processing needs to be explained to individuals. This is important, because it makes clear that individuals cannot just be given incomprehensible information about which data is processed, but they need to provide me meaningful and understandable explanation about what exactly is done then with my data, not only by humans but also by the machine carrying out the automated processing. We need to be able to understand the logic behind it. This is very important in times of closed algorithms and hidden interests involved in all these new technologies.

We need to have this knowledge and that is important not only for the individual. It is important for society as a whole and for democracy. If we as a democracy, if our representatives in the in the parliaments, are no longer able to understand what is actually happening in the infrastructure of our digitalized lives, then we will no longer be able to take the right decisions to protect rights and interests of all of us. And we will no longer be able to ensure that the rules which we agreed are applied, and that in the end the rule of law is also upheld in the digital society.

09

EUDPR Unveiled: From Genesis to Enforcement

Thomas Zerdick, LL.M.

EUDPR Unveiled: From Genesis to Enforcement

Thomas Zerdick, LL.M. (*)

Through the EUDPR, the European Union's GDPR was adapted for Union institutions and bodies. However, the EUDPR contains some specificities in comparison to the GDPR, and it also contains additional provisions which cannot be found in the GDPR. Detailed examples of EUDPR enforcement actions and legal challenges illustrate the dynamic landscape of data protection within the EU, highlighting the critical role of the EDPS in overseeing compliance and guiding future legislative changes.

1. Introduction

When the European Union's General Data Protection Regulation (the 'GDPR') ([1]) entered into force in 2016 (and in full application on 25 May 2018), it contained two interesting provisions: The first, Article 2(3) GDPR (material scope), disapplied the GDPR to the processing of personal data by the Union institutions, bodies, offices and agencies, by mandating that instead Regulation (EC) No 45/2001 ([2]) applies. Furthermore, it laid down an obligation that Regulation (EC) No 45/2001 (and other Union legal acts applicable to such processing of personal data) was to be adapted to the principles and rules of the GDPR 'in accordance with Article 98'. Secondly, Article 98 GDPR required the European Commission to submit, if appropriate, legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. The

(*) EU official, and currently Head of Unit "Supervision and Enforcement" in the office of the European Data Protection Supervisor ('EDPS'). The views expressed are solely those of the author and do not necessarily reflect those of the EDPS.

([1]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

([2]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1.

Commission was specifically required to align the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies ('Union institutions and bodies') and on the free movement of such data.

The object of the explicit instruction to the Commission by the European legislators was in particular Regulation (EC) No 45/2001. Based on former Article 286(2) EC ([3]) as the legal basis, this regulation had governed the protection of natural persons in the processing of personal data by the institutions and bodies of the EU since 2001. The definitions and content of Regulation (EC) No 45/2001 were closely aligned with the Data Protection Directive ('DPD') ([4]), but were partly more precise and detailed than the DPD. Additionally, the European Data Protection Supervisor ('EDPS'), together with an Assistant Supervisor, was established as an independent data protection supervisory authority, based in Brussels ([5]).

Given its legal nature of a Regulation, the wording of some provisions of Regulation (EC) No 45/2001 clearly served as an inspiration for corresponding provisions in the Commission's proposal for the GDPR ([6]), in particular those relating to supervisory authorities as well as the data protection officer.

2. Genesis of the EUDPR

A formal adjustment of Regulation (EC) No 45/2001 in light of the Treaty of Lisbon was announced by the Commission as early as 2010 ([7]).

The EDPS already recommended in 2011 incorporating the substantive rules for Union institutions and bodies in the proposed Regulation, for the sake of legal certainty and uniformity. A single legal text would avoid the risk of discrepancies between provisions and would be the most suitable vehicle for data exchanges between the EU level and the public and private entities in the Member States ([8]).

([3]) Treaty establishing the European Community, OJ C 340, 10.11.1997, p. 294.

([4]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.1.1995, p. 31.

([5]) See Article 41 Regulation (EC) No 45/2001. Further provisions on fixing of the salary of the EDPS, the seat of the EDPS in Brussels as well clarification on the procedure for appointing the EDPS were laid down by Decision 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, OJ L 183, 12.7.2002, p. 1. See also further the contribution by Hustinx, P., 'The EDPS' first ten years', Chapter 2.

([6]) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 011 final.

([7]) Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, p. 18.

([8]) EDPS Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – ''A comprehensive approach on personal data protection in the European Union'', issued on 14 January 2011, paragraph 45.

The Commission, however, did not make a corresponding proposal part of the legislative package on the EU data protection reform presented in 2012 ([9]). This drew some fierce criticism from the European Parliament as well as the Member States ([10]), plus from the EDPS ([11]), who all preferred one regulation for all personal data protection rules of the Union.

To avoid further lengthy delays in the legislative process of the GDPR by incorporating substantive rules for Union institutions and bodies in the text of the proposed Regulation, the Commission declared during the negotiations that it intended to present the necessary proposals to adapt Regulation (EC) No 45/2001 to the GDPR within the two-year transition period between the entry into force and entry into application of the GDPR ([12]). This political commitment was then anchored in Article 2(3) and in Article 98, and elaborated on in Recital 17, according to which the necessary adjustments to Regulation (EC) No 45/2001 were to be made following the enactment of the GDPR so that they could be applied simultaneously with the GDPR.

The Commission presented its proposal in January 2017 ([13]). The co-legislators of the EUDPR felt committed to a coherent approach to personal data protection throughout the Union, and to aligning the data protection rules for Union institutions and bodies as far as possible with the data protection rules adopted for the public sector in the EU Member States. As a consequence, the co-legislators in general did not reopen substantive discussions on the provisions of either the GDPR or the Law Enforcement Directive ('LED') ([14]).

After brief negotiations between the European Parliament and the Council, the new Regulation (EU) 2018/1725 (the 'EUDPR') was formally adopted on 11 October 2018 and came into force on 11 December 2018 ([15]).

([9]) See in particular the reference to Regulation (EC) No 45/2001 in Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, COM(2012) 9 final, footnote 14.

([10]) See Albrecht, P.J., Jotzo, F., *Das neue Datenschutzrecht der EU*, Nomos, 2016, part 3, paragraph 20.

([11]) EDPS Opinion on the data protection reform package, issued on 7 March 2012, paragraph 29.

([12]) See the Draft Commission Declaration in the annex to Council document 10227/13 of 31 May 2013.

([13]) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM(2017) 8 final. Its explanatory memorandum reveals a scarcity of explanations and understandably relies heavily on the 'solutions' (painfully) negotiated for the GDPR. See in particular its section 5 with the article-by-article presentation. The absence of the conduct of an impact assessment accompanying the legislative proposal is also a telling element.

([14]) Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89. See more on the LED in the contribution by Coudert, F., Quintel, T., and Sajfert, J. 'Area of Freedom, Security and Justice', Chapter 10.

([15]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

3. The EUDPR compared to the GDPR

A quick comparison of the EUDPR with the GDPR shows that the EUDPR very closely follows the structure of the GDPR: the GDPR has 99 Articles, subdivided in eleven chapters; the EUDPR contains 102 Articles, divided in twelve chapters. In conformity with the co-legislators' express wish, the EUDPR's substantial provisions are identical to, or follow very closely those of the GDPR.

A closer look, however, reveals that the EUDPR represents a more complete data protection instrument than the GDPR. The co-legislators of the EUDPR certainly did more than limiting themselves to a 'copy and paste' from the GDPR. Instead, they carefully adapted several of its provisions to the context of the Union institutions and bodies. As a result, the EUDPR contains some specificities in comparison to the GDPR, and it also contains additional provisions which cannot be found in the GDPR. The following explores some of those specificities and additions ([16]).

3.1. Union institutions and bodies

The EUDPR only applies to processing of personal data by Union institutions and bodies ([17]). 'Union institutions and bodies' are defined as the Union institutions, bodies, offices and agencies set up by, or on the basis of, the TEU ([18]), the TFEU ([19]) or the Euratom Treaty ([20]). In that context, the EUDPR contains specific definitions of 'controller' and of 'controllers other than Union institutions and bodies' ([21]).

As a consequence, in its current practice, the EDPS applies its supervisory powers exclusively to Union institutions and bodies, and where necessary, seeks the cooperation under Article 61 EUDPR with those national supervisory authorities that have jurisdiction over controllers or processors which are non-Union institutions and bodies ([22]).

([16]) See for other examples, Kranenborg, H., and Buchta, A., 'Institutional Report Topic 2: The New EU Data Protection Regime', in: Rijpma, J. J., *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, Boom Uitgevers, The Hague, 2020.

([17]) Article 2(1) EUDPR.

([18]) Consolidated version of the Treaty on European Union, OJ C 202, 7.6.2016, p. 13.

([19]) Consolidated version of the Treaty on the Functioning of the European Union, OJ C 202, 7.6.2016, p. 47.

([20]) Consolidated version of the Treaty establishing the European Atomic Energy Community, OJ C 203, 7.6.2016, p. 1. See Article 3(10) EUDPR. For an overview of Union institutions and bodies, see the EDPS list of Data Protection Officers appointed by the EU institutions and bodies.

([21]) Article 3(8): 'controller' means the Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law'. Article 3(9) EUDPR: 'controllers other than Union institutions and bodies' means controllers within the meaning of point (7) of Article 4 of Regulation (EU) 2016/679 and controllers within the meaning of point (8) of Article 3 of Directive (EU) 2016/680'.

([22]) This is however without prejudice to the possibility for the EDPS to request direct cooperation of processors which are non-Union institutions and bodies during investigations related to processing for which those Union institutions and bodies are controllers.

3.2. The mystery of the missing missions

The Union's Common Security and Defence Policy ('CSDP') missions are excluded from the scope of the EUDPR ([23]). The position of the Council in particular was based on the legal reasoning that rules on data protection for missions and operations in the CSDP area should only be based on Article 39 TEU ([24]).

This is somewhat surprising: while Article 16 TFEU provides a legal basis for establishing data protection rules also in the area of Common Foreign and Security Policy ([25]), including the CSDP, the different legal basis and procedure laid down by Article 39 TEU applies only when personal data are processed in this area *by the Member States* ([26]).

As a result of the exclusion from the scope of the EUDPR, there are at the time of writing no data protection rules in place for such missions when processing operations are being carried *by Union institutions, bodies, offices and agencies* in the context of the CSDP.

In the absence of specific rules for these CSDP missions, the EDPS declared it would *'interpret the applicable rules in the spirit of the EUDPR'*, and *'apply the principles of the Regulation in areas where specific rules are missing'* ([27]). This announcement seems to have been noticed by the legislator ([28]).

3.3. Cookie rules for Unions institutions and bodies

Unlike the GDPR, but following Regulation (EC) No 45/2001, the EUDPR integrates rules based on the Directive on privacy and electronic communications ([29]) for the protection of the confidentiality of electronic communications. Articles 36, 37 and 38 EUDPR require the Union institutions and bodies to ensure the confidentiality of electronic communications, to protect the informa-

([23]) Article 2(4) EUDPR. For a list of former and current missions, see the European External Action Service overview.

([24]) See Council document 15961/17 of 22 December 2018, p. 4.

([25]) As regards the former second pillar, i.e. the Common Foreign and Security Policy ('CFSP'), Article 39 TEU makes use of the derogation foreseen in Article 16(2) TFEU in relation to CFSP and establishes a distinct regime for the processing of personal data by the Member States when they carry out activities falling within the scope of CFSP. With regard to these issues, the Council is empowered to adopt a decision on the regulation of Member States' processing of personal data in the area of CFSP. However, until the present day the Council has not adopted such a decision.

([26]) See the Commission's declaration in Council document 12221/18 ADD1 of 21 September 2018.

([27]) EDPS Strategy 2020 – 2024: Shaping a safer digital future, issued on 30 June 2020, p. 17.

([28]) See e.g. Article 70 of Council Decision (CFSP) 2021/509 of 22 March 2021 establishing a European Peace Facility, and repealing Decision (CFSP) 2015/528, OJ L 102 24.3.2021, p. 14 which applies the 'principles and procedures' of the EUDPR, 'without prejudice to Article 2(4)' of the EUDPR.

([29]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37. Amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, p. 11. See also further the contribution by Barcelo, R., 'The ePrivacy Directivey: Then and Now, Chapter 5.

tion transmitted to, stored in, related to, processed by and collected from the terminal equipment of users accessing publicly available websites and mobile applications of Union institutions and bodies, in accordance with Article 5(3) of Directive 2002/58/EC, and to limit personal data of users in its directories.

3.4. Chapter IX EUDPR: rules for law enforcement agencies

The most important political issue during the EUDPR negotiations concerned the processing of so-called 'operational personal data' by Union bodies, offices and agencies carrying out activities in the field of judicial cooperation in criminal matters and police cooperation. On the one hand, to reduce fragmentation of data protection rules, the European Parliament considered that all processing of personal data by Union agencies and offices in this specific field (the European Union Agency for Criminal Justice Cooperation ('Eurojust'), the European Union Agency for Law Enforcement Cooperation ('Europol') and the European Public Prosecutor's Office ('EPPO') and possibly other agencies carrying out law enforcement activities) should be laid down in the new Regulation. On the other hand, because of the alleged specific needs of law enforcement agencies when processing personal data, the Council wanted these agencies to continue to have specific data protection rules for their operations in their founding acts.

In order to converge the positions of the Council and the Parliament, the co-legislators agreed on inserting in the EUDPR a new Chapter IX with general rules on processing of operational personal data by Union bodies, offices and agencies when carrying out activities in the field of judicial cooperation in criminal matters and police cooperation, while retaining specific tailor-made provisions in the founding acts of the agencies. This was flanked with a specific obligation for the Commission to review the relevant legal acts governing the processing of operational personal data and to make legislative proposals, in particular with a view to applying the provisions to Europol and EPPO ([30]).

Operational personal data are defined in the EUDPR as *'all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies'* ([31]).

Chapter IX replicates in a large part the provisions of the LED. It contains substantive provisions corresponding to most provisions of Chapters II to V of the EUDPR (general principles, rights of data subjects, certain obligations of controllers and processors, international data transfers), with some differences to take the specific nature of law enforcement into account (e.g. rules on (not) informing data subjects and on their right of access to their data).

([30]) Article 98 EUDPR.

([31]) Article 3(2) EUDPR. The processing of administrative personal data, such as staff data, by those Union bodies, offices or agencies is fully covered by the other provisions of the EUDPR.

The EDPS has since then, however, highlighted that Chapter IX is not without shortcomings. By way of example: the fragmentation of the provisions on EDPS powers creates confusion as to the role of the EDPS as supervisory authority, as not all Union institutions and bodies are put on the same footing. It is not clear, for instance, to what extent the EDPS can conduct data protection audits as these investigative powers are not explicitly mentioned in any of the still existing specific instruments. It is also not clear whether Union institutions and bodies processing operational data have the same legal obligation to cooperate, on request, with the EDPS, as set out under Article 32 EUDPR ([32]).

In addition, while Article 3 and Chapter IX EUDPR apply to Eurojust since 12 December 2019 ([33]) and to Europol since 28 June 2022, it does not yet apply to the EPPO whose establishing Regulation ([34]) was adopted prior to the EUDPR and which provides for a standalone regime for processing operational data. This has two consequences: First, some provisions in the EPPO Regulation differ in substance from the EUDPR chapter, such as the processing of 'restricted' personal data ([35]). Second, some provisions of the EPPO Regulation, although similar in substance, are worded differently than the Chapter IX EUDPR, which could lead to different interpretations.

3.5. Administrative fines

Another controversial discussion during the negotiations covered the extent and conditions under which the EDPS should have the authority to impose administrative fines on Union institutions and bodies for violations of the EUDPR. At national level, some Member States opted for the possibility provided for in Article 83(7) GDPR of imposing fines on authorities and public bodies when applying the GDPR, while other Member States rejected this on considerations of principle. At the EU level, this question was ultimately decided in the affirmative, with the enthusiastic support of the EDPS ([36]). Therefore, if Union institutions and bodies violate the EUDPR, a fine must be paid to the EU general budget, which can amount to up to 50 000 EUR per violation and up to a total of 500 000 EUR per year.

([32]) See, also for more examples, EDPS Contribution to the Report on the application of Regulation (EU) 2018/1725, issued on 21 December 2021, p. 36.

([33]) Article 26(1) Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018, p. 138.

([34]) Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, p. 1.

([35]) Compare Article 61(4) of the EPPO Regulation with Article 82(3) EUDPR.

([36]) EDPS, Upgrading data protection rules for EU institutions and bodies, Opinion 5/2017 on the proposal for a Regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, issued on 15 March 2017, paragraph 80.

At the same time, the administrative fines framework for Union institutions and bodies under the EUDPR diverges significantly from the GDPR. Unlike the GDPR, where fines can complement or replace other corrective actions, the EUDPR mandates fines solely for non-adherence to specific corrective measures outlined in Article 58(2)(d) to (h) and (j) ([37]). Additionally, Article 66 EUDPR sets lower maximum fines – typically not surpassing 25 000 EUR per violation and 250 000 EUR annually. Only for severe breaches, such as those against basic processing principles, data subjects' rights, or transfer rules to third countries, fines can reach up to 50 000 EUR per incident and 500 000 EUR annually. Also, the cumulative fines for multiple related infringements cannot exceed the penalty for the most serious violation.

3.6. Homogeneity of interpretation

Regulation (EC) No. 45/2001 already explicitly emphasized the necessity of a coherent and homogeneous application of the provisions for the protection of fundamental rights and freedoms of persons in the processing of personal data throughout the (then) European Community ([38]).

Since the EUDPR was explicitly aimed to be aligned with the GDPR, the uniformity and coherence demanded by Article 98 GDPR must also continue at the level of legal application. In particular, in accordance with the jurisprudence of the CJEU on the DPD and Regulation (EC) No. 45/2001, the provisions of the GDPR and the EUDPR are now to be interpreted homogeneously ([39]). Recital 5 EUDPR explicitly underscores this corresponding intention of the EU legislator: *'Whenever the provisions of this Regulation follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union (the 'Court of Justice'), be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679'*.

Therefore, in the light of this requirement of homogeneous interpretation, judgments of the Union courts on the application of the EUDPR can regularly provide valuable guidance for the interpretation of the GDPR and LED ([40]), and vice-versa ([41]).

([37]) Recital 81 EUDPR speaks of '*a sanction of last resort*'.

([38]) Recital 12 Regulation (EC) No 45/2001.

([39]) See in particular Judgment of the Court of Justice of 9 March 2010, *Commission / Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 28, where the Court decided that in view of the fact that Article 44 of Regulation (EC) No 45/2001 and Article 28 of Directive 95/46 are based on the same general concept, those two provisions should be interpreted homogeneously, so that not only the independence of the EDPS, but also that of the national authorities, involve the lack of any instructions relating to the performance of their duties.

([40]) See e.g. as regards the definition of personal data within the meaning of Article 3(1) EUDPR (and Article 4(1) GDPR), Judgment of the General Court of 26 April 2023, *SRB / EDPS*, T-557/20, ECLI:EU:T:2023:219; appeal pending before the Court of Justice, C-413/23 P.

([41]) See e.g. as regards the determination of the existence of a conflict of interests of a data protection officer, within the meaning of Article 38(6) GDPR (and Article 44(6) EUDPR), Judgment of the Court of Justice of 9 February 2023, *X-FAB Dresden*, C-453/21, ECLI:EU:C:2023:79, paragraph 44.

4. EUDPR supervision and enforcement in practice

The EDPS is the independent data protection supervisory authority for Union institutions and bodies, mirroring the role of the national data protection supervisory authorities established in the Member States under the GDPR and the LED ([42]).

The EDPS specified the application of the EUDPR in its Rules of Procedures ([43]) and adopted, in accordance with Article 39(4) and (5) EUDPR, a list of the kinds of processing operations subject to a data protection impact assessment ('DPIA') as well as kinds of processing operations not subject to a DPIA ([44]).

The EDPS also stepped up its enforcement activities, and has used most of its corrective powers under the EUDPR; however, at the time of writing, it has not used its new power to issue administrative fines. The EDPS has equally issued many decisions which have often involved situations and technologies that are relevant outside the context of Union institutions and bodies.

Some noteworthy examples of EDPS supervision and enforcement in practice include:

4.1. Social media monitoring

The EDPS made use of his corrective power under Article 58(2)(g) EUDPR to impose for the first time a temporary ban on the processing operation for social media monitoring by the then European Asylum Support Office ('EASO'), in the absence of a legal basis for the processing operations at hand ([45]).

4.2. NationBuilder

As part of its campaign activities for the 2019 EU parliamentary elections, the European Parliament had set up a website called thistimeimvoting.eu, aimed at promoting public engagement. During the campaign, the website collected personal data from over 329 000 individuals, which were processed on behalf of the Parliament by the US political campaigning company NationBuilder. Taking into account previous controversy surrounding this company, the EDPS

([42]) Articles 52 to 60 EUDPR. The EUDPR abolished the position of the Assistant EDPS.

([43]) See EDPS Decision of 15 May 2020 adopting the Rules of Procedure of the EDPS, OJ L 204, 26.6.2020, p. 49 and EDPS Decision of 14 October 2022 amending the Rules of Procedure of the EDPS of 15 May 2020, OJ L 274, 24.10.2022, p. 78.

([44]) EDPS Decision on DPIA lists issued under Articles 39(4) and (5) of Regulation (EU) 2018/1725, issued on 16 July 2019.

([45]) EDPS letter concerning a consultation on EASO's social media monitoring reports, issued on 14 November 2019. See in a similar case, EDPS Supervisory Opinion on the use of social media monitoring for epidemic intelligence purposes by the European Centre for Disease Prevention and Control ('ECDC'), issued on 9 November 2023.

launched an investigation in February 2019, in order to determine whether the Parliament's use of the website, and the related processing of personal data, complied with the EUDPR. ([46])

The EDPS' investigation into the European Parliament's use of NationBuilder resulted in the first ever EDPS reprimand issued to an EU institution, in accordance with Article 58(2)(b) EUDPR, for a contravention by the Parliament of Article 29 EUDPR, involving the selection and approval of sub-processors used by NationBuilder. A second reprimand was subsequently issued by the EDPS, after the Parliament failed to publish a compliant Privacy Policy for the thistimeimvoting website within the deadline set by the EDPS.

The European Parliament responded promptly by implementing the EDPS recommendations, including informing individuals of their revised intention to retain personal data collected by the thistimeimvoting website until 2024. The EDPS visited the European Parliament in November 2019, to check its data retention procedures, and confirmed the deletion of data from over 260 000 users who had not accepted the updated privacy policy.

4.3. Moving to the cloud and international transfers

In 2020, the EDPS investigated the institutions' use of Microsoft products and services, and found a number of areas of non-compliance, including a lack of control over the location of data processing and what data were transferred out of the European Economic Area ('EEA') ([47]). In a follow-up investigation into the European Commission's use of Microsoft Office 365, the EDPS found infringements of key data protection rules related to purpose limitation, international transfers and unauthorised disclosures of personal data. In its decision, the EDPS imposed corrective measures on the Commission ([48]).

In addition, in 2022 the EDPS reprimanded the European Parliament for the use of Google Analytics that resulted in transfers of personal data to the US without appropriate safeguards ([49]).

On 1 April 2022, the EDPS reprimanded the European Border and Coast Guard Agency ('Frontex') for a breach of the EUDPR's rules on accountability, responsibility as well as the legal obligation of data protection by design, for having moved to a hybrid cloud consisting of Microsoft Office 365, Amazon Web Services ('AWS') and Microsoft Azure. On top of the reprimand, the EDPS

([46]) EDPS, EDPS investigates European Parliament's 2019 election activities and takes enforcement actions, Press Release, issued on 28 November 2019.

([47]) EDPS, Outcome of own-initiative investigations into EU institutions' use of Microsoft products and services, Public Paper, issued on 2 July 2020.

([48]) EDPS decision on the investigation into the European Commission's use of Microsoft 365, issued on 8 March 2024

([49]) EDPS Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament, issued on 5 January 2022, see EDPS Annual Report 2022, p. 34.

ordered Frontex to review its Data Protection Impact Assessment and the Record of Processing activities relating to the processing of personal data in cloud services ([50]).

Conversely, in a Decision published on 13 July 2023, the EDPS found that the use of Cisco Webex videoconferencing and related services by the Court of Justice of the European Union met the data protection standards of the EUDPR ([51]). The EDPS issued this decision on the basis of the revised agreement between the Court and Cisco, which ensures that the processing of individuals' personal data occurs only in the EEA, and the Court's inclusion of technical and organisational measures to prevent the risks associated with transfers of personal data outside the EEA.

4.4. Supervising Europol

On 15 July 2022, the EDPS referred to Europol a breach of the amended Europol Regulation following Europol's failure to consult the EDPS before adopting four Management Board decisions implementing Articles 18(2), 18(6), 18(6a) and 18a of the amended Europol Regulation. On 19 July 2022, the EDPS also referred this matter to the European Parliament, as well as the Council and the Commission, in accordance with Article 43(3)(g) of the amended Europol Regulation and making use of this power for the first time.

On 16 September 2022, the EDPS requested the Court of Justice of the European Union ('CJEU') to annul two provisions of the amended Europol Regulation ([52]). In the eyes of the EDPS, these new provisions, Articles 74a and 74b, have the effect of legalising retroactively Europol's practice of processing large volumes of individuals' personal data with no established link to criminal activity. This type of personal data processing is something that the EDPS found to be in breach of the Europol Regulation, which it made clear in its Order issued on 3 January 2022 requesting Europol to delete concerned datasets within a predefined and clear time limit ([53]). This action represented the first time that the EDPS took the European Parliament and the Council to the Court for adopting legislation ([54]).

([50]) EDPS Decision concerning the investigation into Frontex's move into the cloud, issued on 1 April 2022.

([51]) EDPS Decision on the Court of Justice of the EU's request to authorise the contractual clauses between the Court of Justice of the EU and Cisco Systems Inc. for transfers of personal data in the Court's use of Cisco Webex and related services, issued on 13 July 2023.

([52]) EDPS, EDPS takes legal action as new Europol Regulation puts rule of law and EDPS independence under threat, Press Release, issued on 22 September 2022.

([53]) EDPS Decision on the retention by Europol of datasets lacking data subjects categorisation, notified on 3 January 2022.

([54]) The action was dismissed on grounds of inadmissibility with Order of the General Court of 6 September 2023, CEPD/Parliament and Council, T-578/22, ECLI:EU:T:2023:522; an appeal is pending with the Court of Justice of the EU, CEPD/Parliament and Council, C-698/23 P.

5. Outlook on the future of the EUDPR

A first evaluation of the EUDPR was carried out by the Commission in 2022 ([55]), including on the basis of an EDPS contribution ([56]). In its report, the Commission expressed satisfaction with the working of the EUDPR. However, it suggested a future amendment to the EUDPR to clarify the relationship of the chapter on law enforcement to the other provisions of the Regulation and in this way to better and more uniformly capture the EPPO, Europol, Eurojust, and Frontex, and the operational data processed by them.

In the meantime, based on practical experience, the EDPS has underlined an additional need for complementary detailed rules for cases where personal data flows from Union institutions and bodies to other public bodies or private entities within the EEA and vice-versa: data protection authorities have encountered several obstacles to efficient cooperation and enforcement between them, resulting in particular from a lack of clarity on the terms of cooperation between the EDPS and national supervisory authorities([57]).

5.1. Concluding remarks

The EUDPR represents a significant evolution in the EU's approach to data protection by Union institutions and bodies, aiming to address the multifaceted nature of privacy in the digital age more effectively. By building on the foundation of the GDPR and integrating additional provisions that reflect the realities of electronic communications and the specific needs of law enforcement, the EUDPR represent a more comprehensive framework for protecting individuals' data protection rights.

However, this evolution also underscores the ongoing challenge of matching the need for robust data protection with the practicalities of application and enforcement. This in turn provides for a critical role of the EDPS in supervising compliance and guiding future legislative changes.

([55]) Communication from the Commission to the European Parliament and the Council First report on the application of the Data Protection Regulation for European Union institutions, bodies, offices and agencies (Regulation 2018/1725), COM(2022) 530 final.

([56]) EDPS Contribution to the Report on the application of Regulation (EU) 2018/1725, issued on 21 December 2021.

([57]) EDPS Contribution in the context of the Commission initiative to further specify procedural rules relating to the enforcement of the General Data Protection Regulation, issued on 25 April 2023. See also EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, adopted on 19 September 2023, paragraphs 182-189.

10

The Area of Freedom, Security and Justice

Fanny Coudert
Teresa Quintel
Juraj Sajfert

The Area of Freedom, Security and Justice

Fanny Coudert (*) **Teresa Quintel (**)** **Juraj Sajfert (***)**

During the last 20 years, EU policy in the Area of Freedom, Security and Justice ('AFSJ') has been slowly taking shape. The EU data protection rules for law enforcement evolved from a fragmented and unreadable landscape under the Maastricht regime to the authoritative leadership of the Law Enforcement Directive ('LED') in the Lisbon era (section 1). In the field of border management, EU large scale IT systems have developed to facilitate data exchanges, culminating with the set-up of the Interoperability framework (section 2). The supervision model has also evolved towards a full coordinated supervision model, integrating both national and EU levels, with the EDPS as the supervisor of AFSJ EU Agencies and bodies, with similar powers as national Data protection Authorities. (Section 3). This Chapter chronicles the development of the Area of Freedom, Security and Justice and the related data protection challenges from these three perspectives.

1. From Maastricht to Lisbon: the emergence of the Law Enforcement Directive

1.1. The three pillars and the unreadable legislative landscape

In the early nineties, the Maastricht Treaty built the European Union on three pillars. Next to the existing supranational European Communities, two intergovernmental policy areas formed the second and the third pillar of the

(*) Head of Sector Area of Freedom, Security and Justice, Supervision & Enforcement Unit, European Data Protection Supervisor. The views expressed are solely those of the author and do not necessarily reflect those of the EDPS.

(**) Assistant Professor at the European Centre for Privacy and Cybersecurity (ECPC) at Maastricht University.

(***) European Commission official and postdoctoral researcher at the Vrije Universiteit Brussel. Information and views set out in this article are those of the author and do not reflect the official opinion of the European Commission.

EU: common foreign and security policy, and justice and home affairs ([1]). The latter consisted of police cooperation and judicial cooperation in criminal matters. Shortly thereafter, the EU adopted its first horizontal data protection instrument, the Directive 95/46/EC. However, it was applicable only in the first, Community pillar. On the other hand, the third pillar data protection was structured around a series of separate sets of rules establishing a series of actors ([2]). As stated by Hijmans and Scirocco, the regime is '*best defined as a patchwork of data protection regimes*', with '*no legal framework which is stable and unequivocal, like Directive 95/46/EC in the First pillar*' ([3]).

For the entire duration of the Maastricht EU architecture, the legislator in the third pillar invested heavily in the creation of *sui generis* data protection rules, tailored for the purposes of a particular instrument. The legislator would first detect a data protection instrument of general application, and then create some specific data protection rules. For the activities on the margins of competencies of law enforcement authorities (e.g. border management), which were included in the first pillar, it was easy to find an instrument of general application, since the EU had a horizontal data protection instrument available – Directive 95/46/EC. However, for the core law enforcement activities under the third pillar, the EU did not have such an instrument up until the very end of the Maastricht regime when Framework Decision 2008/977/JHA was adopted. The legislator had no real choice but to rely on the Council of Europe instruments, in particular the Convention 108 and the Recommendation 87(15). In order to fill the horizontal legislative void, the legislator resorted to two legislative techniques, the combination of which became the law enforcement data protection blueprint in the Maastricht EU: a) referring to Council of Europe instruments –Convention 108 and the Recommendation 87(15), and/or b) creating *sui generis* data protection rules for the purposes of an individual legislative act.

The Maastricht Treaty not only created the EU and the third pillar, but also envisaged institutionalising the third pillar activities through the creation of EU law enforcement agencies. Europol was established for the police cooperation and Eurojust for the judicial cooperation in criminal matters.

([1]) De Witte, B., 'A Legal Paradox of Maastricht: The Creation of the European Union', in: Baroncelli, S., Spagnolo, C., Talani, L.S. (eds.), *Back to Maastricht. Obstacles to Constitutional Reform within the EU Treaty (1991-2007)*, Cambridge Scholars Publishing, Newcastle, 2008.

([2]) See further in González Fuster, G., Paepe, P., 'Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects' in: Geyer, F., Guild, E. (eds.) *Security versus Justice? Police and Judicial Cooperation in the European Union*, Taylor and Francis, 2008, p. 129-150.

([3]) Hijmans, H., Scirocco, A., 'Shortcomings in EU Data Protection in the Third and the Second Pillars; Can the Lisbon Treaty be Expected to help;' *Common Market Law Review*, Vol. 46(5), 2009, p. 1496.

At the time, the Union institutions, bodies, offices and agencies were in a situation comparable to the rest of the EU. They had a horizontal data protection instrument for the first pillar, the Regulation (EC) No 45/2001 ([4]). This Regulation was adopted in order to lay down the rules on personal data protection applicable to Community institutions, bodies, offices and agencies. While building on the principles of the Directive 95/46/EC ([5]), the different nature of the instrument and its limited scope allowed the Regulation to introduce more precision and additional safeguards compared to the Directive ([6]). Moreover, it served as a founding act establishing the European Data Protection Supervisor (EDPS) as the data protection authority for Community institutions, bodies, offices and agencies. In that context, Europol and Eurojust were left in a data protection vacuum. Their founding acts had to come up with their own, standalone data protection regimes and their own *ad hoc* supervisory authorities – Joint Supervisory Bodies.

1.2. A glimmer of harmonisation hope: Framework Decision 2008/977/JHA

In 2005, the European Commission proposed a Council Framework Decision on the exchange of information under the principle of availability, which was never adopted. That proposal was one half of a package deal, coupled with the Commission proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters ([7]). After three years of long and difficult negotiations, this Decision was adopted in the zenith of the Maastricht era, to become Council Framework Decision 2008/977 JHA ([8]). It was the only horizontal data protection instrument adopted in the history of the third pillar.

The objective of the 2008 Framework Decision was to combine and render more coherent the existing standards for data protection applicable in the field of police cooperation and judicial cooperation in criminal matters. The Commission proposal included similar principles and data subject rights as those of Directive 95/46/EC and was intended to be applicable to processing at both the national level and to cross-border data exchanges between the EU law enforcement authorities. However, those initial drafts were watered down

([4]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p.1.

([5]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

([6]) For instance, specific rules on transmissions to recipients covered by the Directive, mandatory data protection officers, central registers of processing operations held by each institution and body in a publicly accessible format. See further in Schild, H.-H., Tinnefeld, M.-T., 'Datenschutz in der Union–Gelungene oder missglückte Gesetzentwürfe?', *Datenschutz und Datensicherheit – DuD*, Vol. 36(5), 2012, p. 312–317, p. 316.

([7]) COM(2005) 475 final.

([8]) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.

during the negotiations ([9]). The Council and the Multidisciplinary Group on organized Crime, which assumed the drafting process of the 2008 Framework Decision in 2006, were anything but strong supporters of strict data protection rules in an area where the safeguarding of high security standards was the first priority ([10]).

Therefore, the final text of the Decision included numerous exemptions and had a very limited scope of application ([11]). All the law enforcement data exchange instruments (SIS, Prüm, Swedish Initiative, Europol, Eurojust) were left intact. They kept their *sui generis* data protection regimes and remained out of scope of the Framework Decision. What is more, the horizontal effect of the Framework Decision was severely undermined by limiting its application to a specific type of processing: cross-border data exchanges between the Member States' law enforcement authorities ([12]). 'National' processing of operational law enforcement data was simply not covered. Hence, not much was *de facto* left for the Framework Decision to regulate, and even then it had done a poor job ([13]). Substantively, the 2008 Framework Decision included a rudimental set of data subject rights, including the right to receive compensation and the right to judicial remedy, in Articles 16-20. However, those provisions contained a number of exemptions and deferred significantly to applicable national law. Furthermore, the 2008 Framework Decision subjected the processing falling under its scope to the oversight of data protection supervisory authorities (Article 25). However, the powers of those authorities were severely limited, in particular their 'effective powers of intervention'. As regards the rules on international transfers or transmissions to private parties in Member States (Articles 13 and 14), the 2008 Framework Decision recycled some solutions from German data protection law ([14]) applicable at the time to its public sector. Finally, the 2008 Framework Decision included a number of technical data protection rules (e.g. on data security, logging and documentation) and basic data protection principles, again, with a lot of deference to national law. It is not surprising that, as soon as the Lisbon Treaty entered into force, some authors warned that the 2008 Framework Decision, although brand new, already had to be replaced by another instrument, because it had not fulfilled the criteria of Article 16 TFEU ([15]).

([9]) Quintel, T., 'Data Protection, Migration and Border Control', *The GDPR, the Law Enforcement Directive and Beyond*, Vol. 17, Bloomsbury Publishing, 2022, p. 98.

([10]) Bellanova, R., 'The 'Prüm process': The way forward for EU police cooperation and data exchange? in: Guild, E., Geyer, F., (eds.), *Security Vs. Justice? – Police and Judicial Cooperation in the European Union*, Ashgate, 2008, p. 208.

([11]) Mitsilegas, V. 'The Third Wave of Third Pillar Law: Which Direction for EU Criminal Justice?', *European Law Review,* Vol. 34, 2009, p. 559.

([12]) O'Neill, M., 'The issue of data protection and data security in the (pre-Lisbon) EU third pillar', *Journal of Contemporary European Research*, Vol. 6, No. 2, p. 21.

([13]) On the shortcomings of the 2008 Framework Decision, see more in De Hert, P., Papakonstantinou, V.,'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for', *Computer Law & Security Review*, Vol. 25, No. 5, p. 403–414.

([14]) See further in Schild, H.-H., Tinnefeld, M.-T., op. cit. (footnote 66).

([15]) Hijmans, H., Scirocco, A., op. cit. (footnote 3), p.1519.

1.3. Lisbonisation and depillarisation of the EU data protection law

The 2009 Treaty of Lisbon, and in particular its reform of the EU architecture, introduced major novelties relevant for EU data protection law. Firstly, the Lisbon Treaty abolished the pillar structure and thus created an opportunity for harmonisation of EU data protection rules. Secondly, it made the Charter binding, embedded in EU primary law. The Charter explicitly provides for the right to personal data protection in its Article 8 ([16]). The reformed EC Treaty, now TFEU, introduced a very strong legal basis for EU to legislate in the area of data protection, already mentioned Article 16. The latter established a clear rule that the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and relating to the free movement of such data, are regulated under the ordinary legislative procedure exercised by the European Parliament and the Council, aimed at ensuring the uniform application of rules in all areas of EU law in relation to the processing of personal data.

At the same time, the Member States gathered in the Intergovernmental Conference adopting the Treaty of Lisbon were eager to keep some of their prerogatives stemming from the to-be-abandoned pillar structure, in particular in the area of law enforcement. In relation to the processing of personal data, the Conference declared that, '*whenever rules on protection of personal data to be adopted on the basis of Article 16 [TFEU] could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter. It recalls that the legislation presently applicable (see in particular Directive 95/46/EC) includes specific derogations in this regard*' ([17]). What is more, the Intergovernmental Conference adopted the Declaration No 21, stating that '*specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields*' ([18]). This Declaration ultimately lead to a different set of data protection rules, i.e. the LED and not the GDPR, to be applicable to law enforcement authorities processing personal data for law enforcement purposes ([19]).

([16]) On the emergence of the fundamental right to personal data protection in the EU, see further González Fuster, G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer Science & Business, 2014.

([17]) Consolidated versions of the Treaty on European Union and the Treaty on the functioning of the European Union Declaration, OJ C 326, 26.10.2012, p.347.

([18]) *Ibid.*

([19]) As regards the former second pillar, i.e. the Common Foreign and Security Policy, Article 39 TEU made use of a derogation foreseen in Article 16(2) TFEU in relation to CFSP and established a different regime for the processing of personal data by the Member States when they carry out activities falling within the scope of CFSP. With regard to these issues, the Council is empowered to adopt a decision on the regulation of the processing of personal data in the area of CFSP. However, until the present day the Council has not adopted such a decision.

1.4. 2012 Data Protection Reform Package

In January 2012, the European Commission presented a comprehensive proposal for the review of the data protection framework in the European Union ([20]). The review covered, on the one hand, the replacement of the Directive 95/46/EC with a Regulation as regards the general processing of personal data, and, on the other hand, the replacement of the 2008 Framework Decision with a Directive as regards the processing of personal data for law enforcement purposes by competent authorities ([21]).

The new data protection architecture proposed by the Commission was welcomed with mixed feelings. The EDPS and the Article 29 Working Party ('WP29') were concerned about the failure of the reform package to remedy the lack of comprehensiveness of the EU data protection rules ([22]). This was visible in particular in the third pillar, where the proposal for what became Article 60 of the Directive (EU) 2016/680 – LED – grandfathered the specific data protection rules developed for *inter alia* abovementioned instruments like Schengen Information System, Prüm and Swedish Initiative, and thereby preserved a certain level of fragmentation. In particular, the EDPS and the WP29 voiced concerns regarding some aspects of the LED ([23]) proposal and where equally disappointed that the law enforcement data processing would be regulated by a Directive offering lower standards of protection and lesser harmonisation.

In any event, the adoption of the data protection reform was turbulent and long. On 15 December 2015, after four years of negotiations, the Luxembourgish Presidency of the Council and the European Parliament reached an agreement on the text of both the GDPR and the LED. The legislative texts were formally adopted in April 2016 and entered into force/application in May 2018.

The LED is the first piece of EU data protection legislation that is horizontally applicable to all personal data processing activities by law enforcement authorities, carried out for law enforcement purposes. As such, the LED was specifically designed to ensure the protection of personal data in the law enforcement context, while enabling LEAs to process and exchange personal data in the digital era ([24]). This is visible from the two principal objectives of the LED: the increased level of fundamental rights protection in the area of police and criminal justice, and the improved sharing of personal data between the Member States, i.e. reliance on harmonised data protection rules (Article

([20]) COM(2012) 9 final, COM(2012) 10 final and COM(2012) 11 final.

([21]) For a critical view of this dual approach, see further in Kosta, E., 'A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon', SSRN, 2021.

([22]) Article 29 Working Party Opinion 01/2012 on the Data Protection Reform Proposals, adopted on 23 March 2012.

([23]) The purpose limitation principle, the processing of special categories of data, the data subject rights, the oversight exercised by the supervisory authorities, and the rules on international transfers.

([24]) See De Hert, P., & Sajfert, J., 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data' in: Briere, C., and Weyembergh, A. (eds.), *The needed balances in EU Criminal law: Past, present and future,* Hart Publishing, 2017, p. 245.

1(2)). The LED is a major step forward in establishing a comprehensive EU data protection regime, as the first horizontal and legally binding instrument laying down the rules for national and cross-border processing of personal data in the area of law enforcement ([25]). Although the LED did not show the ambition to consolidate the entire former third pillar data protection rulebook at once, it was clear from the moment of the adoption that its gradual, mid-term goal was to create a spill-over effect and become the standard for data protection rules for law enforcement authorities in the EU. Article 62(6) of the LED tasked the Commission to review, by May 2019, '*other legal acts adopted by the Union which regulate processing by the competent authorities … in order to assess the need to align them with this Directive and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of this Directive*'. In the meantime, this exercise has almost been finalised. *Sui generis* rules have been gradually replaced with reliance by references on the LED rules. References to the Council of Europe instruments have been removed. Only two instruments are still not revised: the EU PNR Directive (EU) 2016/681, which depends on the follow-up to the CJEU judgment *Ligue des droits Humains*; and the alignment of the EU-Japan Mutual Legal Assistance Agreement, which depends on international negotiations, and not only on the EU itself.

Furthermore, the LED-lead consolidation had also a spill-over effect on the EU law enforcement agencies and bodies Regulation (EU) 2018/1725 on processing of personal data by Union institutions, bodies, offices and agencies (EUDPR) includes Chapter IX ([26]) as 'a Regulation within the Regulation', the 'LED within the GDPR'. Chapter IX replicates the provisions of the LED, while the rest of the Regulation replicates the GDPR provisions. And only Chapter IX, together with Article 3 on definitions, applies to EU law enforcement agencies when processing operational personal data.

1.5. Conclusion

The EU data protection rules for law enforcement evolved from a fragmented and unreadable landscape under the Maastricht regime to the authoritative leadership of the LED in the Lisbon era. The LED achieved an unprecedented level of completeness, thoroughness, and harmonisation in Member States, where its transposition has been completed. What is more, the LED succeeded where its predecessor FD failed: the LED rules kick-started the harmonisation of data protection rules in the entire former third pillar of the EU. By doing so, the LED became the golden standard for data protection in law enforcement.

([25]) Marquenie, T., 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', *Computer Law & Security Review*, Vol. 33, No. 3, p. 325.

([26]) Processing of operational personal data by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 Of Title V Of Part Three TFEU.

2. AFSJ as an interconnected ecosystem for border management

2.1. Interoperability of AFSJ databases and EU Large-Scale IT Systems

The concept to create an interconnected ecosystem of EU databases to make better use of the information stored in separate systems dates back to 2005, when the Commission called for enhanced synergies among European databases in the area of Justice and Home Affairs ([27]). The Communication followed the Hague Programme, and the 'principle of availability', in a period that marked the beginning of a move towards a more integrated management of the EU's external borders ([28]). The control of the external borders to better manage migration flows, to contribute to the prevention of terrorism ([29]) and organised crime led to a general rise in security measures, including the introduction of biometric passports ([30]), the establishment of the Frontex Agency ([31]) and the abovementioned intention to improve the use of information stored in separate EU databases.

At that time, the operational databases were the Visa Information System ('VIS'), Eurodac and the Schengen Information System ('SIS'). These large-scale databases were set up at EU level to deal with matters related to the administration of Schengen visas, asylum applications and the EU's internal security respectively. Each of these databases was established to serve a specific purpose, each having associated retention periods for information stored and strict conditions for competent authorities to access the data. Interoperability, on the other hand, refers to the functionality of enabling the sharing of information between different systems, creating new processing operations and additional access opportunities for relevant authorities ([32]). Already in 2006, the EDPS warned that interoperability would risk paving the way for subsequent calls to diminish legal requirements limiting the use of the EU databases, making it easier to utilize the data stored therein and, therefore, would involve political choices rather that purely technical ones ([33]).

([27]) European Commission, Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final.

([28]) European Commission, Communication from the Commission to the Council and the European Parliament, towards Integrated Management of the External Borders of the Member States of the European Union, COM(2002) 233 final, p. 2.

([29]) In this context, the Madrid and London bombings in 2004 and 2005 respectively.

([30]) Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, 29.12.2004, p. 1.

([31]) Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25.11.2004, p. 1.

([32]) EDPS work on interoperability. Also see: EDPS, Comments on the Communication of the Commission on interoperability of European databases, issued on 10 March 2006, p. 2.

([33]) *Ibid.*

The next steps in the EU's integrated border management ([34]) materialised in 2013, when the Smart Borders Package was proposed. The package consisted of an Entry/Exit System to replace the procedure of manually stamping the passports of Third Country Nationals (TCNs) when crossing Schengen borders and a Registered Traveller Programme ('RTP') to give frequent third-country travellers the option of pre-screening ([35]). In his Opinion on the Smart Borders Package, the EDPS underlined that the question of necessity should be analysed in the broader context of large scale IT systems ([36]), which should only be created to support an established EU policy ([37]). In 2015, the proposals were withdrawn because of significant concerns voiced by the co-legislators and the Commission announced their revision ([38]).

However, in 2016, following the so-called migration crisis and terrorist attacks in various Member States, two new proposals for an Entry Exit System ([39]) and for a European Travel Information and Authorisation System ('ETIAS') ([40]) were introduced. While both systems' primary objective was of a border control nature, competent law enforcement authorities were granted access to stored information under certain conditions. Already at that time, the EDPS observed that migration management and security purposes were increasingly associated in the context of access to existing and systems for law enforcement purposes or extending the competences of existing bodies, such as Frontex ([41]).

Simultaneously, amendments to the Eurodac (in May 2016) and the SIS (in December 2016) were proposed and, in 2017, a proposal on the European Criminal Records Information System for third country nationals and stateless persons ('ECRIS-TCN') followed.

([34]) See European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Preparing the next steps in border management in the European Union, COM(2008) 69 final.

([35]) European Parliament legislative train schedule, Entry/Exit System (2013 Smart Borders Package).

([36]) EDPS Opinion on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), issued on 18 July 2013, paragraph 32.

([37]) *Ibid*, paragraph 28.

([38]) European Parliament legislative train schedule, Entry/Exit System (2013 Smart Borders Package).

([39]) Proposal for a Regulation of the European Parliament and of the Council stablishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM(2016)194 final.

([40]) Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 731 final.

([41]) EDPS Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS), issued on 6 March 2017, paragraph 14.

2.2. The interoperability regulations

At the end of 2017, two regulations were proposed to establish the interoperability of the above systems and to close the alleged information gaps about travellers, visa applicants, asylum seekers and criminals. Both proposals were adopted in May 2019 ([42]).

In his Opinion on the interoperability proposals from April 2018, the EDPS called the EU legislator's decision to render the large-scale IT systems interoperable a 'point of no return' ([43]). Interoperability would fundamentally change the current architecture of AFSJ large-scale IT-systems and introduce a shift from separated silos to an interconnected framework, where personal data will be stored on a centralized basis. It will provide a search infrastructure to simultaneously query the underlying databases, and will allow direct access by designated national authorities such as border guards, visa and asylum authorities, and law enforcement authorities, as well as EU Agencies such as Frontex and Europol. In addition, the system stores the biometric data from the underlying databases and serves as a platform to automatically match them to carry out a risk assessment of all third country nationals who (intend to) enter the Schengen Area ([44]).

In the meantime, because the interoperable framework required amendments to the underlying systems and in order to make them interoperable amongst each other, changes were proposed by introducing consequential amendments ([45]),

([42]) Regulation (EU) 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135, 22.5.2019, p. 27 and Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019, p. 85.

([43]) EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, issued on 16 April 2018, p. 3.

([44]) Quintel, T., *Data Protection, Migration and Border Control. The GDPR, the Law Enforcement Directive and Beyond*, Hart Publishing, 2022.

([45]) Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System, OJ L 248, 13.7.2021, p. 1; Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System, OJ L 248, 13.7.2021, p. 11; Regulation (EU) 2021/1151 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the European Travel Information and Authorisation System, OJ L 249, 14.7.2021, p. 7; and Regulation (EU) 2021/1152 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861 and (EU) 2019/817 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the European Travel Information and Authorisation System, OJ L 249, 14.7.2021, p. 15.

an adjusted Eurodac proposal ([46]) and numerous implementing and delegated acts. The EDPS issued formal comments for approximately 70 of those acts, shedding light on some of the issues such as the ETIAS watchlist ([47]), comparisons of datasets in the interoperable system against Interpol and Europol data ([48]), questions of data ownership and log security ([49]), or data inaccuracies in the system ([50]).

While the date for the operationalisation of the complete interoperable system is anticipated for mid-2024 until the end of 2026 ([51]), it is important to recognise that interoperability in its current form is by no means a final product, but rather an extendable toolbox, as the EDPS predicted already in 2018 ([52]). In that light, additional legislation was proposed to expand the interoperable system's functionalities. The Prüm II Regulation, which will connect the interoperable framework with an infrastructure to be utilised for automated searches of police records indexes ([53]), or the screening regulation that will introduce a pre-screening for (almost) anyone arriving at an EU borders irregularly and for which a political agreement was found in December 2023 ([54]) are only two examples of such expansion.

([46]) Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818, COM(2020) 614 final.

([47]) EDPS, Formal comments on the Draft Commission Implementing Decision defining the technical specification of the ETIAS watchlist and of the assessment tool, issued on 22 January 2021.

([48]) EDPS, Formal comments on the draft Commission Delegated Decision on supplementing Regulation (EC) No 767/2008 and of the Council concerning the Visa Information System (VIS) and the exchange of information between Member States on short-stay visas, long-stay visas and residence permits with a manual laying down the procedures and rules necessary for queries, verifications and assessments, issued on 13 September 2023.

([49]) EDPS, Formal comments on the draft Commission Implementing Decision on the rules on the operation of the public website and the app for mobile devices, pursuant to Article 16(10) of Regulation (EU) 2018/1240 of the European Parliament and of the Council, issued on 4 September 2020.

([50]) EDPS, Formal comments on the draft Commission Implementing Decision on measures for accessing, amending, erasing and advance erasing of data in the ETIAS Central System, issued on 22 January 2021.

([51]) European Council/Council of the European Union, IT systems to fight crime and secure EU borders. While the upgraded version of the SIS became operational in March 2023, the EES will be ready to enter into operation in autumn 2024 and ETIAS will be operational by spring 2025, according to an updated plan agreed upon by the JHA Council in October 2023. With regard to Eurodac and VIS, the operationalisation of their amended versions and inclusion in the interoperability framework is not yet clear, as parts of the VIS amendments depend on a Commission decision and the amendments regarding Eurodac were only agreed by the co-legislators in December 2023. Personal data contained in the SIS III will not be directly linked to the interoperability components, as the SIS III also includes the personal data of EU citizens, while the interoperable system is to only include the personal data of TCNs. Nevertheless, personal data in the SIS III will be searchable via the ESP.

([52]) EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, issued on 16 April 2018, p. 20, paragraph 144.

([53]) European Council/Council of the European Union, Council and EU Parliament reach deal to advance police cooperation in Europe, Press release. See EDPS Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation ("Prüm II"), issued on 2 March 2022.

([54]) European Commission, Historic agreement reached today by the European Parliament and Council on the Pact on Migration and Asylum. See: EDPS Opinion 9/2020 on the New Pact on Migration and Asylum, issued on 30 November 2020.

A. Purpose limitation

The complexity that the interoperability regulations add to the already complicated system of EU databases, the intertwinedness that new forms of cooperation between authorities at national and EU level will bring about, and the broadened mandate that EU Agencies obtained to process personal data of third country nationals for a variety of purposes, stands at odds with some of the most important data protection principles. Already in 2017, the EDPS argued that the EU legislator appeared to follow an increasing trend of addressing security and migration management purposes jointly, without taking into account the substantial distinctions between these two policy areas. This would have a significant impact on the right to the protection of personal data, since various kinds of data, collected initially for very different purposes, would become accessible to a broader range of public authorities ([55]). According to the EDPS, interoperability must be implemented with due respect for data protection principles and in particular the purpose limitation principle ([56]), as a clear definition of the purposes is not only essential to ascertain what data are needed for a specific processing operation and to achieve an objective, but also to help establish safeguards and in assessing both necessity and proportionality of such processing operation ([57]). General policy objectives such as streamlining law enforcement access to non-law enforcement information systems or providing a solution to detect and combat identity fraud would not necessarily equal purposes of data processing under data protection law ([58]).

By streamlining law enforcement access to non-law enforcement databases that hold information concerning third country nationals, interoperability not only changed the initial purpose of the underlying databases more drastically than previous revisions of their founding acts. The interoperability regulations substantially elevated the ancillary objective of these databases (the fight against serious crime). Against that background, the EDPS pointed out that convincing evidence to support the necessity of Europol access to travellers' data was missing and stressed that necessity and proportionality of new schemes are to be assessed in the specific case of third country nationals who are legally visiting and entering the EU ([59]).

([55]) EDPS Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS), issued on 6 March 2017, p. 3.

([56]) EDPS, Comments on the Communication of the Commission on interoperability of European data bases, issued on 10 March 2006, p. 3.

([57]) EDPS, Reflection paper on the interoperability of information systems in the Area of Freedom, Security and Justice, issued on 17 November 2017, paragraph 16.

([58]) *Ibid*, paragraphs 12 and 13.

([59]) EDPS Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS), issued on 6 March 2017, paragraph 119.

B. Actors and roles

The growing involvement of EU Agencies in the processing of personal data of third country nationals may also raise concerns regarding the data protection rules applicable to EU Agencies, as certain provisions leave room for interpretation. For instance, the establishment of new systems and the forthcoming operationalisation of interoperability will add changes regarding the way in which Frontex may access the operational and forthcoming databases. In that regard, the EDPS made clear that any activity by Frontex in relation to the prevention, detection and investigation of criminal offences is secondary and should be carried out primarily as a form of support to Europol, Eurojust and Member States' competent authorities ([60]).

Additional EU Agencies such as Europol, eu-LISA and, to a more limited extend, Eurojust and the European Union Agency for Asylum ('EUAA'), will be granted access to the personal data of third country nationals stored in the interoperability components, which also raises questions related to joint control. This was already highlighted by the EDPS in 2017, when he recommended a more accurate description of the division of roles between Frontex and eu-LISA, including their designation as joint controllers where appropriate ([61]). Most importantly, the EDPS recalled that the concept of controllership must be based on a factual analysis. For that reason, he recommended clearly designating joint controllers, each with their clearly defined tasks and responsibilities ([62]).

The inclusion of the EU-level Agencies is also relevant because discrepancies may arise in the context of interoperability where systematic data exchanges take place between actors at different levels that apply different data protection regimes. Furthermore, certain EU Agencies increasingly collect and generate personal data themselves through their own data analyses. On the one hand, this makes it difficult for data subjects to comprehend how their personal data are processed. On the other hand, the interoperable data flows contribute to challenges that already exist with regard to supervision.

([60]) EDPS Supervisory Opinion on the rules on processing of operational personal data by the European Border and Coast Guard Agency (Frontex) (Case 2022-0147), issued on 7 June 2022, paragraph 15.

([61]) EDPS Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS), issued on 6 March 2017, paragraph 87.

([62]) EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, issued on 16 April 2018, paragraph 107. Also see EDPS, Formal comments on the draft Commission Implementing Decision on the rules on the operation of the public website and the app for mobile devices, pursuant to Article 16(10) of Regulation (EU) 2018/1240 of the European Parliament and of the Council, issued on 4 September 2020.

C. Data subject rights and supervision

While understanding the interoperable system is already challenging for experts working in the field of EU databases, one can only imagine the difficulties that third country nationals would experience trying to understand the interconnected regime of databases, how to exercise their rights, or what negative consequences they might face due to wrong matches in the system. This could lead to a situation where the increased connectivity of EU databases, allowing more authorities to have access to the systems, while those whose data are stored in the databases might be less and less capable of understanding and exercising their data subject rights ([63]).

Therefore, compliance with the data protection principles to ensure clearly defined processing activities that are subject to strict supervision are of utmost importance to uphold fundamental rights standards.

However, where data exchanges take place at different levels and between different agencies that apply different data protection regimes and are subject to different rules on supervision, the powers of the EDPS may be undermined once another authority subsequently processes certain operational personal data. Not only will it be more challenging for national DPAs and the EDPS to supervise the increased data exchanges. In addition, the high standards that exist under one data protection instrument may be undermined where another data protection regime includes different, less strict rules, which could be circumvented by exchanging those data.

Therefore, supervisory authorities should be able to *follow* data flows between the different authorities instead of considering each specific controller separately. In order to achieve an effective supervision of the complex network of different actors, closer cooperation between national supervisory authorities and the EDPS is of utmost importance to better comprehend the steps behind certain decision-making processes and to handle data subject requests effectively ([64]). With the blurred lines between migration and security leading to the obscuring of different purposes and the dilution of responsibilities between different actors, it will be challenging for supervisory authorities to get a concrete picture of processing activities and hence, the risks involved for data subjects. Just like the merging of previously disconnected AFSJ databases under the interoperability regulations, and the increased exchanges of personal data between different authorities, supervisory authorities should gain a better overview of the connected systems to be able to provide more effective supervision ([65]).

([63]) Quintel, T., Why should we care about the Privacy of Asylum Seekers?, *Migration Policy Centre blog*.

([64]) Quintel, T., *Data Protection, Migration and Border Control. The GDPR, the Law Enforcement Directive and Beyond*, op. cit. (footnote 44), p. 87.

([65]) Coudert, F., in the panel 'Checks and balances in the AFSJ: rethinking governance', Computers, Privacy and Data Protection Conference 2019.

2.3. The important role of the EDPS

Interoperability will drastically change the way in which competent authorities can access, retrieve and process the personal data stored in the EU databases. The interoperable system abandons the traditional silo-based approach, pursuant to which these databases were set up according to specific purposes, with precise time limits and strict access conditions. The proliferation of new systems and the interoperability framework signify a paradigm shift by streamlining law enforcement access to non-law enforcement databases and abolishing important safeguards that were inherent when initially setting up the operational systems.

In a world where more and more data are being used to analyse the movement of individuals, connecting information from different sources on a systematic basis may be a logical step so as to carry out such analyses more effectively. In addition, interoperable databases allow immediate data exchanges that are intended to facilitate and streamline decision-making by digital means ([66]). However, the question is whether this is done in the right way and in a necessary and proportionate manner. Importantly, these developments must be subject to control by an independent authority, in line with the EU Charter.

3. Supervising the Area of Freedom, Security and Justice

3.1. Ensuring respect for fundamental rights and freedoms while guaranteeing EU public security

Since the Stockholm Program, the AFSJ was conceived as a single area in which fundamental rights and freedoms are protected ([67]). Respect for the human person and human dignity and for the other rights set out in the Charter of Fundamental Rights of the European Union and the European Convention for the protection of Human Rights and fundamental freedoms were identified as EU core values. This was reflected in secondary legislation, where multiple references were made to the need of the EU Agencies and Bodies to perform their task in full respect with fundamental rights ([68]).

([66]) See EDPS, Reflection paper on the interoperability of information systems in the Area of Freedom, Security and Justice, issued on 17 November 2017.

([67]) The Stockholm Programme – An open and secure Europe serving and protecting citizens, OJ C 115, 4.5.2010, p. 1.

([68]) See for example Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, OJ L 295, 14.11.2019, p. 1, where the reference to fundamental rights appears more than 200 times.

The EDPS is tasked with monitoring and ensuring compliance with all provisions concerning data protection. According to Article 1 of the EUDPR, this Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies. By doing so, it protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The EDPS thus participates to operationalising the protection of fundamental rights of individuals in the AFSJ by ensuring data protection compliance.

AFSJ Agencies, Bodies and Offices ([69]), while all tasked with the protection of EU public security in the broad sense (with the exception of the EU Agency for Asylum), operate in different fields whose specificities should be taken into account (law enforcement, criminal justice, border management). Their data processing activities all have a high impact on individuals' rights and freedoms such as the right to fair trial, the right to non-discrimination or the right to asylum and relate to individuals who are in a vulnerable position (people on the move, people under criminal investigations).

When supervising the AFSJ, the EDPS must take into account these different realities, the different fundamental rights impacted by personal data processing activities and the need to protect other public order interests. The use of supervisory powers will rarely be limited to a literal implementation of the law and thus implies a certain degree of balancing between the different interests at stake. The EDPS performs such balancing exercise in view of the greater goal of protecting individuals' dignity and freedom.

To realise its mission, the EDPS is given a supervisory toolbox, which includes advisory, investigative and corrective powers. The granting of investigative and corrective powers to the EDPS, when instated as supervisor of AFSJ Agencies, Bodies and Offices, has marked a turning point in the supervision model of these Agencies, which were previously subject to the supervision by Joint Supervisory Bodies composed of representatives of national data protection authorities, with no corrective powers. The EDPS is tasked not only with providing advice to controllers and data subjects but also with monitoring and enforcing the data protection provisions where a breach is identified. This aligns the position of the EDPS with national supervisory authorities under the LED and with the general data protection regime under the GDPR and the EUDPR.

([69]) AFSJ Agencies, Bodies and Offices refer to the European Union Agency for Law Enforcement Cooperation ('Europol'), European Union Agency for Criminal Justice Cooperation ('Eurojust'), the European Public Prosecutor's Office ('EPPO'), the European Border and Coast Guard ('Frontex'), the European Union Agency for Asylum ('EUAA') and the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice ('eu-LISA').

Another specificity for the supervision of the AFSJ comes from the fact that national and EU levels are closely intertwined, resulting in complex data flows where personal data are collected at national level to be further shared with Agencies, Bodies and Offices. These, in turn, enrich and further share these data to competent authorities at both EU and national levels. All these authorities are subject to different legal frameworks and to different supervisory authorities. It thus appears paramount that for the supervision to be efficient, the EDPS and national supervisory authorities must closely cooperate, adding another layer of complexity.

Since 2017, the EDPS has progressively taken up the mantle of its new role of supervisor of AFSJ Agencies, Bodies and Offices. In May 2017, the EDPS became the supervisor of Europol. In 2020, it gained new supervisory powers over Eurojust and EPPO, while the reform of the Frontex Regulation in 2019 ([70]) substantially transformed the Agency from a merely supportive role to a more active role in the EU Integrated Border Management continuum, and the large-scale deployment of Standing Corps on the ground, calling for a new type of supervision. The EDPS took stock of this evolution and highlighted in its Strategy for 2020-2024 the challenges that the patchwork of measures in the areas of police and judicial cooperation and border management was creating for its supervisory and enforcement powers ([71]). In order to address this challenge, the EDPS committed to identify discrepancies in the standards of data protection within EU law in the AFSJ and to enforce the rules consistently as a way to actively promote justice and the rule of law and a vision of digitalisation that enables us to value and respect all individuals. In 2021, the EDPS decided to create a dedicated Sector within the Supervision & Enforcement Unit, tasked with monitoring this Area.

The past five years have been devoted to establishing the EDPS in this new role of supervisor of AFSJ Agencies, Bodies and Offices, building a strong expertise in the field, putting the emphasis on cooperation with the Agencies and Bodies, in particular with their Data Protection Officers ('DPOs'), but also enforcing the law where necessary. To that end, efforts have concentrated on three main lines: 1) shedding light on an opaque environment through on-site visits, audits and providing advice; 2) monitoring and enforcing the law in case of breach; 3) fostering coordinated supervision with national supervisory bodies to ensure an efficient end-to-end supervision.

([70]) Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, OJ L 295, 14.11.2019, p. 1.

([71]) EDPS Strategy 2020-2024: Shaping a Safer Digital Future, issued on 30 June 2020.

3.2. Shedding light on an opaque environment

The first challenge posed by the supervision of personal processing by AFSJ Agencies, Bodies and Offices is to monitor an area that has long operated under a high level of opacity due to the imperative to protect EU public security. One of the first missions of the EDPS is thus to lift the veil of opacity in order to be able to advise about compliance with the data protection framework and alert about data processing activities with a high impact on individuals' rights and freedoms. By doing so, the EDPS is also contributing to the societal debate by shedding light, where it is able to do so, on ongoing data processing activities that are of key public concern and central to ongoing discussions surrounding the evolution of privacy and its relationship vis-a-vis other public interests.

To that end, the EDPS has been using his advisory powers, allowing him to provide advice to controllers and data subjects on compliance with the applicable data protection provisions. This advisory function allows the EDPS to support AFSJ Agencies, Bodies and Offices and to contribute to the difficult task of upholding fundamental rights without jeopardising the EU public security interest.

Three supervisory tools are at EDPS disposal to achieve this goal: audits which are meant to obtain knowledge about how an EU Agency, Body or Office is implementing data protection provisions in a specific processing activity or area (e.g. processing of data about minors or of biometric data) and formulate recommendations to ensure a higher level of compliance; prior consultations where the EDPS is tasked by the legislator to assess compliance of the processing and in particular of the risks for the protection of operational personal data of the data subject and of the related safeguards of processing operations with higher impact for data subjects and provide written advice to the controller; and the possibility to issue supervisory opinions, either ex-officio or upon request of the controller, on specific issues of interpretation where the EDPS advises about compliance with the data protection framework. In addition, the EDPS actively engages in a regular and constructive dialogue with the Data Protection Officers of AFSJ Agencies, Bodies and Offices, in order to support them in raising their overall level of compliance. This advisory function also allows the EDPS to get a better understanding of the data processing activities of the Agencies and to alert about risks to data subjects at an early stage of the processing.

In that capacity, the EDPS has conducted, together with national Supervisory Authorities, annual audits of Europol since 2017, covering a broad range of topics going from the processing of data of minors, to the processing of data linked to migrant smuggling or of PNR data and one audit of Eurojust, EPPO and Frontex.

The EDPS has also issued 45 opinions on the basis of prior consultations, giving advice on topics such as the use of machine learning pre-trained models ([72]), facial recognition software ([73]), or the use of cloud services ([74]) by Europol or on the set up of the war crime module by Eurojust ([75]).

Finally, the EDPS issued 59 opinions based on consultations, such as on the scope of searches in the context of the exercise of the right of access by Europol – in particular in view of the processing of large and unstructured datasets ([76]); or the use of derogations for international transfers in the context of returns by Frontex ([77]).

These opinions contribute to not only guide controllers in operationalising the protection of fundamental rights in their tasks but also allow the EDPS and the controllers to engage in a constructive dialogue, which should result in the adaptation of the circumstances that gave rise to a conflict of interests or a conflict of rights. This proactive scrutinising and advising role is also important in view of the vulnerable position of the individuals affected by the processing (migrants, asylum seekers, those under the scope of law enforcement activities). In this field, compliance issues are less likely to come to the EDPS' attention from the bottom-up, e.g. through complaints.

3.3. Investigating and enforcing

In addition to advisory powers, and to the difference from the previous supervisory model in place for the AFSJ, the EDPS was also given investigative and corrective powers. For the EDPS to wield investigation and enforcement powers in the AFSJ area confers on this institution a very concrete role in operationalising fundamental rights in this area.

Indication of risks of non-compliance can come from different sources: directly from supervisory activities such as audits or interactions with data controllers, from information provided by the public (press articles or brought to the direct attention to the EDPS by the public), or from the investigation of complaints.

([72]) EDPS Supervisory Opinion on a Prior Consultation requested by Europol on the development and use of machine learning models for operational analysis, issued on 5 March 2021.

([73]) EDPS Supervisory Opinion on a prior consultation requested by Europol on a Face Recognition Solution, issued on 20 December 2023.

([74]) EDPS Supervisory Opinion of 27 June 2022 on a prior consultation requested by Europol on the European Platform for takedown of illegal content online (Plateforme Européenne de Retraits des Contenus illégaux sur Internet – 'PERCI'), issued on 27 June 2022.

([75]) EDPS Supervisory Opinions of 14 December 2022 and 9 February 2023 on two prior consultations requested by Eurojust on the implementation of Regulation (EU) 2022/838 regarding the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences (not published).

([76]) EDPS Supervisory Opinion on Europol's Procedure to Handle Data Subject Access requests under Article 36 & 37 of Regulation (EU) 2016/7941 ('the Europol Regulation'), issued on 13 December 2021.

([77]) EDPS Supervisory Opinion of 20 December 2021 on International Data Transfers by Frontex in the Context of Return Operations, issued on 20 December 2022.

The EDPS launched a total of 27 investigations (including pre-investigations or enquiries) and used nine times his corrective powers in the AFSJ alone. The EDPS also investigated 19 complaints against Europol.

The EDPS for instance investigated the use of Palantir software by Europol in 2018, where the 2017 Europol inspection reVealed potential difficulties in complying with the provisions applying to the processing of sensitive data and specific categories of data subjects, who should be identified and labelled as such in Europol systems. The EDPS also launched two investigations based on the findings of the 2022 audit of Frontex on the processing of personal data in the context of joint operations. The collection of personal data from debriefing interviews raised specific matters of concern with regard to the nature of the data collected during these interviews and their further exchange with Europol. A first concern comes from the high vulnerability of the individuals targeted for data collection, and the apparent lack of foreseeability for individuals from whom data is collected. Other concerns stem from the lack of appropriate procedural safeguards, that are coherent with the status of interviewees as detainees in some countries and the law enforcement nature of the information and personal data provided, and that would protect individuals concerned from adverse and disproportionate risks to their fundamental rights. Both investigations are ongoing at the time of writing.

Other investigations were prompted by information provided by the public. In 2020, the EDPS enquired about the alleged use of Clearview.AI by Europol, when a press article reported a use of this software by the Swedish police, following a demonstration of the software performed during a workshop held at Europol. The potential use of Clearview AI, a controversial face recognition software relying on the scrapping of images from public sources by an EU law enforcement agency was considered as sufficiently serious for EU citizens as to motivate an enquiry. The EDPS decided to issue an ex-officio supervisory opinion with a series of recommendations ([78]). More recently, in 2023, two inquiries were opened against Frontex on the basis of information provided by, in the first instance, a journalist who learned in the context of a request for access to documents that Frontex might be processing personal data about NGOs staff members in their debriefing reports, which could be further shared with Europol. In the second instance, the EDPS enquired about the alleged photographing by Frontex border guards of people on the move when intercepted irregularly crossing EU borders on the basis of information provided by an NGO who was concerned that such practices could be unlawful.

The use of EDPS enforcement powers can also be prompted by consultations from EU Agencies, Bodies or Offices. This was the case when the EDPS was consulted on the set up of a new centralised FIU.net system to be hosted at Europol in 2018. FIU.net is a decentralised computer network that provides information exchange between the Financial Intelligence Units ('FIUs') of the

([78]) EDPS Supervisory Opinion on the possibility to use Clearview AI and similar services at Europol, issued on 29 March 2021.

European Union. FIUs are central national units responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicated offences and terrorist financing. They collect financial intelligence and as such they act before the start of any preliminary proceedings or criminal investigation. The EDPS took into account the legislator's will to keep financial intelligence tasks separated from financial criminal investigations as they pursue different purposes. In this case, and for the first time, the EDPS used his corrective powers and issued a ban of all processing by Europol of data related to individuals who are not classed as 'suspects' under the applicable national criminal procedure law in the context of the technical administration of FIU.net, as this would run counter to the provisions of the Europol Regulation ([79]).

In 2020, on the basis of information provided by Europol on the growing use of the Computer Forensic Network for operational analysis purposes, the EDPS launched a formal investigation on the processing by Europol of 'large datasets' received as contributions from Member States, from other operational partners or collected in the context of open source intelligence activities. This new practice reVealed a substantial change in how Member States and Europol cooperate. Member States have increasingly been sending larger volumes of unstructured data to Europol, due to the change in nature of the data collected at national level in the context of criminal investigations and criminal intelligence operations, growingly moving from targeted to indiscriminate data collection.

The evolution of Europol's personal data processing activities towards Big Data Analytics raised concerns linked to the compliance with the Europol's data protection framework, in particular with the principles of purpose limitation, data minimisation, data accuracy, storage limitation, with the impact of potential data breaches, location of storage, general management and information security. The EDPS took issue with the risks posed for data subjects where large amounts of personal data are stored on Europol systems for several years. The processing of data about individuals in an EU law enforcement database can have deep consequences on those involved. Without a proper implementation of the data minimisation principle and the specific safeguards contained in the Europol Regulation, data subjects run the risk of wrongfully being linked to a criminal activity across the EU, with all of the potential damage for their personal and family life, freedom of movement and occupation that this entails.

On 17 September 2020, the EDPS admonished Europol and asked them to devise mitigation measures that can both reduce the risks for data subjects and ensure that Europol does not lose its operational capabilities ([80]). The EDPS also invited Europol to provide an action plan to address the admonishment within two months and to report on the measures taken within six months. Despite considerable improvement in the management by Europol of these

([79]) EDPS Decision relating to the technical administration of FIU.net by Europol, 19 December 2019.
([80]) EDPS Decision relating to EDPS own inquiry on Europol's big data challenge, 17 September 2020.

large datasets, the EDPS and Europol diverged in their interpretation of the law as regards the obligation to delete large datasets '*lacking a Data Subject Categorisation*'. These refer to datasets which, because of their characteristics and notably their size, did not undergo the data classification process as provided for in the Europol Regulation (the so-called 'data subjects categorisation') and extraction of data categories according to Annex II B of the Europol Regulation and the Opening Decision Orders, which specify, for each operational analysis project, the categories of personal data and categories of data subjects that can be processed according to Article 18(3)(a) of the Europol Regulation. On 3 January 2022, the EDPS issued an order to delete data processed in breach of the Europol Regulation ([81]).

3.4. Supervising complex data flows

Another important task of the EDPS is to ensure efficient supervision, which in the field of the AFSJ requires to put in place coordinated supervision with national data protection authorities. The difficulty to achieve an efficient supervision, understood as of the whole life cycle or end-to-end supervision, from data collection to data deletion, lies in the cross-border and multi-level elements. Controllers processing the same personal data are subject to different legal frameworks and supervisory authorities. This thus requires an increased and closer cooperation between the EDPS and national data protection authorities.

This cross-border element is obvious in the investigation of data subjects' complaints, for instance against Europol or Eurojust, where the specific Regulations impose an obligation to check the lawfulness of the processing both to the EDPS and to national supervisory authorities. The need for coordinated supervision was further evidenced in the context of the aforementioned FIU.net case, which revolved around the definition of 'suspect', a concept proper to national criminal laws. The EDPS therefore first consulted the Europol Cooperation Board and based his decision on the opinion delivered by this body. Another example of the EDPS' efforts to intensify joined-up supervision in the AFSJ was the coordinated action launched in 2020 to ensure that the processing of data about minors under 15 labelled as suspects complies with national laws and the Europol Regulation. In that case, it was key to ensure that only data about individuals who have reached the minimal age of criminal responsibility are shared with Europol, an assessment that can only be made at national level in lack of a pan-European framework. This coordinated action was then taken over by the EDPB, under the Coordinated Supervisory Committee. Only a coordinated supervision action could ensure that there is no gap created by multi-level cooperation, gaps which would leave vulnerable individuals exposed to very high risks. This ensure that accountability and responsibility for processing is properly attributed.

([81]) EDPS Decision on the retention by Europol of datasets lacking data subjects categorisation, notified on 3 January 2022.

The EDPS has also put in place bilateral cooperation agreements, under Article 61 EUDPR. In 2023, the EDPS cooperated with the Hellenic Data Protection Authority (DPA) in order to carry onsite checks in the hotspot in Lesvos where Frontex collaborates with national authorities in the context of joint operations, collecting information about migrants. The EDPS, as competent supervisory authority over Frontex checked processing activities performed by the Agency at the hotspot, while the Hellenic DPA checked processing activities performed by national authorities. This allowed to remove any blind spot and have an overview of all personal data processing activities taking place in the context of joint operations.

In addition to the interconnection of national and EU levels, EU Agencies, Bodies and Offices are also asked to foster their cooperation and increase personal data exchanges in the performance of their tasks. This has led the EDPS not to limit its supervisory activities to one Agency, but to follow the data. For instance, in the context of the ongoing investigation into the exchange of debriefing reports between Frontex and Europol, the EDPS decided to conduct onsite checks at Europol to understand how the information is further processed after it is shared by Frontex ([82]).

3.5. Challenges ahead

In view of the successive legislative reforms in the AFSJ, two main challenges arises in terms of supervision.

First, in order to address the increasing cooperation between AFSJ Agencies, Bodies and Offices as well as the cooperation between national and EU level with the development of the interoperability framework ([83]), under the proposed API Regulation ([84]), or the exchange of biometrics under the proposed Prüm II Regulation ([85]), the EDPS should adopt a holistic approach to the supervision of the AFSJ Agencies, Bodies and Offices and strengthen mechanisms of coordinated supervision. The supervision of AFSJ Agencies, Bodies and Offices, to be efficient, cannot anymore be predicated on the basis of a merely organic approach, i.e. one that focuses on the processing activities of one controller (one EU Agency or body). Instead, supervision should become systemic, i.e. one that embraces the whole system and not only look at what one actor of the

([82]) EDPS Wojciech Wiewiórowski's speech at the 13th meeting of the Joint Parliamentary Scrutiny Group on Europol, 21 September 2023.

([83]) Regulation (EU) 2019/817 and Regulation (EU) 2019/818.

([84]) Proposal for a Regulation of the European Parliament and of the Council On the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC, COM(2022) 729 final; Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818, COM(2022) 731 final.

([85]) Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM(2021) 784 final.

system is doing. As mentioned above, data protection authorities should 'Follow the data' and be able to supervise the data life cycle throughout the different systems (from creation to destruction), even if different actors are involved. In that sense, the EDPS made specific recommendations for the introduction of clear procedural rules to streamline this cooperation in its contribution to GDPR procedural harmonisation ([86]).

Second, AFSJ Agencies, Bodies and Offices are increasingly processing large and unstructured datasets, leveraging the need to use AI to be able to make sense of the data and be more efficient in the performance of their tasks. This will require the EDPS to embrace even more decisively an approach to data protection supervision that reflects the spirit of Article 1 EUDPR. As far as AI heavily relies on personal data for training, development and testing, data protection becomes the first line of defence for other fundamental rights. This also means that the EDPS should further develop its cooperation with other supervisory or advisory bodies in the field of fundamental rights, such as the Fundamental Rights Agency or the Ombudsman, and act together with these bodies to ensure the protection of the full spectrum of fundamental rights. A first example of such broader approach to the protection of fundamental rights is taking place in the context of the ETIAS Fundamental Rights Guidance Board, which gathers representatives from the EDPS, the EDPB, the Fundamental Rights Agency, Frontex Fundamental Rights Office and Frontex Consultative Committee.

([86]) EPDS, EDPS contribution in the context of the Commission initiative to further specify procedural rules relating to the enforcement of the General Data Protection Regulation, 25 April 2023; EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, issued on 19 September 2023.

11

Eurojust evidence database relating to genocide, crimes against humanity, war crimes and related criminal offences

Diana Alonso Blas, LL.M.

Eurojust evidence database relating to genocide, crimes against humanity, war crimes and related criminal offences

Diana Alonso Blas, LL.M. (*)

Shortly after the start of the Russian military aggression against Ukraine, the European Union took urgent action to amend the Eurojust mandate to allow the preservation, analysis and storage of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences by Eurojust in a new 'automated data management and storage facility'. The implementation of this amendment of the Eurojust Regulation raises important data protection challenges, given the sensitivity of the operational data at stake as well as the urgency of the actions to be taken. Eurojust is addressing these issues in close consultation with the EDPS.

1. War on European ground: the new Eurojust mandate

On 24 February 2022 the Russian Federation began a military aggression against Ukraine ([1]). Regrettably enough, there is a reasonable basis to believe that crimes against humanity and war crimes have been and are being committed in Ukraine in the context of the current hostilities. In view of the gravity of the situation, the European Union decided to take all necessary measures, as a matter of urgency, to ensure that those who commit crimes against humanity

(*) Head of Data Protection Office/Data Protection Officer at Eurojust.

([1]) See Recital 3 of Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 amending Regulation (EU) 2018/1727 as regards the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences, OJ L 148, 31.5.2022, p.1.

and war crimes in Ukraine are held responsible ([2]). This included an exceptionally quick amendment of the Eurojust Regulation ('EJR') ([3]) to extend the mandate of Eurojust.

Eurojust is given a central role in the context of the processing of war crimes data due its expertise and experience to support investigations and prosecutions of cross-border crimes, including genocide, crimes against humanity, war crimes and related criminal offences and the fact that such support includes the preservation, analysis and storage of evidence as far as its admissibility before courts and its reliability are concerned ([4]). Additionally, Eurojust had concluded a cooperation agreement with Ukraine on 27 June 2016 ([5]) and, in accordance with that agreement, Ukraine has posted a liaison prosecutor to Eurojust to facilitate the cooperation between Eurojust and Ukraine ([6]).

The amendment to the EJR by Regulation 2022/838 included three main elements.

1. The mandate of Eurojust as defined in Article 4(1) of the EJR is extended with letter (j) adding that Eurojust shall '*support Member States' action in combating genocide, crimes against humanity, war crimes and related criminal offences, including by preserving, analysing, and storing evidence related to those crimes and related criminal offences and enabling the exchange of such evidence*'. The amended EJR does not, however, aim at changing the supportive role of Eurojust in relation to national authorities ([7]), as it is underlined by the EDPS in Opinion 6/2022 ([8]). Consequently, the new point (j) in Article 4(1) of the EJR, and in particular the 'collection of evidence' by Eurojust, should be interpreted strictly in accordance with Article 85 TFEU, including paragraph 2 thereof, according to which '*formal acts of judicial procedure shall be carried out by the competent national officials*'.
2. Annex II of the EJR, which enumerates the categories of personal data referred to in Article 27, is amended to include some additional categories of data which are considered necessary in the context of

([2]) See Recital 4 of Regulation (EU) 2022/838.

([3]) Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation ('Eurojust'), and replacing and repealing the Council Decision 2002/187/JHA, OJ L 295, 21.11.2018, p.138. The urgency of the situation was put forward as a reason to justify the entry into force of the amended Regulation the day following that of its publication in the Official Journal (30 May 2022).

([4]) See Recital 10 of Regulation (EU) 2022/838.

([5]) European Union Agency for Criminal Justice Cooperation, Agreement on cooperation between Eurojust and Ukraine, 27 June 2016.

([6]) See Recital 5 of Regulation (EU) 2022/838.

([7]) See COM (2022) 187 final, p. 2.

([8]) EDPS Opinion 6/2022 on the Proposal for a Regulation of the European Parliament and the Council amending Regulation (EU) 2018/1727 of the European Parliament and the Council, as regards the collection, preservation and analysis of evidence relating to genocide, crimes against humanity and war crimes at Eurojust, issued on 13 May 2022. See in particular point 11 of this opinion.

war crimes investigations such as video and audio recordings, satellite images and photographs. The EDPS did not comment on these new categories in Opinion 6/2022.

3. A new paragraph 8 is added to Article 80 of the EJR allowing a temporary derogation of Article 23 ([9]) of the EJR which establishes that '*for the processing of operational personal data, Eurojust shall not establish any automated data file other than the case management system*' ('CMS')'. Article 80(8) EJR allows the creation of an '*automated data management and storage facility*' outside of Eurojust CMS for the purpose of the performance of the operational function referred to in Article 4(1), point (j).

EDPS opinion 6/2022 makes relevant comments regarding this derogation ([10]) underlining that this derogation should be of a temporary nature and the automated data management and storage facility should be integrated into the new case management system which is expected to be established under the Proposal for a Regulation on the digital information exchange on terrorism cases ([11]). Additionally, the EDPS stressed the importance of ensuring that this new automated data management system operates in a secure technical environment, taking into account state of the art technical and organizational measures on security and data protection. The system should follow the standards of privacy by design and by default as provided by Article 85 of Chapter IX of the EUDPR ([12]).

2. Data protection safeguards

Article 80(8) of the EJR, providing for the legal basis for the processing of operational personal data linked to war crimes, genocide and related offences, also known as 'core international crimes', introduces a good number of data protection safeguards.

First of all, it is established that the automated data management and storage facility should meet the highest cybersecurity standards.

([9]) Interestingly enough, Article 80(8) of the EJR refers to Article 23(6) EJR while in fact it should refer to Article 23(7) as the text clearly aims at allowing Eurojust to create a database outside the CMS.

([10]) See EDPS Opinion 6/2022 on the Proposal for a Regulation of the European Parliament and the Council amending Regulation (EU) 2018/1727 of the European Parliament and the Council, as regards the collection, preservation and analysis of evidence relating to genocide, crimes against humanity and war crimes at Eurojust, issued on 13 May 2022, paragraphs 8-9.

([11]) This Proposal has in the meantime been published as Regulation (EU) 2023/2131 of the European Parliament and of the Council of 4 October 2023, L2131, 11.10.2023, p. 1.

([12]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

Secondly, in addition to the already existing obligations of Article 90 EUDPR, Article 80(8) EJR foresees the need to consult the EDPS via a notification of the DPO before the new '*automated data management and storage facility*' starts operation including: (a) a general description of the processing operations envisaged; (b) an assessment of the risks to the rights and freedoms of data subjects; (c) the measures envisaged to address the risks referred to in point (b); and (d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of the data subjects and other persons concerned. Given the need to proceed in a timely manner, Article 80(8) EJR requires the EDPS to provide a 'prior consultation' opinion within 2 months.

Thirdly, the data protection provisions included in the EJR and the EUDPR remain applicable insofar as they do not directly relate to the technical set-up of the CMS. This technical precision is crucial as the temporary derogation of the use of the CMS and the possibility to create a separate processing system, while foreseen as an opportunity for Eurojust, is also a big challenge in practice. It means actually that Eurojust has to put in place as a matter of urgency ([13]), a complete new processing system which should fit the needs of this new field of activity, while still complying with the extensive and robust data protection regime in place. The exclusion of the provisions linked to technical set-up of the CMS offers Eurojust the possibility to comply with the data protection provisions via both technical and organisational measures, offering therefore some flexibility in the practical implementation.

This means for instance that, regarding the time limits reviews, which in accordance with Article 29(2) and Article 29(3) require automatic deletion, there is the possibility of ensuring deletion in respect of the rules using organisational measures if the new system does not allow the automatic review and deletion of entities as the CMS presently does. Similar considerations apply to automatic notifications to the DPO as defined by the EJR.

This technical precision does not, however, affect the general level of data protection that the new processing system should meet as the amended EJR refers ([14]) to the need to comply with the highest standards of data protection, in accordance with Article 7 and 8 of the Charter of Fundamental Rights of the European Union, the EUDPR (and in particular Article 91 thereof) and the specific data protection rules set out in the EJR.

([13]) See Recitals 4, 12, 16 and 21 of Regulation (EU) 2022/838.

([14]) See Recital 13 of Regulation (EU) 2022/838.

3. From 'automated data management and storage facility' to CICED

The '*automated data management and storage facility*' referred to in Article 80(8) EJR has been established as the Core International Crimes Evidence Database ([15]) ('CICED'), which consists of three components so far: a secure data transmission method for the national authorities allowing the transmission of big files to Eurojust, a safe data storage solution and advanced analysis tools.

In order to allow a step by step development of CICED while ensuring full compliance with data protection requirements, the EDPS has agreed to a 'phased approach' in the prior consultations ([16]). In practice, three subsequent consultations ([17]) have been launched for the three completed phases of the CICED project so far. In this way it has been possible to implement the recommendations received from the EDPS in every module of the project when going live and Eurojust has been able to take on board the useful advice and guidance provided by the EDPS in its opinions for the subsequent phases of the system.

From a data protection perspective, the new mandate of Eurojust has raised quite a number of challenges, developing in unchartered territory while the military aggression in Ukraine continues and the needs of the parties involved might evolve as well. For instance, when the amendment to the EJR was being negotiated ([18]), the preservation of evidence was seen as a priority due to the risk that the evidence could not be safely stored on the territory where the hostilities take place ([19]). So far, however, the Ukrainian authorities have developed methods allowing them to safely store the available evidence.

The wording of Regulation (EU) 2022/838 contains, possibly due to the extremely quick negotiation of this instrument, some terminology which might raise some interpretation questions, such as the term 'evidence'. From the Eurojust perspective this term is understood as referring to digital copies, as the

([15]) See for further information European Union Agency for Criminal Justice Cooperation, Core International Crimes Evidence Database (CICED).

([16]) This 'phased approach' as to the prior consultation to the EDPS is explained in the first opinion of the EDPS of 14 December 2022 following the first notification of Eurojust as to CICED 1.0: *'As EJ intends to implement the Regulation (EU) 2022/838 in stages, it was informally agreed with the EDPS that the prior consultation will also be carried out in stages, allowing EJ to implement the proposed solutions gradually. In the indicative implementation timeline provided by Eurojust, three notifications to the EDPS were envisaged, corresponding to the three stages of implementation of the new mandate. At each stage of implementation of the project, before the new technical components will be deployed, new workflows and processes will be developed and prior consultation of the EDPS will be carried out, including analysis of the risks and mitigating measures'.*

([17]) The first EDPS consultation was launched on 13 October 2022 on CICED 1.0 (Tool for transmission of big file) and the EDPS Opinion was received on 14 December 2022; the second notification on CICED 2.0 (Evidence storage solution) was sent on 13 December 2022 and the EDPS Opinion was received on 9 February 2023; the third notification on CICED 3.0 (Structured data analysis) was sent on 20 June 2023 and the EDPS Opinion was received on 16 August 2023 (Opinions not published).

([18]) See Explanatory Memorandum of COM (2022) 187 final.

([19]) See Recital 9 of Regulation (EU) 2018/1727.

originals stay at national authorities' level. The definition of the additional types of data included in Annex II EJR might also raise questions as imprecise terminology such as '*information relating to criminal conduct*' is used ([20]). Annex II needs however to be read together with Article 27 EJR, meaning therefore that the limitations included in this article as to categories of data and categories of data subjects fully apply and, additionally, all processing of operational data may only take place if it is necessary for the fulfilment of the tasks of Eurojust, within the framework of its competence and in order to carry out its operational tasks.

Facing the possibility of receiving large scale and unstructured data sets, Eurojust was concerned that received information might not be clearly labelled as to the category of persons to which it belongs and possibly not in conformity with the limitations imposed by Article 27 EJR which limits the personal data which Eurojust may legally process to '*only the operational personal data listed in point 1 (paragraph 1) or in point 2 (paragraph 2)*' of Annex II.

In order to mitigate this risk and taking into account the fact that Article 27 underlines the fact that the qualification of the persons whose personal data Eurojust processes should happen '*under the national laws of the Member States concerned*', Eurojust has developed a form for the transmission of data from national authorities with tick boxes, which allows a first basic analysis of the contents of the transmission. Through the use of this form the national authorities have to provide the 'label' as to the categories of persons and Eurojust therefore ensures that every piece of evidence received is properly 'labelled' as to the categories of persons concerned and types of data allowed by the EJR. In practice every file received by Eurojust has its own data subject category defined by the national authorities as well as the evidence type and the event to which they refer, including also a short description. This is achieved through a clear labelling of the fields in the registration form, which has proved to be useful both from the operational and the data protection viewpoint.

This requires some commitment and resources, both from the side of the national authorities, given the volume of the data provided, and from the CICED team at Eurojust, who liaises closely with the national authorities and provides them the necessary guidance before the transmission of data takes place. The CICED team also reviews the information once received to verify that only operational data compliant with Article 27 and Annex II of the EJR is processed within the CICED database.

([20]) In practice, Eurojust is receiving mainly the following types of electronic evidence: witness/victim and suspects statements, medical documents, audio recordings, fingerprints and DNA, expert examinations, communication data, video recordings and photographs, satellite images.

So far the analysis tools in place under CICED 3.0, following the positive EDPS opinion of August 2023, work for structured information but do not allow the automated analysis of unstructured information ([21]). Additional analysis tools will need to be deployed in the future, following further consultation with the EDPS, allowing for instance for automatic translation and associated activities such as automatic detection of languages, Optical Character Recognition ('OCR') and so forth.

4. Rights of the data subjects

In the context of CICED, Eurojust will receive structured and unstructured operational personal data concerning suspects, victims, and other categories of persons as defined in Article 27 EJR. It is however possible that persons other than those listed in Article 27 will be visible in unstructured data files, such as in the background of photos or videos.

In order to ensure the protection of the individuals' rights in the CICED database, Eurojust has developed a specific procedure which has been recently updated following the EDPS opinion of 16 August 2023 ([22]). All the data in CICED, regardless of where and how it is stored and processed, shall be subject to data subject requests and every request shall be handled individually and respecting all data protection principles laid down in Article 71 of EUDPR. In accordance with Article 78(1)-(4) EUDPR, Eurojust will take all reasonable steps to respond to the data subject request in a concise, intelligible, and easily accessible form, using clear and plain language, by an appropriate means, and where possible in the same form as the request. Eurojust will follow-up to the request in writing without undue delay, and take action free of charge, unless the request is manifestly unfounded or excessive.

Eurojust shall take 'all reasonable efforts' ([23]) to clarify whether the operational personal data belong to the requester or not and to clarify whether individuals (other than those listed in Article 27 EJR) whose data might be displayed in the images or videos of the received contributions can be identified or not.

([21]) CICED 3.0 went live in December 2023.

([22]) Opinion not published.

([23]) EDPS Supervisory Opinion on Europol's Procedure to Handle Data Subject Access requests, issued on 13 December 2021, paragraph 53:*'Europol must make reasonable efforts to clarify whether the personal data belong to the requester'* at p. 4 and 9, and *'it is up to Europol to make reasonable efforts to retrieve and assess the requested information'* at p 6; EDPB Guidelines 01/2022 on data subject rights – Right of access, adopted on 28 March 2023 *'the controllers should undertake all reasonable efforts to make sure that the exercise of data subject rights is facilitated'*.

In accordance with the judgments of the General Court in *SRB v EDPS* ([24]) and *OC v European Commission* ([25]), and the CJEU in *Breyer* ([26]), when determining whether data relates to an identifiable natural person, it is necessary to consider the means reasonably likely to be used to identify individuals. In *OC v European Commission,* the General Court found that cross-referencing the indirect identifiers of a data subject contained in a press release (such as age, gender, nationality) with a third party database in order to identify the data subject constituted means that were not reasonably likely to be used by the readers of the press release and that 'certainly require[d] additional time' ([27]). In *SRB v EDPS*, the General Court found that, in order to determine whether information transmitted to a recipient related to an identifiable person, it was necessary to consider whether the recipient '*had legal means available to it which could in practice enable it to access the additional information necessary*' to identify individuals ([28]).

In order for Eurojust to identify individuals other than those listed in Article 27 EJR, whose data may be displayed in unstructured data files (e.g. photos and videos), it would be necessary for Eurojust to spend additional and disproportionate effort in terms of time, cost, manpower, and means which will not be reasonably likely to be used to identify individuals, such as by deploying additional intrusive software applications (AI for face recognition, etc.), cross-referencing with a third party database(s) or collecting additional information from open sources, etc.

The EDPS has emphasised that the burden of the task for the controller has to be kept in mind when responding to access requests ([29]). Moreover, the EDPB has stated that, in accordance with data protection by design and by default ([30]), controllers '*should implement appropriate ways to find and retrieve information regarding a data subject when handling a request. However, […] an excessive interpretation in this regard could lead to functions for finding and retrieving information that in itself pose a risk for the privacy of data subjects*' ([31]).

([24]) Judgment of the General Court of 26 April 2023, SRB v EDPS, ECLI:EU:T:2023:219, paragraph 104.

([25]) Judgment of the General Court of 4 May 2022, *OC/Commission*, T-384/20, ECLI:EU:T:2022:273, paragraphs 46 and 48.

([26]) Judgment of the Court of Justice of 19 October 2016, Breyer, C-582/14, ECLI:EU:C:2016:779, paragraph 45.

([27]) *OC v European Commission,* unofficial translation from paragraph 72.

([28]) *SRB v EDPS,* see footnote 26, paragraph 105.

([29]) EDPS Supervisory Opinion on Europol's Procedure to Handle Data Subject Access requests under Article 36 & 37 of Regulation (EU) 2016/7941 ('the Europol Regulation'), issued on 13 December 2021, p. 6; EDPS guidelines on the rights of individuals with regard to the processing of personal data, p. 17; EDPS guidance paper on Articles 14-16 of the new regulation 45/2001, issued on 25 February 2014, p. 9-10.

([30]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39, Article 85.

([31]) EDPB Guidelines 01/2022 on data subject rights – Right of access Version 2.0, adopted on 28 March 2023, paragraph 126.

The procedure defined by Eurojust therefore explains that, as already mentioned, for unstructured data files such as photos and videos, the CICED team, despite all efforts to verify the information received from national authorities, cannot rule out with certainty the appearance of individuals not listed in Article 27 EJR. However, Eurojust does not plan on implementing any additional technological solutions/means (e.g. AIs for facial recognition, cross-referencing with a third party database(s), collecting additional information from open sources) to identify such individuals, which would imply an additional processing of data which is not necessary and proportionate, as the data identifying those individuals is not directly/indirectly linked to the ongoing investigation of CIC and will not be relevant and/or necessary ([32]).

Where Eurojust is not able to determine with certainty that search results match the requester, it will not be able provide this data to the requester, who will be informed accordingly ([33]). Considering the principle of data minimisation and Article 12 EUDPR, Eurojust is not obliged to maintain or acquire additional information in order to identify a data subject for the sole purpose of complying with a data subject request ([34]). This is because the purpose of the storage and analysis of data in the CICED does not require identification by Eurojust of all individuals, such as individuals in photos or videos other than the main subjects concerned ([35]).It is further clearly stated in the procedure that any information provided by the data subject to establish his/her identity for the purpose of facilitating the data subject rights request will be used solely for that purpose, and will not be used for operational purposes.

In case of a personal data breach involving the operational personal data in the CICED database, Eurojust will communicate the data breach to data subjects in the cases foreseen by Article 93 EUDPR, taking into account possible restrictions subject to the conditions referred to in Article 79(3) EUDPR. Additionally, and in line with Article 39 EJR, Eurojust will notify without undue delay the competent authorities of the Member State(s) concerned of that breach.

([32]) See, e.g. EDPB Guidelines 5/2022 on facial recognition technology in the area of law enforcement, adopted on 26 April 2023, Scenario 6, concerning the use by a police department of a facial recognition tool to identify individuals in a video through biometric identification. The tool, provided by a private entity, scrapes facial images off the internet to create a database. The EDPB observes, *inter alia,* that '*there is no connection between the personal data collected and the pursued objective by the law enforcement authority.*' The EDPB concludes that '*the use of the application would not meet the necessity and proportionality requirements and would mean a disproportionate interference of data subjects' rights to respect for private life and the protection of personal data under [the EU Charter of Fundamental Rights].*'

([33]) EDPS Supervisory Opinion on Europol's procedure to handle data subjects requests, issued on 13 December 2021, p. 5,'*Where Europol is not able to determine with certainty that the personal data in its systems match the requester, the EDPS supports Europol's current approach: that it should not provide this data to the requester*'. Where the request concerns data stored and processed in CICED, the reply to the data subject will include the following disclaimer (subject to review in line with future developments and Eurojust's technical capabilities):'*Please be informed that parts of the Core International Crimes Database (CICED) database were excluded from alphanumerical searches (i.e. unstructured audio-visual data displaying persons that have not been identified by Eurojust because this goes beyond current Eurojust's technological capabilities and its legal mandate.*)'.

([34]) EDPS Supervisory Opinion on Europol's procedure to handle data subjects requests, issued on 13 December 2021, p. 5.

([35]) EDPS Supervisory Opinion on Europol's procedure to handle data subjects requests, issued on 13 December 2021, p. 4-5; EDPB Guidelines 01/2022 on data subject rights – Right of access, adopted on 18 January 2022, paragraphs 59-61 including Example 10.

5. Conclusion and future perspective

In conclusion, the continuous and constructive dialogue with the EDPS has allowed Eurojust to ensure a privacy by design approach through the whole CICED implementation process. The cooperation with the EDPS remains a key element for the following phases of this project, particularly in what regards the processing of unstructured operational data. Eurojust is aware of the need to ensure as soon as possible the automatic processing and indexation of unstructured personal data, both from the operational and data protection perspective, and will work on this in the context of the following phases of the CICED project.

It should also be noted, as a final remark, that the derogation of Article 23 EJR as to the use of the separate '*automated data management and processing facility*' (CICED) applies *'as long as the CMS composed of temporary work files and of an index remains in place'* ([36]). This means in practice that the functionalities being now put in place by Eurojust in the context of the CICED database will need to be integrated in the new CMS which is presently also being developed by Eurojust to take into account the requirements as to the digital information exchange in terrorism cases as defined by the amendments to the EJR of 4 October 2023 ([37]). The new CMS, as already underlined in the EDPS opinion 6/2022 ([38]), should integrate the CICED database functionalities and the CICED database should cease to exist at that point of time. From that moment on no derogation will affect the application of Article 23.7 and the CMS will remain the only automated system for the processing of operational data at Eurojust.

There is therefore a need to consider the CICED requirements in the context of the new CMS project, another major project requiring Eurojust to integrate data protection by design and by default in all steps of the process. The new CMS is being developed in parallel to the CICEC project, also in close consultation with the EDPS.

([36]) See the last sentence of Article 80(8) EJR, added by Article 1 of Regulation (EU) 2018/1727.

([37]) Regulation (EU) 2023/2131 of the European Parliament and of the Council of 4 October 2023 amending Regulation (EU) 2018/1727 of the European Parliament and of the Council and Council Decision 2005/671/JHA, as regards digital information exchange in terrorism cases, OJ L 2023/2131, 11.10.2023, p. 1.

([38]) EDPS Opinion 6/2022 on the Proposal for a Regulation of the European Parliament and the Council amending Regulation (EU) 2018/1727 of the European Parliament and the Council, as regards the collection, preservation and analysis of evidence relating to genocide, crimes against humanity and war crimes at Eurojust, issued on 13 May 2022, underlines that the derogation to Article 23 EJR should be of a temporary nature and the automated data management and storage facility should be integrated into the new case management system which is expected to be established under the Proposal for a Regulation on the digital information exchange on terrorism case.

12

The making of the European Data Protection Board

Andrea Jelinek
Isabelle Vereecken

The making of the European Data Protection Board

Andrea Jelinek (*) **Isabelle Vereecken (**)**

The EDPB and EDPS are two separate institutions that are narrowly intertwined, but with different responsibilities. Before the GDPR entered into application in May 2018, a great deal of preparation went into the setting up of the EDPB as a new EU body, with the EDPS playing an instrumental role in getting the EDPB Secretariat up and running. Andrea Jelinek, EDPB Chair 2018-2023, and Isabelle Vereecken, Head of the EDPB Secretariat, stood at the cradle of the EDPB and its Secretariat and look back at the preparatory phase and the challenges of the early days. Today, the EDPB is an influential decision-making body with many tasks and, in parallel, the workload of the EDPB Secretariat has grown. The EDPB and its Secretariat are preparing for future challenges, including staying on top of rapid technological development and an increase in litigation.

1. A new EU body sees the daylight

When the GDPR was adopted in 2016, the seed was planted for the European Data Protection Board ('EDPB'), a new and one-of-a-kind EU body with a legal personality. The EDPB is formed by representatives of the European national Data Protection Authorities ('DPAs') [1] and the European Data Protection Supervisor ('EDPS'). The European Commission participates in the activities and meetings of the Board without voting rights.

(*) Chair of the European Data Protection Board (2018-2023).

(**) Head of Unit of the European Data Protection Board Secretariat.

[1] Called Supervisory Authorities in the GDPR, Article 4(22) GDPR. In addition to the EU DPAs, the supervisory authorities of the EFTA EEA States (Iceland, Liechtenstein and Norway) are also members of the EDPB without voting rights.

The core mission of the EDPB is to ensure the consistent application of the data protection rules in Europe. It provides guidelines, recommendations and best practices to clarify the law and to promote a common understanding of EU data protection law. The EDPB also provides, together with the EDPS, joint opinions on legislative proposals, which are of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data ([2]). An important difference with its predecessor, the Article 29 Working Party ('WP29') ([3]), is that the EDPB has the authority to adopt binding decisions addressed to the national DPAs aiming to settle disputes arising when they cooperate to enforce the GDPR, with the purpose of ensuring the correct and consistent application of the GDPR in individual cases ([4]) or to decide on urgent measures ([5]). This is a far-reaching competence, because of the nature of the decisions (binding for DPAs) but also because they usually relate to matters concerning large companies and processing of all European individuals' personal data ([6]).

The EDPS had a key role in the setting up of the EDPB, as it is required to provide its Secretariat (Article 75(1) GDPR).

> *The EDPS has always been very supportive of the EDPB: Giovanni's reputation in the world of data protection and the respect for him opened many doors for the EDPB. Wojciech was always on Giovanni's side and carried on his legacy with his strong support for the EDPB.*
>
> Andrea Jelinek, EDPB Chair 2018-2023

In view of the fact that the EDPS provides the Secretariat of the EDPB, the co-legislators were careful not to give any advantages to the EDPS in comparison with the other members of the EDPB. Article 75(2) GDPR (exclusive instructions of the Chair) and Article 75(3) GDPR (separate reporting lines) aim to ensure that the EDPS does not have more influence over the Secretariat than any of the other EDPB members.

([2]) While the EDPS has a general competence relating to legislative consultation, the EDPS and the EDPB issue joint opinions for proposals considered by the Commission as of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data. See Article 42 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

([3]) Article 29 Working Party, composed of representatives of DPAs and the EDPS, which was set up by the Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

([4]) See Article 65 GDPR.

([5]) See Article 66 GDPR.

([6]) See for instance the EDPB Binding decision 01/2023 on the dispute submitted by the Irish SA on data transfers to the USA by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), adopted on 13 April 2023, which led to the imposition of a fine of €1.2 billion on Meta by the Irish DPA, or the EDPB Binding decision 02/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), following which the Irish DPA ordered Tiktok to eliminate unfair design practices concerning children.

Notwithstanding this structural separation, it is important to underline that the EDPS is also an important and highly valued member of the EDPB. In that capacity, the EDPS regularly plays an important role in the drafting of EDPB documents, actively takes part in discussions of both technical and strategic nature, and acts as coordinator of different expert subgroups.

2. Good preparation is the key to success

The EDPS started to prepare the creation of the EDPB Secretariat – and of the EDPB – early on, for instance with the creation of a dedicated budget title under the EDPS budget to provide resources for the coming board. Isabelle Vereecken was appointed as 'liaison officer' within the EDPS in May 2017 to ensure that everything needed for the existence of the EDPB and its Secretariat would be ready in time.

One of the early action points was to adopt a logo and a visual identity, a prerequisite to get the EDPB website ready in time. The logo that was chosen by the DPAs out of several options was the 'baby' of both EDPS and the French DPA ('CNIL'), whose President was Chair of the WP29 at the time.

To create the EDPB Secretariat and to organise the communication flows among DPAs under the GDPR, a large and complicated puzzle had to be put together, and all of its pieces needed to be in place by a strict deadline.

An IT system needed to be selected and the EDPB ([7]) opted for the Internal Market Information system ('IMI' ([8])), adapting it to the future needs of the EDPB by creating new flows dedicated to GDPR cooperation. In less than 6 months, 14 IMI modules, 19 forms and more than 10.000 IT fields were created with the cooperation of all the DPAs, and a Commission implementing act was adopted ([9]).

All the intense activities for the preparation of the implementation of the GDPR also existed within the DPAs, which were simultaneously engaged in intensive preparations at national level, with numerous measures to be ready within the allotted timeframe.

([7]) At that time, the Article 29 Working Party, see footnote 3.

([8]) See Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation'), OJ L 316, 14.11.2012, p. 1, and European Commission, Internal Market Information (IMI).

([9]) Commission Implementing Decision (EU) 2018/743 of 16 May 2018 on a pilot project to implement the administrative cooperation provisions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council by means of the Internal Market Information System, OJ L 123, 18.5.2018, p. 115.

> *May 2016 kicked of a race to be ready for the GDPR, not just for private and public sector organisations, but for regulators as well. DPAs acquired new powers and new cooperation duties, which meant the majority had to undergo a far-reaching administrative transformation to get ready for 25 May 2018.*
>
> Isabelle Vereecken – Head of the EDPB Secretariat

The DPAs, working together under the umbrella of the WP29 led by Isabelle Falque-Pierrotin, the head of the French DPA, developed many guidelines in order to provide consistent and clear explanations on different aspects of the GDPR. During this preparatory phase, the EDPS-EDPB Memorandum of Understanding ('MoU') ([10]) was also negotiated, to ensure rules for the good cooperation between the EDPS and the EDPB. This MoU aimed to clarify the tasks entrusted to the EDPS as provider of the EDPB Secretariat and the activities performed by the Secretariat under the direct instructions of the Chair of the EDPB. Giovanni Buttarelli, Supervisor at the time, was personally closely involved in creating the EDPB Secretariat and invested a great deal of time in developing the MoU. The EDPS was also hosting meetings of DPA representatives to negotiate the future Rules of Procedure ('RoP') ([11]) of the EDPB. From the moment Andrea Jelinek was appointed as Chair of the WP29 (in March 2018), with the perspective to become Chair of the EDPB, she was chairing these important meetings with the support of her team.

> *Preparing for the EDPB was a challenge for each and every Member, but the fact that we knew each other from many years working together in the WP29 was of tremendous value. It meant that we understood the challenges others were facing. These close relationships were a solid foundation to build the EDPB on.*
>
> Andrea Jelinek, EDPB Chair 2018-2023

In November 2017, a dedicated Sector was created within the EDPS. While before that, liaison officer Isabelle Vereecken was working with the help of EDPS colleagues where needed, a team of seven colleagues was from that moment working full time to establish the future EDPB Secretariat and to prepare the cooperation among DPAs. This small team was the core of what was to become the EDPB Secretariat in May 2018. Together, these colleagues finalised the work on the future EDPB website and the IMI system and created all the processes for the future organisation of EDPB meetings.

([10]) See Article 75(4) GDPR and the Memorandum of Understanding between the European Data Protection Board and the European Data Protection Supervisor, signed on 25 May 2018.

([11]) See EDPB, Rules of Procedure, adopted on 25 May 2018.

3. Steering the ship

During the EDPB's very first meeting (25 May 2018), Andrea Jelinek was unanimously elected as Chair of the EDPB. During this same meeting, the RoP were adopted and the MoU between the EDPS and the EDPB was signed. The EDPB also endorsed 16 guidelines adopted by the WP29, which aimed to clarify the application of GDPR and to promote its uniform application.

> *When I applied for the function of Chair of the EDPB, I really wanted to approach the role as a primus inter pares, and to give everyone in the EDPB a voice.*
>
> Andrea Jelinek, EDPB Chair 2018-2023

Suggestions were made to modernise the working methods and to increase the use of technical means for meetings, e.g. videoconference system, electronic vote in order to make sure that all Data Protection Authorities, especially the small ones, are able to participate more actively in the meetings. This set the tone for the future working methods of the EDPB, which changed rapidly. Today, the vast majority of EDPB meetings take place remotely. The EDPB also relies on a systematic vote (during in person meetings, with an electronic system) for the adoption of documents, compared with WP29, for which members relied more on the consensus method. This change implied broader participation of all the members in the decision-making.

> *Ensuring all members were able to work together on an equal footing has always been a key requirement when selecting working tools and methods.*
>
> Isabelle Vereecken, Head of the EDPB Secretariat

The EDPB has known many watershed moments in its relatively short span of existence. There have been many firsts and each of these brought its own challenges. The first Article 65 Binding Decision (adopted in November 2020) spurred the EDPB to adopt guidance on relevant and reasoned objections ([12]). The year after, a Binding Decision was challenged for the first time in Court ([13]) and the Secretariat needed to secure resources to defend the EDPB's position. Gradually, as DPAs learned from their experience in enforcing the GDPR, it became clear there was a role for the EDPB and its Secretariat in supporting enforcement cooperation. This led to the Vienna declaration ([14]) and the creation of synergy-driven programmes, such as the Coordinated

([12]) EDPB Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679, adopted 9 March 2021.

([13]) Order of the General Court of 7 December 2022, *WhatsApp Ireland/Comité européen de la protection des données*, T-709/21, ECLI:EU:T:2022:783. At the time of drafting this article, the EDPB is involved in 12 legal procedures to which the EDPB is a party.

([14]) EDPB Statement on Enforcement Cooperation, adopted on 28 April 2022.

Enforcement Framework ([15]) and the Support Pool of Experts ([16]). Building on the work done by the DPAs, awareness raising among a large audience became the next important project, culminating in the creation of the SME Guide for Small Businesses ([17]).

> *I was very proud, on behalf of all the Members, when the Board adopted the Vienna declaration: it opened the door to a different level of cooperation between DPAs and the European Commission immediately put the EDPB wish list at the top of their agenda.*
>
> Andrea Jelinek, EDPB Chair 2018-2023

The EDPB Secretariat has grown as the Board's many responsibilities were increasing: today, it consists of 39 staff members, divided over five sectors ([18]). However, the EDPB Secretariat needs further expansion in order to keep the pace and to continue fulfilling its legal duties at the service of the EDPB and of the GDPR. For instance, the number of binding decisions, for which the Secretariat nearly always holds the pen ([19]), has increased a great deal in the last years. Given the importance of the issues at stake, these decisions are challenged systematically before Court, which also further increases the workload of the Secretariat.

4. Getting ready for the future

In December 2023, the EDPB adopted its contribution to the European Commission's Report on the Application of the GDPR ([20]). This text offers a good summary of where the EDPB stands today and what it sees as future challenges.

There is general agreement among DPAs that the GDPR has strengthened, modernised and harmonised data protection principles across the EU. Awareness of data protection rights and obligations has risen significantly. Additionally, DPAs are using their investigative and corrective powers whenever

([15]) The Coordinated Enforcement Framework ('CEF') provides a structure for the EDPB to coordinate enforcement action carried out by EEA DPAs. The annual coordinated action focuses on a pre-defined topic and allows DPAs to pursue this topic using the agreed-upon methodology. In 2022, the CEF was about the use of cloud based services by the public sector and in 2023 about the role of Data Protection Officers.

([16]) The Support Pool of Experts ('SPE') was developed as part of the EDPB Strategy 2021-2023, adopted on 15 December 2020, to help DPAs to increase their capacity to enforce by developing common tools and giving them access to a wide pool of experts, either from other DPAs or from outside the EDPB.

([17]) An entire section of the website of the EDPB is dedicated to this interactive guide on GDPR for SMEs.

([18]) Litigation & International Affairs, Cooperation and Enforcement, Information and Communications, Administrative matters, and IT matters. In addition to the 39 staff working within the EDPB Secretariat, 7 EDPS staff members, paid under the budget of the EDPB, are integrated in the staff of the EDPS and provide horizontal services to the EDPB Secretariat.

([19]) This is reflected in Article 11(5) of the EDPB Rules of procedure (op. cit. footnote 12) and the reason was that the EDPB Secretariat does not take part in the horizontal cooperation between national data protection authorities during which objections can be raised.

([20]) EDPB, Contribution of the EDPB to the report on the application of the GDPR under Article 97, adopted on 12 December 2023.

appropriate and have reinforced their cooperation. The GDPR is also contributing to an increased global visibility of the EU legal framework and is often considered as a model by countries outside the EU.

The understanding today is that DPAs will in the coming years cooperate even more closely on enforcing the GDPR than they do today. Many regulators working in the same direction can achieve a great deal more than each of them working on its own priorities. The 'economy of scale' and synergies that are generated by an EU approach will directly benefit individual authorities. In the future, the Secretariat will play an even more important role in enabling the cooperation among DPA staff members across the EEA.

> *There is an irrefutable and natural logic in the development of the EDPB. Many of today's projects build upon the experience of the past years and we could not have tackled these earlier on in the process. It would have been impossible to arrive at the present point without the lessons learned from the past six years.*
>
> Isabelle Vereecken, Head of the EDPB Secretariat

Nevertheless, there are still obstacles to the cooperation and consistency mechanism. The Regulation laying down additional procedural rules ([21]) will play an important role in overcoming these, once adopted.

The technological landscape is continuously evolving and new technologies emerge regularly. The EDPB will continue to develop guidance on new and emerging technologies and follows regulatory developments closely. The DPAs and the EDPB will also play an important role in the application of the new digital rules ([22]), and they need to make sure they have sufficient expertise available to keep step with emerging technologies. The Support Pool of Experts ('SPE') initiative ([23]), which was initially suggested by the EDPS, as member of the EDPB, is very useful in this regard. This initiative enables staff

([21]) Proposal for a regulation of the European parliament and of the council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM(2023) 348 final.

([22]) For instance, the EDPB will provide guidance on the interplay between the application of GDPR and the AI Act, the legislations of the EU Data Strategy and the Digital Services Package. The EDPB will contribute to the DGA and DA European Data Innovation Board and of the DMA High Level Group. It is also worth mentioning that the DPAs are responsible to monitor the Data Act, insofar personal data is concerned, and that the GDPR cooperation procedures and the EDPB consistency mechanism also apply, implying the EDPB will have the competence to also adopt binding decisions on this matter, see Article 31(2)(a) of Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L 2023/2854, 22.12.2023.

([23]) EDPB Call for Experts, the new EDPB Support Pool of Experts, 21 February 2022.

exchanges between DPAs, the EDPS and the EDPB Secretariat ([24]) but also helps DPAs to increase their enforcement capacity by developing common tools and giving them access to a wide pool of external experts.

The EDPB has established itself as an influential decision-making body since its creation in 2018. Through its legal advice and, even more importantly, its binding decisions, the EDPB has a far-reaching impact on fundamental legal questions in the field of data protection.

The EDPB and EDPS have come a long way together since the early beginnings of the GDPR in 2016. The excellent cooperation between the two institutions is ample reason to look at the future with confidence.

([24]) Between 2022 and 2023, 22 staff members worked within 15 host authorities for a duration between 2 weeks and 6 months.

13

International cooperation: an imperative at the core of EDPS activities

Olivier Matter

International cooperation: an imperative at the core of EDPS activities

Olivier Matter (*)

International cooperation with stakeholders beyond the EU has moved from the margins to the core of the activities of many data protection authorities. This article describes the role and milestone achievements of different international fora, such as the Council of Europe, the Spring Conference, the Global Privacy Assembly, the OECD, the G7 DPAs roundtable and the International organisations workshop. The EDPS' active role on the international stage during the last 20 years has been instrumental in advancing high data protection standards globally.

> *Make men work together, show them that beyond their differences and geographical boundaries there lies a common interest.*
>
> Jean Monnet

1. Introduction

There is a feeling of vertigo when we look back and consider the evolution of our digital societies from 2004 to 2024. Over the last 20 years, we witnessed a digital revolution deeply impacting many aspects of our lives. There are few domains that have gone through such deep transformation in such a short period of time.

In 2004, when the European Data Protection Supervisor ('EDPS') was established, WiFi was still presented as an emerging technology, the iPod and Skype were dominating their markets and the Facebook company was just created. In

(*) Head of International cooperation at the EDPS. The comments and opinions contained in this contribution are expressed by the author in a personal capacity and may not necessarily reflect the positions of the EDPS.

2024, we are discussing Large Language Models and generative artificial intelligence ('AI'), digital identity, Internet of behaviours, extended reality, deepfake detection, etc ([1]).

We should certainly celebrate innovation, the unprecedented speed of technological advancement and the breakthroughs in medicine or science, but we cannot neglect to consider and address the challenges linked to these evolutions, including for the protection of privacy and personal data.

Data protection in the last 20 years has moved from the margins of a group of 'data protection geeks' to the mainstream of public policy, social lives and citizen advocacy.

There is an equal feeling of vertigo when one considers that the EDPS – in the same period of time and like other data protection authorities ('DPAs') in the world – had to grow from scratch and had to demonstrate their adaptability to face a constantly changing institutional, legal and technological landscape. The EDPS has indeed done a lot to grow over the years as a strong and mature institution thanks to the leadership of the three supervisors since the creation of the institution and thanks to the expertise and dedication of the EDPS staff. The active role of the EDPS on the international stage has played an integral and instrumental role in this development.

2. Why international cooperation matters

As a small European Union ('EU') institution with a specific mandate, the EDPS understood very early in its existence – and this is still valid today – the strategic importance of dialogue and cooperation with its peers. Such cooperation takes place first and foremost within the framework of the EU. The national DPAs of the EU ([2]) are the most privileged and 'natural' partners for the EDPS. Such cooperation first took place within the framework of the Article 29 Working Party. Since the entry into application of the General Data Protection Regulation ('GDPR') ([3]), it takes place within the framework of the European Data Protection Board.

But the challenges linked to our digital societies do not stop at the borders of the EU. In the field of data protection, like in many other today, the challenges are global. The aim of this contribution is to assess the importance of international cooperation beyond the borders of the EU.

([1]) See for instance on these topics the EDPS TechSonar reports on emerging technologies.

([2]) References to 'EU' or 'national DPA of the EU' made throughout this contribution should be understood as references to 'EEA' or 'national DPAs of the EEA'.

([3]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

2.1. A world with more data protection laws but still in search of a global standard

Many of the national laws and bills over the world present similarities with the European model of data protection. This model finds its roots and origins in the standards set in the early 80's in the Organisation for Economic Co-operation and Development ('OECD') Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ([4]) and the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (so called 'Convention 108') ([5]).

Since its adoption, the GDPR has also served as an inspirational model for many countries outside the EU. The GDPR has surely been a global turning point for privacy and its impact cannot be underestimated. In that sense, the so-called 'Brussels effect' is a reality, particularly in the field of digital regulation ([6]). The data protection flagship law of the EU indeed provides a solid and modern basis for a human-centric data economy and society.

The key message of Václav Havel´s famous speech in Aachen in 1996 is still very relevant today, including in the context of digital regulation: '*Europe's task is no longer, nor will it ever be again, to rule the world, to disseminate by force its own concepts of welfare and of what is good, to impose its own culture upon the world or to instruct. The only meaningful task for the Europe of the next century is to be the best it can be, that is, to resurrect and imbue its life with its best spiritual traditions and thus help to shape creatively a new pattern of global coexistence. We shall do most for the world if we simply do as we are bidden by our conscience, that is, if we act as we believe everyone should act. Perhaps we will inspire someone as we do so, perhaps we won't.*' ([7])

According to the works of Professor Graham Greenleaf, we could count 162 national laws and 20 Bills on the protection of privacy and data protection in February 2023 ([8]). Professor Greenleaf forecasts that most jurisdictions without privacy laws will adopt them this decade. Many existing data protection laws are also being updated and often upgraded.

By contrast, and to illustrate the rapid pace of adoption of laws, the same author found that as of mid-2011, there were 'only' 76 countries that had laws

([4]) OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/Final, 23 September 1980.

([5]) Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981.

([6]) Bradford, A., *The Brussels Effect,* Oxford University Press, 2020. In her book, Columbia Law Professor, Ms Anu Bradford, argues the EU remains an influential superpower that shapes the world in its image. By promulgating regulations that shape the international business environment, elevating standards worldwide, and leading to a notable Europeanization of many important aspects of global commerce, the EU has managed to shape policy in areas such as data privacy, consumer health and safety, environmental protection, antitrust, and online hate speech.

([7]) The New York Review, 'The Hope for Europe', Speech of President Václav Havel, delivered in Aachen on 15 May 1996.

([8]) Greenleaf, G., *Global Tables of Data Privacy Laws and Bills (8th Ed.)*, *SSRN*, 2023.

that at least cover most of their private sector and include privacy principles meeting or exceeding the minimum standards of international data protection and privacy agreements ([9]).

At the same time, it is a fact that there is not yet any uniform and global standard on data protection applied throughout the world. There is no UN universal binding declaration or convention specifically on data protection. And still our challenges are present and global. There is still fragmentation among the various legal frameworks in the world and one needs to identify and address the risks linked to such fragmentation. Even more, there should be no gap or vacuum in the protection of the fundamental right to the protection of personal data – regardless of whether you are based in Belgium or Poland, Armenia or Serbia, New-Zealand or Japan.

2.2. DPAs are stronger and more effective together

For a stronger and effective protection of personal data at a global level, DPAs from all over the world need to cooperate, among themselves as well as with other public authorities and key stakeholders. One often hears calls for more convergence among the different regions of the world, but words are not enough. Convergence actually requires concrete actions and projects. The EDPS strongly believes such concrete actions may lead to a better mutual understanding and facilitate the building of bridges between our jurisdictions.

The EDPS, Wojciech Wiewiórowski, identified international cooperation as a main priority for its mid-term Strategy for the institution ([10]). International cooperation should help to promote global common approaches on privacy and data protection challenges, which may also contribute to facilitate data flows from and to the EU.

The basic rationale is that DPAs from all over the world are stronger and more effective together. As recently recalled by the EDPS Secretary General, Leonardo Cervera Navas ([11]), international cooperation is no longer an option or an ancillary activity for a DPA; it is vital and should be at the core of all its actions, from policy to enforcement or new technologies monitoring aspects. DPAs need to pool limited resources and exchange expertise and findings to be more effective.

DPAs often remain small institutions facing colossal tasks and challenges. They need to exchange and whenever possible act together on common challenges to have an impact and make a difference. DPAs can thus play a role to nuance the negative effects of regulatory fragmentation, which is in the interest of all.

([9]) Greenleaf, G., 'Global Data Privacy Laws: Forty Years of Acceleration', *Privacy Laws and Business International Report,* No. 112, SSRN, 2011, p. 11-17 UNSW Law Research Paper No. 2011-36.

([10]) EDPS, Annual Report 2022, p.10.

([11]) EDPS, International cooperation in data protection: not an option, but vital to our tasks, 20 September 2023.

3. Cooperation and convergence in action: a few examples

3.1. The central role of the Council of Europe

The Council of Europe is undoubtedly a central player in privacy and data protection, not only in Europe but increasingly on other continents where pan-European norms are often taken as a source of inspiration for legislation and policies. 'Convention 108' ([12]) opened for signature on 28 January 1981 and 28 January is still celebrated today as the data protection day in many jurisdictions in the world. The Convention represented the first legally binding international instrument in the field of data protection and is open to accession by both European and non-European countries.

Giovanni Buttarelli rightly recalled in a speech back in 2016 that *'The Council of Europe and the EU have led the way in renewing the rulebook for a new generation'* and that *'As regards the Convention [108], one of its best assets is its material scope. Unlike the EU Charter of Fundamental Rights and the GDPR, which are limited by the transfer of competences to the EU by its Member States, the Convention does not contain a general exemption for national security'* ([13]).

The Consultative Committee of the Convention 108 ('T-PD') – involving DPAs and government representatives – is responsible for the interpretation of the provisions of Convention 108 and to facilitate and improve its implementation.

The Committee meets twice a year in Strasbourg; its Bureau meets three times a year. The EDPS participates in all T-PD meetings as an observer. In this capacity, the EDPS actively contributes to the discussions and provides comments on the documents prepared by the T-PD. The EDPS also represents since June 2019 the Global Privacy Assembly before the T-PD. The EDPS' role, in this respect, involves promoting a high standard of data protection and compatibility with EU data protection standards.

The activities of the T-PD are diverse and concern topics of strategic importance. A few recent examples include facial recognition, artificial intelligence, digital contact tracing, digital identity, processing of personal data in the context of political activities and elections, inter-state exchanges of data for Anti-Money Laundering/Countering Financing of Terrorism, and tax purposes, etc. The EDPS also follows with utmost attention the ongoing work on oversight by intelligence services as well as the development of contractual clauses in the context of trans-border data flows.

([12]) Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981.

([13]) EDPS speech on Convention 108: from a European reality to a global treaty, Council of Europe International Conference, Strasbourg, 17 June 2016.

After long and intense negotiations, Convention 108 has been modernised in May 2018 ([14]). The modernisation aims to deal with challenges resulting from the use of new information and communication technologies and to strengthen the Convention's effective implementation. The EDPS actively supports the efforts of the Council of Europe on the ongoing ratification process of this modernised Convention 108, as the sole legally binding international convention on the protection of personal data. 38 ratifications are necessary for the entry into force of this unique and landmark instrument. In late February 2024, 7 ratifications are still needed for the entry into force of Convention 108+ and it is reasonable to hope for such entry into force still in 2024.

As recalled recently by Wojciech Wiewiórowski, we must acknowledge that *'the success or failure of the Convention 108+ will largely depend on the effectiveness of its monitoring mechanism. As shown with the case of Russia, the mere fact that a country is a party to the Convention, does not mean that they are fulfilling its principles, which makes the role of the monitoring mechanism all the more crucial. With an effective monitoring mechanism and an effective cooperation by Member States, Convention 108+ can become a real benchmark and be a booster to facilitate data flows, including from and to the EU'* ([15]).

Increasingly, other aspects of the work of the Council of Europe are of key importance for the data protection community. One can think for instance about the negotiations that led to the Second Additional Protocol to the Budapest Cybercrime Convention ([16]). More recently and still at the Council of Europe, the EDPS partakes in meetings of the Committee on Artificial Intelligence ('CAI'), which has been tasked to elaborate a Convention on the development, design, and application of AI systems, based on the Council of Europe's standards on human rights, democracy and the rule of law, and conducive to innovation ([17]).

The increasing relevance of the work of the Council of Europe in the field of digital regulation led the EDPS to open on 14 March 2023 a new Office in the premises of the European Parliament in Strasbourg. The new EDPS Office provides an opportunity for closer cooperation and engagement with policymakers and other EU institutions present in Strasbourg, as well as with the Council of Europe ([18]).

([14]) Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018.

([15]) EDPS, "Searching for a Mythological Global Standard in Data Protection", 23 May 2023.

([16]) Council of Europe, Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

([17]) Council of Europe, Terms of reference of the Committee on Artificial Intelligence (CAI). Set up by the Committee of Ministers under Article 17 of the Statute of the Council of Europe and in accordance with Resolution CM/Res(2021)3 on intergovernmental committees and subordinate bodies, their terms of reference and working methods.

([18]) EDPS, Inauguration Speeches of the EDPS Office in Strasbourg, 22 March 2023.

3.2. The European Conference of DPAs ('Spring conference')

The DPAs of EU Member States and the Council of Europe meet annually for a Spring Conference to address issues of common interest, emergent trends and new developments relating to the rights to privacy and data protection.

The EDPS has actively supported this unique forum of all DPAs of 'Greater Europe'. In a keynote speech delivered by Giovanni Buttarelli at the Spring Conference in Budapest in 2016 ([19]), the EDPS reflected on the future of this conference and called its members to take action to make this event the definitive data protection event of the year for regulators in Europe. He called for ambition and to focus on the day to day challenges which DPAs face – the complaints, the legal challenges, the inspections, the breach notifications, etc. He pleaded to turn this forum into a training centre for our staff, a sort of high-quality, high-intensity data protection boot camp. He also called for an open session with experts from the wider data protection community.

The EDPS' call has been largely reflected few years later in the Resolution on the Conference Vision, Mission and Steering Group adopted in Croatia on 20 May 2022 ([20]).

The EDPS was also a member of the Interim Steering Group of the Spring conference tasked to update the Conference's rules of procedure. More recently, at the opening session of the 2023 Spring conference, Wojciech Wiewiórowski, reiterated the importance of this forum and underlined the need for more institutional support and to reinforce the links between the Spring conference and the Council of Europe as the Council of Europe in any case needs to create a network of DPAs under Convention 108+.

The EDPS also regularly participates in the annual case-handling workshops which are useful fora to discuss practical issues at staff level and bring together complaint handlers and inspectors from all over Europe.

3.3. The Global Privacy Assembly and the 2018 'Olympic Games of Data Protection'

The Global Privacy Assembly ('GPA'), previously named International Conference of Data Protection and Privacy Commissioners, is an international forum with more than 130 data protection and privacy authorities from across the globe that gather to connect and share their perspectives on the developments in data protection and key elements of their international cooperation.

The EDPS is a member of the GPA, which takes place every year in the autumn, and has been a member of its Executive Committee. To foster convergence

([19]) EDPS, Keynote speech to Spring Conference of European DPAs Budapest, 26 May 2016.

([20]) Spring Conference of the European Data Protection Authorities, Resolution on the Conference Vision, Mission and Steering Group, Cavtat, Croatia, 18-20 May 2022.

on common standards on the protection of privacy at a global level, some important resolutions have been adopted by the GPA, for instance on facial recognition, on government access to data, on AI, on enforcement cooperation and on international standards through the so-called 'Madrid Resolution'. This forum is also an opportunity for developing capacity building activities.

The GPA is more than a conference that takes place once a year as the work continues throughout the year at working group level. For instance, the EDPS, jointly with the French DPA, co-chairs the GPA working group on Ethics and Data Protection in AI and acted as main sponsor for the recent important GPA Resolution on generative AI systems, adopted in 2023 ([21]).

The EDPS also takes part actively in other various GPA working groups, including the working groups on Global Frameworks and Standards, Digital Economy, Data Protection and Other Rights Freedoms, International Enforcement Cooperation, Digital Citizen and Consumer and Data Sharing.

Under the umbrella of the GPA and with the help of a permanent secretariat that will soon be established, there is still room to strengthen this cooperation and turn the GPA into the 'network of networks' that may play a decisive role to foster convergence on high standards to safeguard privacy and data protection worldwide.

One of the highlights in the history of the EDPS is undoubtedly the 2018 International Conference, which was organised jointly by the EDPS and the Bulgarian DPA ([22]). The main theme of the conference was ethics and new technologies.

The EDPS launched the EDPS Ethics Initiative back in 2015, as part of its commitment to forging global partnerships. The EDPS wanted to generate a global discussion on how our fundamental rights and values can be upheld in the digital era. In 2018, the EDPS published an Ethics Advisory Group Report ([23]). However, it was the International Conference, dubbed the '*Olympic Games of Data Protection*' by Giovanni Buttarelli, which really launched the discussion on digital ethics onto the international agenda.

The public session of the International Conference focused on Debating Ethics: Dignity and Respect in Data Driven Life. With over 1000 people from a variety of different backgrounds, nationalities and professions in attendance, high-profile speakers and considerable media coverage, the event served to foster debate on the issue and put new ethical and legal questions high on the agenda of DPAs and others across the world.

([21]) Global Privacy Assembly, Resolution on Generative Artificial Intelligence Systems of the 45th Closed Session of the Global Privacy Assembly, October 2023.

([22]) International Conference of Data Protection & Privacy Commissioners, Debating Ethics: Dignity and respect in data driven life, 40th International Conference of Data Protection and Privacy Commissioners, 22-26 October 2018.

([23]) EDPS Ethics Advisory Group, 'Towards a digital ethics', Ethics Advisory Group Report 2018, issued on 25 January 2018.

Many members of the data protection community present at this event will long remember the moving standing ovation in the hemicycle of the European Parliament for the EDPS, Giovanni Buttarelli. But probably even more, the participants will long remember the inspirational speech in which he set out the strategic importance of defining a truly global digital ethics that safeguards dignity and respect for individuals and groups in the decades to come.

Giovanni Buttarelli reminded us – amongst many other things – that *'Not everything that is legally compliant and technically feasible is morally sustainable'*. Or that *'When media and the digital world become omnipresent, their influence can stop people from learning how to live wisely, to think deeply and to love generously'*. Or that '*Technology is, for now, predominantly designed and deployed by humans, for purposes defined by humans. But we are fast approaching a period where design, deployment and control of new technologies and technological processes are delegated to machines. But before we start to think about the humanised robots of tomorrow, we should consider the 'robotised humans' of today.*' ([24])

These messages still strongly resonate today. After Giovanni Buttarelli's tragic passing – shortly after the conference in 2019 – the GPA, under the leadership of Elisabeth Denham, decided to create an award and to ensure that his legacy is maintained and to pay tribute to the memory of the former EDPS' contribution as an outstanding leader in the global data protection community ([25]).

3.4. The increasing influence of the OECD

Just like the Council of Europe, the OECD played the role of a pioneer with the adoption on 23 September 1980 of the influential OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ([26]). The OECD Privacy Guidelines are widely recognized as a global minimum standard for privacy and data protection. The validity and pertinence of these basic principles were reaffirmed through both the 2013 revision and the 2021 report on implementation – closely followed by the EDPS.

The work of the OECD is becoming increasingly relevant for the EU and the EDPS. The OECD's work on data governance and privacy is carried out by the Working Party on Data Governance and Privacy in the Digital Economy ('DGP'). The DGP develops and promotes evidence-based policies on data governance and privacy. It is composed of delegates from the 38 member countries of the OECD, including in particular representatives of governments and DPAs ([27]).

([24]) 40th International Conference of Data Protection and Privacy Commissioners, Conference Report.

([25]) Global Privacy Assembly (GPA) 'Giovanni Buttarelli Award'.

([26]) OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/Final, 23 September 1980.

([27]) OECD, Why data governance matters.

The EDPS is following the activities of the DGP, in particular on questions linked to Data Free Flow with Trust, on government access to data held by private entities, on enforcement cooperation and on Privacy Enhancing Technologies.

The EDPS is also part of the Privacy Guidelines Expert Group ('PGEG') and follows the activities of the Working Party on Artificial Intelligence Governance ('AIGO'). Of particular importance are two Declarations adopted at the OECD ministerial meeting held on 14-15 December 2022 on a Declaration on a Trusted, Sustainable and Inclusive Digital Future ([28]) and a Declaration on Government Access to Personal Data Held by Private Sector Entities ([29]).

In relation to the last Declaration, the OECD rightly identified a critical gap affecting cross-border flows of personal data in the lack of common safeguards that countries put in place to protect privacy when accessing personal data held by private entities for national security and law enforcement purposes. In December 2022, OECD Members and the EU achieved an important milestone in addressing this gap and promoting trust in cross-border data flows when they adopted the first intergovernmental agreement in this area.

3.5. The G7 DPAs Roundtable of 'like-minded countries'

In September 2022, and for the first time ever, the EDPS participated in a Roundtable of G7 DPAs in Bonn at the invitation of the Federal DPA of Germany. This official event was organised in the context of the German Presidency of the 'Group of Seven', an inter-governmental political forum consisting of Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, as well as the European Union. The EU was represented by the EDPS, Wojciech Wiewiórowski, and the Chair of the EDPB, Andrea Jelinek. At the event, the G7 DPAs discussed a wide range of topics and the EDPS delivered a keynote speech on 'Data Free Flow with Trust and international data spaces from an EU perspective' ([30]).

The EDPS also participated in the 2023 edition of the G7 Roundtable in June 2023, in Tokyo, Japan under the leadership of the Japanese DPA. Together, G7 data protection and privacy authorities discussed joint actions on some of the key issues permeating to data protection. This included the topic of Generative AI and the topic of Data Free Flow with Trust. Exchange of views were also held on emerging technologies, and how these can embed the principles of data protection and privacy, as well as strategies to enforce data protection rules.

This forum – leading to the adoption of important communiqués and action plans ([31]) – is now established on a permanent basis and the EDPS is participating to its different working groups.

([28]) OECD, Declaration on a Trusted, Sustainable and Inclusive Digital Future, C(2023)15, 15 December 2022.

([29]) OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, C(2023)15, 14 December 2022.

([30]) EDPS, 'Data Free Flow with Trust and international data spaces from an EU perspective', Keynote Speech of Wojciech Wiewiórowski at the G7 DPA Roundtable 2022 in Bonn, Germany, 7 September 2022.

([31]) See for instance the G7 Hiroshima Summit 2023 and the G7 DPAs' Action Plan.

3.6. Providing a platform for discussion among international organisations

One of the EDPS' priorities is to generate and foster global partnerships in the field of data protection. One way for the EDPS to pursue this goal is to co-organise, on a regular basis, workshops dedicated to data protection with international organisations. These workshops, initiated by Peter Hustinx in 2005 and pursued by his two successors, are an opportunity for all international organisations to exchange their experiences and views on the most pressing issues they are facing.

The starting point for this initiative is to consider that – to some extent – the EDPS is the DPA of a *sui generis* international organisation, the EU. Over the years, the relevance and significance of these workshops have steadily grown. While the first edition of the workshop in 2005 started with few participants sitting around the table of a very small room, the latest editions of the workshop gathered over 100 participants and more than 50 international organisations with very different profiles and mandates, ranging from humanitarian action to police cooperation, from weather forecast to scientific research, from intellectual property to financial institutions.

Over the years, the EDPS had the honour to co-organise this workshop with the OECD, the European Patent Office, the European University Institute, the World Customs Organisation, the International Committee of the Red Cross, the International Organisation for Migration, the United Nations High Commissioner for Refugees, the World Food Programme and Interpol. In September 2024, for the first time, the Workshop will take place across the Atlantic in Washington and will be co-organised with the World Bank.

The continuous interest in this initiative confirms the need for a platform where international organisations can engage, share best practices and discuss common challenges, as well as increase awareness on the importance of protecting individuals' personal data around the world. As recalled by Wojciech Wiewiórowski, though they may be exempt from national laws, '*international organisations are on the front line when it comes to addressing the challenges and uncertainty of globalisation and, as a result, are expected to show leadership in improving data protection standards* ([32])'.

([32]) Wiewiórowski, W., International Organisations demonstrate dedication to data protection, *EDPS Blog*, 17 July 2018.

3.7. Other Regional and International Networks and further bilateral cooperation activities

Many other fora are of paramount importance for data protection even though they cannot be discussed in detail in this contribution.

For instance, the EDPS is a very active member of the International Working Group on Data Protection in Technology ('IWGDPT'), also known as the Berlin Group, that meets to discuss, in particular, data protection and privacy issues related to information and technology.

The EDPS also follows the activities of other networks to support regional initiatives that aim to strengthen data protection worldwide. These include the Ibero-American data protection network, the Global Privacy Enforcement Network, the Asia Pacific Privacy Forum, the French-speaking association of personal data protection authorities and the meetings of the Central and Eastern Europe Data Protection Authorities.

On top of these various multilateral fora, there is a need for a strong bilateral cooperation between authorities. For instance, the EDPS and the UK Information Commissioner's Office signed on 9 November 2023 a Memorandum of Understanding ('MoU') ([33]), which reinforces their common mission to uphold individuals' data protection and privacy rights, and cooperate internationally to achieve this goal. The EDPS is also pursuing an active and strong bilateral cooperation with many other partners within and outside the EU.

4. Conclusion

As we could see in this contribution, there are many ongoing initiatives in numerous international fora. International cooperation has moved from the 'margins' of small international affairs units to the 'mainstream' and core activities of all sectors and units of many data protection authorities. But a lot remains to be done.

Five key objectives should be kept in mind and accompany us in the years to come: (i) promoting high global standards on data protection compatible with the ones set out in the EU and in Convention 108+; (ii) favouring the emergence of a 'network of networks' to mutualise the efforts of the various international fora active in the field; (iii) exploring more interoperability among the legal frameworks whenever there is sufficient convergence and trust in particular among like-minded countries; (iv) supporting an intense practical cooperation among DPAs for an effective enforcement of data protection laws; (v) always showing humility and flexibility to adapt to the constantly evolving challenges and landscape.

I have no doubt that the EDPS will continue to play its part and take on a decisive role for another 20 years and even more.

([33]) EDPS, EDPS- ICO Memorandum of Understanding, signed on 8 November 2023.

14

The structural link between technology and data protection

Massimo Attoresi
Achim Klabunde
Xabier Lareo

The structural link between technology and data protection

Massimo Attoresi (*) **Achim Klabunde (**)** **Xabier Lareo (***)**

This article describes the evolution of the relationship between technology and data protection in light of the strategies and activities of the EDPS. It also describes the first collective efforts at international level to better understand emerging risks for human rights, while at the same time harnessing technology to protect privacy and personal data. The evolution of EDPS strategies and activities, from the supervision of trans-European Large Scale Information Systems, to the development of technology-oriented guidance and more structured technology monitoring and foresight, is closely intertwined.

1. Introduction

The protection of fundamental rights such as privacy and human dignity is tightly connected with the ways personal data can be processed by available technologies and with the pervasiveness and use of those technologies. The technology landscape is evolving rapidly, featuring more and more AI-based systems that leverage huge amounts of data, much of which relates to natural persons. The EDPS has been aware of the structural link of privacy and data protection with technology since its early days. This article highlights how the EDPS' strategies and activities have accompanied the evolution of the relationship between technology and data protection since the foundation of the Institution.

(*) Deputy Head of the Technology & Privacy Unit of the EDPS.

(**) Former EDPS Official.

(***) Head of Sector – Technology Monitoring and Foresight – Technology & Privacy Unit of the EDPS.

NB: The comments and opinions contained in this contribution are expressed by the authors in a personal capacity and may not necessarily reflect the position of the EDPS.

2. Fundamental rights and the development of information and communication technologies

First discussions about the risks to the fundamental rights of individuals from the processing of their personal data emerged in the 1960s when, 'electronic data processing' equipment was rolled out in public administrations and big companies ([1]). Already in this early stage of technological development, experts were concerned about the control that these already powerful organisations would be able to exercise over the individuals whose data they were processing, sometimes even without their knowledge. These discussions resulted in the creation of privacy and data protection laws in the 1970s, which set legal constraints for some aspects of the processing and defined the rights of the individuals concerned.

Practical experience in the enforcement of data protection laws led to the observation that technology should not only be the enabler of the processing of personal data but also contribute to providing safeguards against misuse, which could impact human dignity and freedom of individuals. Data protection authorities made efforts to understand the specific risks of emerging technologies and develop strategies for mitigation. Technological progress in the telecommunications sector and 'New Media' was an important factor in these developments.

In 1983, the International Conference of Data Protection and Privacy Commissioners ('ICDPPC') ([2]), decided to establish the International Working Group on Data Protection and Telecommunications ([3]) ('IWGDPT'), also known as the 'Berlin Group' since the Berlin Data Protection Authority led the work of the group until recently. Over the last 40 years, the Berlin Group accompanied the technological development with analysis and guidance prepared and agreed by a broad international cooperation of data protection and privacy authorities as well as other organisations from around the globe. The EDPS became an active participant of the group soon after its establishment.

Over the years, the understanding that technology is there not only to create problems, but also to contribute to solutions to protect privacy has gained traction. An important milestone was a report published in 1995 by the Dutch and Canadian Data Protection Authorities ([4]) which coined the term 'Privacy Enhancing Technologies' ('PETs'), which has since then become a field of research within computer science, featuring in numerous publications and conferences. At the 2010 International Conference of Data Protection and Privacy Commissioners

([1]) Van Alsenoy, B., Data Protection Law in the EU: Roles, Responsibilities and Liability, Intersentia, 2019, p. 155-162.

([2]) The ICDPPC was renamed Global Privacy Assembly, GPA.

([3]) The Berlin Group was later renamed as International Working Group on Data Protection in Technology.

([4]) Van Rossum, H., Gardeniers, H., Borking, J., Cavoukian, A., Brans, J., Muttupulle, N., Magistrale, N., *Privacy-Enhancing Technologies: The Path to Anonymity*, Information and Privacy Commissioner / Ontario, Canada & Registratiekamer, The Netherlands, Den Haag, 1995.

in Jerusalem, the then EDPS Peter Hustinx summarized the unsatisfactory progress in the field ([5]), and the Plenary adopted a resolution ([6]) demanding 'Privacy by Design', endorsing the principles promoted by the Ontario Privacy Commissioner Ann Cavoukian.

One of the EDPS' tasks, originally established in Regulation (EC) No 45/2001 ([7]), is to '*monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies*'.

In 2011, the EDPS decided to concentrate its technological competence in a dedicated organisational unit, which would monitor technological development and provide expertise to policy makers and in-depth understanding for supervision and enforcement efforts. The Information Technology Policy sector was established in 2012.

In addition to analysing and evaluating EU policies, such as the Cloud Computing Strategy in 2012 ([8]), one of the objectives was to provide guidance for the use of technology by the EU institutions under the direct supervision of the EDPS through the publication of guidelines on specific use cases, such as mobile devices ([9]), mobile applications ([10]), web services ([11]) and cloud computing services ([12]). Furthermore, the EDPS provided guidelines for IT related organisational and technical measures such as security measures to protect personal data ([13]), IT governance and IT management ([14]) and Data Breach notifications ([15]). All these guidelines were developed in an interactive process with the institutions concerned, giving institutional data protection officers ('DPOs') as well as IT managers the opportunity to comment on draft guidelines, and taking account of their comments as well as of the practical experiences the institutions shared through the DPO network or the inter-institutional IT cooperation. The guidelines

([5]) As expressed also in: Hustinx, P., 'Privacy by design: delivering the promises', *Identity in the Information Society IDIS*, Vol. 3, 2010, p. 253–255.

([6]) Resolution on Privacy by Design, adopted during the 32nd International Conference of Data Protection and Privacy Commissioners, 27-29 October 2010.

([7]) Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22.

([8]) EDPS Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", issued on 16 November 2012.

([9]) EDPS Guidelines on the protection of personal data in mobile devices used by European institutions (Mobile devices guidelines), issued in December 2015.

([10]) EDPS Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions, issued in November 2016.

([11]) EDPS Guidelines on the protection of personal data processed through web services provided by EU institutions, issued in November 2016.

([12]) EDPS Guidelines on the use of cloud computing services by the European institutions and bodies, issued on 16 March 2018.

([13]) EDPS Guidance on Security Measures for Personal Data Processing – Article 22 of Regulation 45/2001, issued on 21 March 2016.

([14]) EDPS Guidelines on the protection of personal data in IT governance and IT management of EU institutions, issued on 23 March 2018.

([15]) EDPS guidelines on personal data breach notification for the European Union Institutions and Bodies, issued on 21 November 2018.

were appreciated and found useful by many organisations also beyond the constituency of the EU institutions. The EDPS applied the proposed approaches and methodologies for the IT under its own control, too.

3. Ubiquitous technology, pervasive surveillance

Over the years, the limitations of information and communication technologies (which also limit the possibilities for the processing of personal data) have decreased and the usability and distribution of technologies and devices have massively increased. Today, small and ubiquitous mobile devices are often more powerful than the data centres of the 1970s and provide connectivity with high speed and capacity. Some milestones in the process were the arrival of workstations and personal computers in the 1980s and 1990s, the roll-out of the world wide web from 1989 onwards, digital mobile communications starting with GSM in the 1990s, the arrival of smart phones at the beginning of the 21st century and the first steps towards the Internet of Things in the same period. The exponential growth of the capabilities of hardware enabled completely new uses for data processing, such as social media, cloud computing, big data processing and most recently the mass accessibility of artificial intelligence solutions.

Information technology came ever closer to the individual, from the data centre at the workplace to the personal computer at home, to the smartphone in the pocket and wearable and implanted devices on or in the human body, and to most environments with more and better surveillance technology in the public space and data collection and communication integrated in home appliances. The availability of huge collections of data about each and every move and action of individuals has provided the raw material for new business models, such as behavioural advertising and for other profiling operations in public and commercial contexts. Social media companies are among the more visible actors in this field, often attracting much public scrutiny. Yet there are also less visible entities, such as data brokers and analytics companies who keep their activities out of the public attention yet are critical actors of the personal data trading ecosystem.

In 2013, the revelations by former US intelligence employee Edward Snowden brought to light an extensive network of data collection and analysis organised by US and other intelligence and national security services. Civil rights defenders and politicians were shocked by the extent of surveillance. The Internet technology community was also concerned about the use of the technology they were developing. The discussions at the 88th meeting of the Internet Engineering Task Force ('IETF') in Vancouver ([16]) in September 2013 took note of poor privacy controls within the Internet and made clear that the designers of the Internet protocols considered pervasive surveillance a risk against which the users should be protected.

([16]) IETF 88 Proceedings, Technical Plenary, 6 November 2013.

The EDPS saw the shared interest in preventing extensive tracking on the Internet as an opportunity to bring the technology and data protection community together and to explore options for common actions. After reaching out to technology forums such as the Chaos Communications Congress ('30c3') ([17]), the Free and Open Software Developers European Meeting ('FOSDEM') ([18]) and members of IETF Security Area ([19]), a first meeting bringing stakeholders together was scheduled in Berlin in September 2014 to inaugurate the Internet Privacy Engineering Network ('IPEN') ([20]). The first meeting of the IPEN network was organised by the EDPS together with the Berlin Data Protection Commissioner, the European Academy for Information Freedom and Data Protection ('EAID'), the Commission Nationale Informatique et Libertés CNIL (France), Unabhängiges Datenschutzzentrum Schleswig-Holstein ULD (Germany), Information Commissioner ICO (UK), Irish Data Protection Commissioner (Ireland) and College Bescherming Persoonsgegevens (Netherlands). The IPEN network has continued to provide a platform for the exchange between technologists and data protection experts.

Keeping up with the technological development and staying in dialogue with technology designers was also a key element in the EDPS strategy 2015-2019 ([21]), in the period of the approval and the entry into force of the GDPR ([22]) and the EUDPR ([23]), the new data protection Regulation for EU institutions.

4. Data protection by design and by default

The technological dimension of data protection is among the many areas for which the GDPR and EUDPR mean a massive step forward. Both instruments not only operationalise the principle of 'data protection by design' (now an obligation), but also incorporate the requirement of 'data protection by default'. Both requirements can be seen as the technological dimension of the principles of fair processing of personal data, mandating the implementation of data minimisation and transparency. Beyond the practical advice on how to apply the principle in its guidelines, the EDPS set its vision on how to foster data protection by design and by default ([24]) and called for a widespread adoption of privacy engineering methodologies, the use of PETs and the promotion of standardisation activities, conscious of the need for public administration

([17]) 30C3: 30th Chaos Communication Congress, 27-30 December 2013.

([18]) FOSDEM '14, 1-2 February 2014.

([19]) IETF Community Wiki, Security Area.

([20]) EDPS, Engineering privacy: the IPEN Initiative, Press Release, issued on 26 September 2014.

([21]) EDPS Strategy 2015-2019, Leading by Example, issued on 30 July 2015.

([22]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

([23]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

([24]) EDPS Opinion 5/2018 – Preliminary Opinion on privacy by design, issued on 31 May 2018.

to lead by example. As standards are being more and more established by jurisprudence as a measure for the state of the art, the development of privacy-related standards such as ISO 27701 ([25]) and ISO 31700 ([26]) became important tools for assessing the technical dimension of data protection.

In the practical work of supervision and enforcement, supervisory authorities have to assess whether controllers have implemented protective measures that represent the state of the art in technology. As in the pre-GDPR era, the EDPS has always been at the forefront in providing its contribution to assessing the data protection impact of technologies and with advice on how to be accountable in using those technologies in compliance with the applicable legislation and its principles ([27]).

5. Covid crisis: the importance of sustainable information technologies

The outbreak of the COVID-19 pandemic called for the use of any available means, including technology, to counter the uncontrolled spread of the virus. Mobile devices are equipped with sensors and protocols to measure position and proximity. This made them obvious candidates for contact tracing and infection tracking to mitigate transmission and contain the pandemics. However, mingling positional data with health related data, as well as providing public health authorities and other stakeholders with access to vast amounts of data, creates privacy and surveillance risks.

After the COVID-19 outbreak, China, Taiwan and other countries implemented strict policies supported by extensive monitoring and geo-tracking of citizens via their mobile phones. Many civil society organisations ([28]) voiced substantial concerns over digital surveillance and recalled that any surveillance measures to address the pandemic must be lawful, necessary and proportionate, as well as implement accountability and provide adequate safeguards against misuse.

The European Union started promptly investigating how to harness digital tools to fight the pandemic. New coordination and collaboration mechanisms were set up to connect national eHealth authorities under a network established by EU law, as well as an EU-wide digital contact tracing infrastructure. The coordinated approach produced several guidelines, a Common EU Toolbox

([25]) ISO/IEC 27701:2019, Security techniques -Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines.

([26]) ISO 31700-1:2023, Consumer Protection – Privacy by design for consumer goods and services, Part 1: High-level requirements.

([27]) The EDPS also contributed to the EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted on 20 October 2020.

([28]) See Joint Civil Society Statement: States use of digital surveillance technologies to fight pandemic must respect human rights, Human Rights Watch, 2 April 2020.

for mobile applications to guide the development and deployment of the national digital contact tracing apps, as well as a common infrastructure for cross-border communication of national apps.

The EDPS and the EDPB reacted to the new crisis by quickly adapting priorities and focussing on providing support and advice for effective solutions implementing the data minimisation principle, with privacy by design and by default embedded in processes and tools ([29]). The EDPS Wojciech Wiewiórowski called for an EU Digital Solidarity based pan-European approach against the pandemic ([30]) and provided continuous advice and support to the European Commission and all the EU institutions. The EDPS joined the EDPB in guiding Member States on the sustainable and compliant use of location data and contact tracing app ([31]) as well in the protection of data subjects' rights during the state of emergency at national level ([32]). Overall, the identification of sustainable solutions for contact tracing app was perhaps the first time where, at EU level, the challenge of data protection by design and by default was not any longer only for specialists but part of a public debate that touched everybody's everyday life.

The pandemic limited our movements and the possibility to gather in presence, changing the way we live, work, communicate, have fun. This has impacted digital innovation and transformation, in particular in advanced economies ([33]). Microsoft CEO Satya Nadella said, '*We've seen two years' worth of digital transformation in two months. From remote teamwork and learning, to sales and customer service, to critical cloud infrastructure and security*' ([34]). Digital industry sectors boosted by the pandemic include cloud computing, remote team collaboration and productivity, e-platforms for the provision of services, extended reality technologies and artificial intelligence. This shift has also been accompanied by a rise of cybersecurity threats and a greater amount of personal data processed. Beyond doing what was necessary to directly support the fight to the pandemic, data protection authorities, including the EDPS, moved their focus also to the use of videoconferencing and collaboration tools. This increased attention has led to some improvements in the way these products and services are used to protect data and people from a cybersecurity and data protection perspective, including within the EU institutions ([35]).

([29]) EDPS response to the COVID-19 outbreak.

([30]) Wiewiórowski W., Video address, EU Digital Solidarity: a call for a pan-European approach against the pandemic, published on 6 April 2020.

([31]) EDPB Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020.

([32]) EDPB Statement on restrictions on data subject rights in connection to the state of emergency in Member States, issued on 2 June 2020.

([33]) Jaumotte, F., Oikonomou, M., Pizzinelli, C., Tavares, M., How Pandemic Accelerated Digital Transformation in Advanced Economies, *IMF Blog*, 21 March 2023.

([34]) Microsoft Earning Press Release FY20 Q3, 29 April 2020.

([35]) EDPS Decision on the CJEU's use of Cisco Webex video and conferencing tools, issued on 13 July 2023.

6. Contributing to a sovereign digital transformation

The business model of most social media platforms relies on tracking its users and monetizing their profiles. Meta´s recent decision of charging 10 dollars monthly to users who want to avoid being tracked and profiled for advertisement purposes is case in point ([36]).

Despite growing awareness of the privacy and data protection issues surrounding some of the most popular social media platforms, the vast majority of users remain on those platforms. This is, to some extent, due to the so-called network effect, that makes social media platforms more attractive and useful the bigger they get. At the same time, the lock-in effect makes it extremely inconvenient for users to leave a platform, which is also partly due to a lack of interoperability. Another possible explanation for the lack of user reaction is a perceived scarcity of compliant, useful alternatives. Many of those platforms (as well as other IT services such as office productivity and collaboration software) are offered by providers from outside the EU, often subject to legal provisions that enable access and control of individuals' personal data in a way not compliant with EU laws and values.

To tackle those issues, the EDPS sucessfully carried out from April 2022 to May 2024 in close collaboration with the European Commission's Directorate General for Informatics ('DIGIT'), the public pilot phase of two social media platforms: EU Voice and EU Video ([37]). Other than the Commission, a few more EU institutions participated, such as the EU Court of Justice and the EU Economic and Social Committee. Both platforms were part of decentralised, free and open-sourcesocial media networks that connect users in a privacy-oriented environment. EU Voice was based on Mastodon ([38]) and provides a functionality similar to the one provided by X (formerly known as Twitter). EU Video was based on PeerTube ([39]) software and provides video hosting and streaming capacities similar to those offered by other video platforms such as YouTube.

7. Data protection audits go digital

Since its creation, the EDPS has taken up the responsibility to supervise IT systems processing personal data under the responsibility of the EU institutions, including those called Large-Scale IT Systems, trans-European systems usually supporting EU policies via the exchange of a large amount of data among Member States and centrally with the EU institutions. These IT systems are all based on a legal basis which, among other provisions, defines the conditions

([36]) Meta, Facebook and Instagram to Offer Subscription for No Ads in Europe, 30 October 2023.
([37]) EDPS, Press Release, EDPS launches pilot phase of two social media platforms, issued on 28 April 2022.
([38]) https://joinmastodon.org
([39]) https://joinpeertube.org

under which personal data may be processed and under what safeguards ([40]). A large share of these IT systems, such as the Schengen Information System, the Visa Information System, etc. are mainly used for asylum, border management and migration policies. The EDPS, together with national data protection authorities, performs a thorough supervision, including at technical level, to verify that the data protection by design and by default is implemented on those IT systems, to ensure that privacy, data protection and relevant citizens' fundamental rights are respected and EU values are upheld when using them.

The experience on Large-Scale IT Systems has upskilled EDPS audit capabilities in other contexts, which led to the creation of tools for advanced automated support to certain audits.

As in many other public and private organisations, the websites of EU institutions process personal data. In 2016, the EDPS issued guidelines to help them comply with the applicable privacy and data protection legal framework ([41]). In 2018, the EDPS decided to inspect EU institutions for their implementation of the recommendations provided in the EDPS guidelines. Given the nature of the processing and the many websites, the EDPS decided to collect evidence on website compliance automatically and remotely. In the absence of existing tools meeting the EDPS requirements, the EDPS developed its own tool, the Website Evidence Collector (WEC), which automated the collection of evidence from the targeted websites ([42]).

The EDPS considered that the Website Evidence Collector could be helpful for other stakeholders, too. Data protection authorities could use the WEC for their own investigations. Data controllers could use the WEC on their websites to find evidence that helps them self-assess their compliance. Consequently, the EDPS decided to make the WEC publicly available. In 2019, the EDPS received the Global Privacy and Data Protection Award for innovation for its efforts to develop the WEC ([43]).

As the EDPS is a supporter of open source transparency and control features, we published the Website Evidence Collector source code under the European Union Public License ('EUPL-1.2') in July 2019. The software is available for download on a dedicated EDPS webpage, the European Commission's collaborative platform Joinup and soon on the EU institutions' own open-source projects code development platform code.europa.eu.

The EDPS continues to improve the WEC and has published several software updates. Furthermore, as other open source projects, the WEC has benefited from the contribution of IT experts from other data protection authorities and private companies.

([40]) See more on the legal basis of Large scale IT systems in the contribution by Coudert, F., Quintel, T., and Sajfert, J., 'The Area of Freedom, Security and Justice', Chapter 10.

([41]) EDPS Guidelines on the protection of personal data processed through web services provided by EU institutions, issued on 7 November 2016.

([42]) The WEC is published and is available for download on the EDPS website.

([43]) EDPS, EDPS software receives Global Privacy and Data Protection Award, Press release, 22 October 2019.

8. Monitoring technology developments

The EUDPR confirmed the task of the EDPS to monitor relevant technology developments, insofar as they have an impact on the protection of personal data ([44]). The EUDPR also reinforced the need to take account of the state of the art in the principle of data protection by design and by default.

The EDPS realised that technology monitoring to support the EDPS advisory and supervisory tasks often reached only a limited audience (e.g. the institutions concerned in a consultation, investigation or audit). To share our assessment with a broader audience outside the EU institutions, the EDPS decided to publish regularly fact sheets on new technology that explain in plain, accessible language factual descriptions of how these technologies work, preliminary assessments on data protection impact and a list of recommended readings. In July 2019, the EDPS published the first issue of the so-called TechDispatch on smart speakers and virtual assistants. Since then, the EDPS has published eleven TechDispatches that deal with topics as diverse as quantum computing ([45]), facial emotion recognition ([46]) or explainable AI ([47]). Recognised by the wider data protection community as an innovative tool ([48]), the TechDispatch has become an integral part of the EDPS's pursuit for a safer digital future.

9. Accelerated adoption of Artificial Intelligence

Researchers introduced the concept of *Artificial Intelligence* ('AI') as early as in the 1950s. However, only during the last decade it became subject to broader public attention due to a number of fascinating achievements. In the 2010s, some types of AI, such as machine-learning and deep-learning systems, started to substantially improve their performance. This was possible due to the broader availability of large data sets for training, large computing power at decreasing costs, and improved algorithms.

Due to their potential to enable widely used commercial applications, the last year and a half saw the rapid and overwhelming deployment to the public of Large Language Models ('LLMs') and Generative AI ([49]). These systems are particularly resource-intensive. The increasing computing power and data requirements shrank the number of entities that could develop and run top performing generative AI systems. At a certain point, the development of

([44]) Article 57(1)(h) EUDPR.

([45]) EDPS, TechDispatch #2/2020: Quantum Computing and Cryptography, 7 August 2020.

([46]) EDPS, TechDispatch #1/2021 – Facial Emotion Recognition, 26 May 2021.

([47]) EDPS, TechDispatch #2/2023 – Explainable Artificial Intelligence, 16 November 2023.

([48]) In the Global Privacy and Data Protection Awards 2021 of the Global Privacy Assembly (GPA), TechDispatch won in the category Education and public awareness. The EDPS was awarded another GPA Award in the Category Innovation in 2023 for the TechSonar.

([49]) Generative AI is a subset of AI systems designed to produce a wide and general variety of outputs, capable of a range of tasks and applications, such as generating text, image or audio, using generative models. LLMs are a type of generative AI systems designed to learn grammar, syntax and semantics of one or more languages to generate coherent and context-relevant language.

competitive high-performance LLMs seemed to be something that only the most resourceful technology companies, such as Google, Meta or OpenAI, could achieve. The training of GPT-4, one of the top LLMs, costed over 100 million dollars ([50]). However, recent developments changed that trend and made LLM development and running more broadly available ([51]).

The rapid adoption of AI systems by individuals and organisations has triggered complex and still unresolved data protection concerns. Evidence of it are the ongoing investigations by EU data protection authorities on the processing of personal data by ChatGPT and the creation by the EDPB of a Task Force ([52]) to foster cooperation and to exchange information on possible enforcement actions.

Adoption of AI has already commenced in EU institutions, too, and the EDPS faced its first supervisory case.

In March 2021, the EDPS issued an Opinion on a prior consultation requested by Europol on the development and use of machine learning models for operational analysis ([53]). The Opinion concluded that the EDPS was not in a position to assess the compliance of the processing operations and included a series of recommendations to ensure that Europol would avoid breaching Regulation (EU) 2016/794 ([54]).

In the following months, the EDPS and Europol followed-up on the recommendations issued. In September 2021, the EDPS conducted, jointly with experts of some EU Member States, the annual Europol inspection. A substantial part of this inspection focused on Europol's development and use of machine learning technologies.

As a result of all the information gathered, the EDPS set a number of requirements so that Europol might continue to process personal data in the development of their AI system. The EDPS also required Europol to conduct data protection impact assessments on each tool and on the interface integrating them before their deployment.

The EDPS' remit as data protection authority encompasses the processing of personal data by EU institutions when using or developing AI systems. In addition, the recently adopted AI Act has designated the EDPS as the as notified

([50]) OpenAI's CEO Says the Age of Giant AI Models Is Already Over, Wired, 17 April 2023.

([51]) The appearance of new parameter efficient fine-tuning techniques like LoRA in 2021 allowed to greatly reduce the amount of resources needed to train an LLM. In May 2022, the publication of a research (the chinchilla paper) showed that there is an optimal set of values when selecting computing power, model size and training dataset size. In February 2023, Meta presented LLaMA a new LLM much smaller than GPT-3, which could compete in performance. In March 2023, LLaMA weights (the knowledge stored in a trained neural network) were leaked and within a few days local running versions of LLaMA appeared for Mac, Windows and even high-end mobile phones.

([52]) EDPB, EDPB resolves dispute on transfers by Meta and creates task force on ChatGPT, Press release, 13 April 2023.

([53]) EDPS Opinion on a Prior Consultation requested by Europol on the development and use of machine learning models for operational analysis, issued on 5 March 2021.

([54]) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), OJ L 135, 24.5.2016, p. 53.

body, market surveillance authority and competent authority for the supervision of the development, provision or use of AI systems by EU institutions. This new role will entail a substantial development in the EDPS' supervisory and advisory tasks in relation to AI.

10. 'The best way to predict the future is to create it' ([55])

Aware of the ongoing COVID-19 crisis and the overall challenges ahead, the EDPS integrated a Foresight pillar in its Strategy 2020-2024, oriented to shaping a safer digital future ([56]).

The TechDispatch is an essential component of that pillar. But there is more. Using the words of EDPS Wojciech Wiewiórowski, '*instead of reacting to new emerging technologies when their added value and risks for society are already visible, we should be able to anticipate their developments. In this way, we can foresee the risks and better support the value-creation process of these technologies. As a result, we might be able to nudge their developers and their development towards respecting fundamental rights and interests of individuals, reducing their risks from the earliest stages of their adoption*' ([57]).

This is the rationale behind the TechSonar, our new *'tool for navigating the surface of the complexity and uncertainty of the tech domain in general'* ([58]) The TechSonar reports on emerging technologies that, in the short and medium period, might become mainstream and have a meaningful impact on people's privacy, data protection and relevant fundamental rights.

The EDPS issued its first TechSonar reports in December 2021 and since it has tackled technologies ranging from biometric continuous authentication ([59]) and synthetic data ([60]), to extended reality ([61]) and AI large language models ([62]).

The TechSonar methodology has been continuously evolving and has undergone further review also this year, though a process combining resource management, opportunities and EDPS priorities. The EDPS intends to continuously fine-tune its foresight methodology and action, possibly seeking synergies also with other actors (e.g. other data protection authorities who have undertaken a similar exercise). In an ever more complex technological and digital policy landscape, the dream would be to evolve more and more towards an anticipatory posture, ideally expanding it to all EDPS tasks, being better prepared in the present to influence the future.

([55]) Quote attributed to Abraham Lincoln and Peter Drucker.
([56]) EDPS Strategy 2020-2024: Shaping a safer digital future, issued on 30 June 2020.
([57]) Wiewiórowski W., 'Technologies worth monitoring', foreword to TechSonar 2021-2022 Report.
([58]) EDPS Blog, TechSonar: technologies worth monitoring, 28 September 2021.
([59]) Vemou, K., Biometric continuous authentication, EDPS TechSonar.
([60]) Riemann, R., Synthetic data, EDPS TechSonar.
([61]) Benardo, V. Extended reality, EDPS TechSonar.
([62]) Lareo, X., Large language models (LLM), EDPS TechSonar.

15

‘A clear imbalance between the data subject and the controller’: data protection and competition law

Christian D’Cunha
Anna Colaps

‘A clear imbalance between the data subject and the controller’: data protection and competition law

Christian D’Cunha (*) **Anna Colaps (**)**

The early 2010s saw the rapid emergence of powerful companies whose business model depended on the exploitation of personal data. The EDPS in its ‘preliminary opinion’ of 2014 launched a debate in the EU about how enforcement, in particular through the interaction of competition and data protection authorities, could adapt to address this challenge. Two years later, the EDPS attempted to move beyond largely theoretical discussions with the concrete initiative of the Digital Clearinghouse, a forum for enforcement authorities and other experts from various fields concerned with the regulation of the digital economy. The intention was to reflect on common lessons learned from previous enforcement and to pave the way for possible collaboration in future actions. It spurred the EU into adopting a new generation of laws of asymmetric obligations which targeted the most powerful companies with heavier compliance burdens. The history of the issue illustrates the fundamentals about power, where consent and other principles of data protection cannot operate in a radically unequal environment. As the EDPS argued, in an era of continued concentration of power, data protection authorities have an important role if there is to be a shift away from exploitative business models towards sustainable data practices in the interest of society and individuals. However, such a transition may require a ‘whole-of-government’ approach not only to enforcement but also, crucially, to the dispersal of digital power.

(*) Official, European Commission, and former Head of Private Office, EDPS. The views expressed here are entirely his own.
(**) Member of Cabinet of the Supervisor, EDPS. The views expressed in this chapter are entirely her own.

> *...consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller...*
>
> (Recital (43), GDPR).

1. Introduction

All data controllers are equal before the GDPR, but some are more equal than others.

Market power in the digital economy implies the power to do things with data which rivals cannot, and which are hard for data subjects to contest. In these markets, control over data and computing power is assumed to be primordial. It allows those wielding such control to impose unfair contractual terms on other businesses as well as take-it-or-leave-it privacy policies on individuals. In the middle of the 2010s, a handful of private companies emerged as the most valuable companies in the world, and it soon became clear that they would use their limitless resources to counter any attempt to force them to relinquish lucrative data practices. It therefore made perfect sense for authorities responsible for supervising separate but related areas of law to find ways to work together where there were common interests.

This article reviews developments since the EDPS published in 2014 its pioneering Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data ([1]), and the initiative of the Digital Clearinghouse for authorities to work together towards common aims. It reflects on the underlying logic behind the policy intervention, namely that data protection in the digital economy is increasingly a function of power, and in particular a function of market power which is the concern of competition enforcement. It then looks ahead to the strategic needs of data protection and other fundamental rights as we enter an era of geopolitical uncertainty and the continuing concentration of power and resources.

2. More in common

It was as the EDPS approached its 10th year as an institution that it began to grapple with notions of power. Then Supervisor Peter Hustinx gave a speech ([2]) at a seminar entitled 'Data Protection Law in the Context of Competition Law Investigations' in Brussels in 2013. He addressed the textbook procedural question of the constraints on competition authorities in handling personal data, but went considerably further. He reflected on the dissenting opinion of Commissioner Pamela Jones Harbour in the US Federal Trade Commission

([1]) EDPS, Preliminary Opinion on Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, issued on 26 March 2014.

([2]) EDPS speech on Data Protection and Competition: interfaces and interaction, Data Protection Law in the Context of Competition Law Investigations Seminar, 13 June 2013.

decision to clear the Google Double/Click merger in 2007 and on the synergies between antitrust and privacy. After acknowledging the distinctiveness of the two regimes, he said,

> *But there is a common aspect to both areas: the violation of these rules harms the consumer/individual/data subject, and they also address the wider public interest of a free and open society based on the rule of law and not only on survival of the most powerful.*

He added,

> *We are reflecting about a possible scenario whereby an infringement of data protection rules by a dominant firm could substantiate an abuse pursuant to the competition law criteria, but at this stage we do not have an answer to this complex issue yet.*
>
> *At the same time, a finding of dominance from a competition point of view could support an investigation on the legality of consent to the processing given by a certain individual: to what extent can consent be valid if the consumer has little or no alternative choice of provider? The issue of "significant imbalance" between parties and its impact on consent now also plays a role in the discussion on the proposed DP Regulation.*

These ideas were expanded in a type of policy document not previously issued by EDPS. The March 2014 preliminary opinion on 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' compared the three EU legal frameworks and suggested that there was so much conceptual overlap that more coordination between enforcers was both logical and necessary. Among the various overlaps, it highlighted fairness as a shared core concern for all three of the frameworks. Business models that involved the intensive processing of personal data had become so lucrative that a handful of companies were becoming the most valuable in the world through the provision of services in exchange for personal data and attention. Insofar as dominant firms in a market had, according to CJEU case law, a 'special responsibility' not to harm competition ([3]), how is this responsibility to be interpreted when monetisation of personal data is at the core of their economic activities? How does the rarely contested notion of exploitative abuse by a dominant undertaking compare with the unfair exploitation of data subjects and consumers? How should merger control respond to the fact that major acquisitions by big tech were motivated, at least in part, by the prospect of acquiring troves of user data? The EDPS therefore recommended a review of competition legislation for 21st century digital markets, including its interfaces with data protection and other areas of law, and exploring possibilities for productive interaction with other relevant authorities.

It was a mark of the maturity of data protection, its profile having been raised by the feverish GDPR negotiations ongoing at the time, that it was now also being seen

([3]) Judgment of the Court of Justice of 9 November 1983, *Michelin/ Commission*, C-322/81, ECLI:EU:C:1983:313, paragraph 57; Judgment of the Court of Justice of 6 December 2012, *AstraZeneca/Commission*, C–457/ 10 P, ECLI:EU:C:2012:770, paragraph 134.

in the wider context of law, politics and market power in the digital economy. The document was followed by a workshop ([4]) with regulators, practitioners, NGOs and academics, including a senior representative of the European Commission's DG Competition, the then chair of the US FTC and former Commissioner Jones Harbour herself. The conversation was considered so tentative that it was held behind closed doors. Early reaction from the competition world in the EU was generally polite but dismissive ([5]), often with the implication that data protection as an emerging area of EU law should focus on its own enforcement tools rather than contaminating the ecosystem of a more established one. The companies in the crosshairs of both EU level data protection and competition action (sanctions in the area of consumer protection are less onerous and rarely attract attention), and the think tanks and industry bodies they funded, were at pains to insist that the legal frameworks were entirely distinct and not to be mixed.

The debate therefore began technical and theoretical, but pressure was building to have a framework for competition law to engage with the digital economy and the phenomenon of so-called 'two-sided markets'. In particular, US west coast companies were seen to be innovating and operating within a less constrained regulatory environment, and had come to dominate new and emerging markets on a global scale, partly through a frenzy of mergers and consolidation which were rarely, if ever, contested or blocked by regulators. There was concern that the GDPR was being weaponised to avoid compliance ([6]).

An actual test case did however present itself immediately after the preliminary Opinion, with the proposed acquisition in 2014 by Facebook of WhatsApp, in which the social media giant offered USD 19bn for a startup which that year generated a mere USD 10m, but which had around half a billion active users. Data protection concerns were broadly dismissed, however, and the merger was waved through on both sides of the Atlantic ([7]). In 2017 the Commission established that Facebook had provided incorrect or misleading information during the WhatsApp merger review, when the company claimed that it was not technically possible to match user identities automatically, and imposed a fine of EUR 110m ([8]).

The debate further intensified with Ashley Madison and other scandals ([9]), and what was perceived as a collective impotence to the discipline using existing

([4]) EDPS, Report on workshop on Privacy, Consumers, Competition and Big Data, issued on 11 July 2014.

([5]) E.g. Chillin'Competition, On Privacy, Big Data and Competition Law (2/2) On the nature, goals, means and limitations of competition law.

([6]) E.g. in 2018, some economic operators claimed that the GDPR prevented them from engaging in basic cooperation in the context of EU investigatory activities, for example from disclosing at all personal data in a competition law case. EDPS, Investigative activities of the EU Institutions and the GDPR, issued on 22 October 2018.

([7]) European Commission, Case No COMP/M.7217 – Facebook/Whatsapp, Article 6(1)(b) Non-opposition, 3 October 2014.

([8]) European Commission, Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover, Press Release, 18 May 2017.

([9]) See the Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner, 22 August 2016. In the words of Privacy Commissioner of Canada Daniel Therrien, '*Privacy breaches are a core risk for any organization with a business model based on the collection and use of personal information*'. Office of the Privacy Commission of Canada, 'Ashley Madison investigation finds security measures lacking; fictitious security trustmark was 'deceptive'', News release, 23 August 2016.

tools a market which had come to assume that even the most sensitive personal data was an infinite resource to be mined at minimal cost, with potential fines an acceptable business risk.

3. The Digital Clearinghouse 1.0

In an attempt to operationalise the theoretical arguments of the 2014 Preliminary Opinion, and having noticed that policy discussions had not delivered any concrete action ([10]), the EDPS launched its Digital Clearinghouse initiative. This was a forum intended to bring together regulators from related areas to discuss how to work coherently in addressing common challenges towards common goals. It involved mainly data protection, competition and consumer protection authorities willing to cooperate and exchange information on cases where their respective competencies would overlap, and later extended to other regulators competent in the digital sphere, notably media regulators and financial authorities ([11]). Although the need for dialogue and cooperation between authorities would seem axiomatic, the Clearinghouse opened amidst some criticism and opposition in a modest meeting room on rue du Trône in Brussels. The brave delegates attending the first meetings would still remember the difficulties of provoking a real discussion. It was not a given that authorities would engage into a discussion on tackling jointly (or maybe passing on to other regulators) cases for which they would traditionally feel in charge.

The Digital Clearinghouse reflected a growing realisation of the relevance of scale in potentially harmful data practices. The GDPR is a neutral baseline applying more or less equally, whether it concerns a small business or a multinational company. The legal obligations contained in the GDPR do not generally depend on an organisation's size or position in a market. That said, the roots of a more differentiated approach to legal obligations with respect to personal data processing are arguably present in the GDPR itself, at least in the risk-based approach and in the principle of accountability which imply a greater burden of compliance ought to fall on the bigger players in digital markets. Nevertheless, it is with the most recent generation of laws, such as the Digital Markets Act, Digital Services Act, Data Act and AI Act, that the EU has attempted to calibrate legal obligations according to relative power.

4. Privacy and power

Brussels on the morning of Wednesday the 9th November 2016 was how you would expect it to be: grey, wet, cold, miserable. Its policymaking population was in a catatonic state at the overnight news of the US presidential elections. The European Data Protection Supervisor, Giovanni Buttarelli, was in a taxi rattling over the cobbled Places des Palais which runs along the Royal Palace

([10]) EDPS, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, issued on 23 September 2016

([11]) The project later transited to an independent cooperation platform managed by Research Centre in Information, Law and Society (CRIDS), University of Namur, the Institute for Law, Technology, and Society (TILT), University of Tilburg and the European Policy Centre (EPC).

on his way to give the keynote speech at the IAPP Congress. He was taking a counter-intuitive, glass-half-full perspective at the big news. The President-elect could end up a good thing for privacy, Buttarelli speculated, because, for a man with so much to hide, the promotion of robust privacy laws could well be in his interest. However, he said as much in his keynote. Whether it was sincere or feigned, this optimism turned out to be misplaced. As events since that day have demonstrated, the hiding of the secrets of the powerful has little if anything in common with the universal human right to privacy.

It has become impossible to talk meaningfully about the fundamental rights to privacy and to data protection without talking also about power. Power in the digital society means the ability to collect and extract value from data. Manipulation techniques, dark patterns, keeping platform users within 'walled gardens', making it easy to be tracked but virtually impossible to avoid being tracked or to compel a company to delete your data: this is how big powerful digital companies have been able to accumulate more personal data than any other organisation – public or private – had ever before, and often claiming that they had acquired people's individual consent to do so. This concerns not only 'consumers' of digital services, but also workers in the gig economy or in ecommerce warehouses, whose right to access data collected about them, or to limit workplace surveillance, is especially hard to exercise ([12]). Needless to say, the most vulnerable groups in society, such as children, low-paid workers, people with health problems and migrants, are also the most vulnerable to exploitation of their data.

This 'data power' goes well beyond the ability of big tech to exploit the users of its own 'inventory' of platforms, applications and websites. It is their market power that enables them to strike favourable deals with almost all other companies with an Internet presence. Ordinary individuals cannot by any means control such deals, according to which data from an individual's use of 'third party' apps, games, VPNs, websites and so on are automatically shared with multiple mysterious 'partners', vendors and third parties, among whom are to be found, inevitably, other major tech companies.

It is through their market power that big tech is able to evade transparency and audits of their data practices, to the extent that advertisers often have no idea whether their ad spend is effective ([13]). It is also market power that enables a company to deploy limitless resources, in the form of lobbying, litigation or revolving doors, to avoid enforcement completely, or to defer it indefinitely.

It is power that enables them to convince policymakers and enforcers that data collected is no longer to be considered 'personal data' over which a person has fundamental rights, but rather anonymised and aggregated and accordingly a business secret – that is, their property. This is now becoming a

([12]) See CNIL, Employee monitoring: CNIL fined AMAZON FRANCE LOGISTIQUE €32 million, 23 January 2024.

([13]) European Commission, Directorate-General for Communications Networks, Content and Technology, Armitage, C., Botton, N., Dejeu-Castang, L. et al., *Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers – Final report*, Publications Office of the European Union, 2023.

particularly acute challenge in the age of generative AI and Large-Language Models (LLMs), which are built on the scraping of 100s of terabytes of data – much of it personal – from the web, and the newly-accepted new orthodoxy that AI's benefits can only be realised through scale, untrammelled by 'legacy' regulation like data protection and antitrust. It is the same imperative, or will-to-scale, that lay behind the slogan of 'big data' in the mid-2010s. The Big Data hype of the time appears minuscule compared with the media and market hysteria that has followed the launch of ChatGPT in late 2022. Now, as then, the biggest companies who have gained a leading edge in a nascent market are demanding to be regulated – but on terms that they themselves intend to influence and determine.

The scale and reach of these private entities enable them to capture and distort the narrative: pretending, for instance, that the issue is whether or not to receive 'targeted ads', rather than the individual's right to be in control of their own profile, their own data; or that the issue is that users are suffering 'cookie fatigue', obscuring the real issue of whether such data should have been harvested in the first place. The ability of corporations to succesfully dictate the terms of the debate also lands among regulators: data protection authorities discuss the appropriateness of fees that users may be requested to pay to avoid targeting, but the legitimacy and sustainability of such models are rarely questioned. With generative AI, the narrative has also been captured. It focuses on putative existential threat to humanity of artificial general intelligence (AGI): a hubristic concept that assumes infinite potential of the technology while distracting from the here-and-now impact on privacy, intellectual property and the exacerbation of social inequality. The regulatory dialogue and resulting actions are therefore perceived as largely reactive to the business imperative of the largest corporations.

Ever greater concentration of infrastructure, computing power and data, first noted by Commissioner Jones Harbour in 2007, continues apace and shows no sign of abating. Driven at least partly by the excitement around generative AI, there are already companies valued at over a trillion dollars, and it is expected that there will be the first trillionaire before the end of the 2020s. This has attracted the attention of enforcement bodies. The FTC in January 2024 opened an investigation into AI investments and partnerships by dominant companies along the entire stack of computing power, data and infrastructure ([14]). The UK Competition and Markets Authority (CMA) has studied concentration in foundation models ([15]). The European Commission and the French competition authority are both running consultations on competition in AI ([16]). The CMA ([17])

([14]) Federal Trade Commission, FTC Launches Inquiry into Generative AI Investments and Partnership, Press Release, 25 January 2024.

([15]) Competition and Markets Authority, AI Foundation Models review, 18 September 2018.

([16]) European Commission, Commission launches calls for contributions on competition in virtual worlds and generative AI, Press Release, 9 January 2024.

([17]) Competition and Markets Authority, CMA seeks views on Microsoft's partnership with OpenAI, Press Release, 8 December 2023.

and the European Commission are also reviewing whether they can investigate the Microsoft/OpenAI partnership under their respective merger control laws ([18]).

Enforcers are increasingly wary that the same narrative of scale is driving the debate, as in the case of 'big data' ten years ago. It is used to justify the necessity of dominance for a market to succeed, but it is likely at odds with the longer-term interests of protection of the data and privacy of individuals. Anyone who attempts to interrogate an LLM-based chatbot about their compliance with GDPR, what personal data are processed in the training data and in providing the service, will encounter an uncanny evasiveness and obfuscation worthy of the best corporate lawyers.

Viewed through this lens, the existential risk to the fundamental rights to privacy and to data protection is an enduring imbalance between '*the haves and the have-nots*'. In other words, those with the power and means to protect their data, to preserve their privacy and guard their secrets, will continue to do so, while for everyone else it will be far less easy. To cite a banal example, already discussed in the 2014 Preliminary Opinion, this can involve by paying a premium to use a particular service – witness in particular the controversy surrounding Meta's decision to charge users to forego targeted advertising. On a more sophisticated level, those with the resources restrict data processing deploy expensive legal tools like non-disclosure agreements and gagging procedures. Most people including the most vulnerable, however, remain trapped in business models which rely on the monetisation of their data in order to access services.

5. Consent as the battleground

The EU's co-legislators who adopted the GDPR were evidently alive to the risk that imbalances of power have the potential to severely hamper an equitable upholding of rights and obligations. Article 5 states, as the first principle of data protection, that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. There has been a tendency among lawmakers and controllers to treat the legal basis of consent as a panacea and the default guarantee against abuse. Consent has subsequently become perceived as an inconvenient obstacle to data processing, with the consequence that it has become a commodity to be 'managed', instead of a vital safeguard to preserve self-determination in the information age. Valid consent is tightly defined in the GDPR as freely given, specific, informed and unambiguous. Can such a principle withstand radical power imbalances? The GDPR, as a product of its time, assumed the most unequal relationship to be between an individual and the state, rather than between an individual and a private company. In a society where certain corporations seem in many ways at least as powerful as a sovereign state, it is open to question whether an ordinary

([18]) European Commission, Commission launches calls for contributions on competition in virtual worlds and generative AI, Press Release, 9 January 2024.

individual's consent to data processing by that company can be legitimate. The 2020 EDPB guidelines on consent remain within the logic of the GDPR, but the implication is clear ([19]):

> *imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by the WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.*

Such questions appear to extend beyond the technical application of the law. Another notable policy intervention by EDPS in the 2010s, and the flagship initiative of the Buttarelli mandate, was developing the notion of 'digital ethics'. The 2015 Opinion, 'Towards a Digital Ethics' ([20]), contained the acknowledgement that with data processing 'feasible, useful or profitable did not equal sustainable', and argued for 'accountability over mechanical compliance with the letter of the law'. An ethical approach to data protection implied that the deployment of certain technologies involving the processing of personal data, such as AI, could conceivably be justified on legal grounds but should rejected by society because of its harmful externalities and impact on human dignity. Consent cannot be a panacea for such practices. The Digital Ethics Opinion was a precursor to the negotiations on the EU AI Act whose most hotly debated provisions involved outright prohibition of certain applications of AI, like biometric categorisation systems using sensitive characteristics and emotion recognition in the workplace and in schools.

6. Exercises in coherent enforcement

The focus on the role of competition law in this space continues to be discussed. After an apparent enforcement hiatus in the digital economy following the 2001 *US vs Microsoft* case, the EU was the first mover in attempting to address exclusionary abuse of dominance in digital markets, when the Commission opened its inquiry into self-preferencing in Google Shopping in 2010, the first of many which would be launched in subsequent years.

The 2019 report on Competition in the Digital Age ([21]), carried out at the request of the EU Competition Commissioner, suggested modest intervention in the areas of self-preferencing, opening up access to data controlled by dominant companies and prevention of 'killer acquisitions', and paved the way to the Digital Markets Act proposal. The three academic authors remained firmly within the traditional logic of competition law, seeking opportunities to open up access

([19]) EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020.

([20]) EDPS Opinion 4/2015 'Towards a new digital ethics', issued on 11 September 2015. The EDPS subsequently set up an expert group and made this the theme of the 2018 International Conference of Privacy and Data Protection Commissioners (now Global Privacy Assembly) which it hosted in Brussels.

([21]) European Commission, Directorate-General for Competition, Montjoye, Y., Schweitzer, H., Crémer, J., *Competition policy for the digital era*, Publications Office, 2019.

to data to competitors, albeit balanced against 'other policy concerns such as … the need to protect privacy (where personal data is concerned)', rather than engaging with broader strategic questions of power and sustainability.

Also in 2019, Google announced its intention to acquire the wearable and fitness tracking company Fitbit. This reignited public debate on the further concentration of control over sensitive – in this case, health-related – data. In its first public acknowledgment from the EDPB, the EU data protection authorities voiced concerns that the '*possible further combination and accumulation of sensitive personal data regarding people in Europe by a major tech company could entail a high level of risk to the fundamental rights to privacy and to the protection of personal data*" ([22]). Nevertheless, the merger was again cleared ([23]). Some may detect a subtle evolution in approaches to big tech mergers more recently. In January 2024, Amazon abandoned its proposed acquisition of iRobot, in the face of objections from the European Commission and the FTC, as well as strong opposition from a privacy perspective given the track record of the two companies' products in monitoring the intimacy of people's homes.

The most high-profile attempt to apply a genuine intersectional approach to competition and data protection law is the Bundeskartellamt's action against Facebook since 2019. In its 2019 decision, the Bundeskartellamt found an abuse of market power based on the extent to which Facebook collected, used and merged data in a user account. In particular, the company was found to have abused its dominant position through its data processing being not compliant with the underlying requirements of the GDPR and, in particular, with Article 6(1) and Article 9(2) of the GDPR ([24]). The competition authority considered the '*European data protection provisions as a standard for examining exploitative abuse*'. Facebook filed an appeal with the Düsseldorf Higher Regional Court questioning *inter alia* the authority of the national competition authority to enforce data protection rules under antitrust laws. The Court requested a preliminary ruling from the CJEU under Article 267 TFEU.

The subsequent CJEU ruling of July 2023, addressed for the first time several of the questions raised by Peter Hustinx in his 2013 speech and by the EDPS 2014 Preliminary Opinion, thus dismantling the widespread assumption that privacy and data protection were an issue exclusively for data protection authorities. In its Preliminary Ruling ([25]), the Court held:

> *… the existence of such a dominant position may create a clear imbalance, within the meaning of recital 43 of the GDPR, between the data subject and the controller, that imbalance favouring, inter alia, the imposition of conditions that are not strictly necessary for the performance of the*

([22]) EDPB, Statement of privacy implications of mergers, issued on 19 February 2020.

([23]) In its press release, the Commission stated it had '*worked in close cooperation with … the European Data Protection Board*'; See European Commission, Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions, Press Release, 17 December 2020.

([24]) Bunderskartellamt, Bundeskartellamt prohibits Facebook from combining user data from different source, Press Release, 7 February 2019.

([25]) Judgment of the Court of Justice of 4 July 2023, Meta Platforms and others (Conditions générales d'utilisation d'un réseau social), C-252/21, ECLI:EU:C:2023:537.

> *contract, which must be taken into account under Article 7(4) of that regulation. In that context, it must be borne in mind that, as stated in paragraphs 102 to 104 above, it does not appear, subject to verification by the referring court, that the processing at issue in the main proceedings is strictly necessary for the performance of the contract between Meta Platforms Ireland and the users of the social network Facebook (para 149).*

Recognising that competition authorities are competent to decide on privacy and data protection, it stated:

> *subject to compliance with its duty of sincere cooperation with the supervisory authorities, a competition authority of a Member State can find, in the context of the examination of an abuse of a dominant position by an undertaking within the meaning of Article 102 TFEU, that that undertaking's general terms of use relating to the processing of personal data and the implementation thereof are not consistent with that regulation, where that finding is necessary to establish the existence of such an abuse (para 62).*

It also acknowledges the duty of sincere cooperation between competition and data protection authorities:

> *In view of this duty of sincere cooperation, the national competition authority cannot depart from a decision by the competent national supervisory authority or the competent lead supervisory authority concerning those general terms or similar general terms. Where it has doubts as to the scope of such a decision, where those terms or similar terms are, simultaneously, under examination by those authorities, or where, in the absence of an investigation or decision by those authorities, the competition authority takes the view that the terms in question are not consistent with Regulation 2016/679, it must consult and seek the cooperation of those supervisory authorities in order to dispel its doubts or to determine whether it must wait for them to take a decision before starting its own assessment. In the absence of any objection on their part or of any reply within a reasonable time, the national competition authority may continue its own investigation (para 63).*

At the same time, it appears to open the possibility of charging users for access to a platform, if those users refuse to consent to the use of their data for certain purposes.

> *Thus, those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations (para 150).*

The motivation here appears to be prevention of digital exclusion of those who wish to exercise control of the use of their own data. Much rides however on the

notion of 'necessity' of such a fee, on what might be considered an 'appropriate' fee, and on who ultimately should make such a judgment, given that a price cannot be placed on a fundamental right which should be enjoyed equally by all citizens. For this, as with all related questions, dialogue between relevant experts including the authorities seems indispensable, but the fundamental question of scale cannot be ignored: if a monopolist player established a certain price that cannot be ever challenged by a competitor, this could conceivably form a basis for competition enforcement.

7. Digital Clearinghouses 2.0

The length of enforcement processes, and the seemingly endless stalling tactics of powerful defendants has led to discussion of solutions like the regulation of monopolies public utilities (the US equivalent being 'common carriers') such that they would be forbidden to discriminate traffic on their platforms, or structural remedies referred to as divestiture or breaking up. The EU's reaction meanwhile has been mostly a regulatory turn to attempt to outlaw rather than punish abusive behaviour, including where it pertains to the use of personal data.

The recent spate of digital regulations in the EU, notably the Digital Services Act, Digital Markets Act and Data Act, set down in effect asymmetrical rules where rights and obligations are to a degree functions of risk and market power, and could together provide a legislative framework for addressing suspected abuses of a fundamental right at scale. Moreover, they create mechanisms and obligations for authorities to cooperate; in a way formally legislating Digital Clearinghouses into existence.

The Digital Markets Act has set up ([26]) the high-level group composed of the European Data Protection Supervisor (EDPS), the European Data Protection Board (EDPB), the Body of the European Regulators for Electronic Communications (BEREC) the European Competition Network, the Consumer Protection Cooperation Network (CPC) and the European Regulatory Group of Audiovisual Media Regulators. The EDPS had recommended establishing an institutionalised and structured cooperation between the relevant competent oversight authorities ([27]). However, it cannot be omitted that the decision setting it up excludes the group from being involved or providing advice in ongoing proceedings or investigations conducted by the Commission under the same regulation ([28]). The Digital Services Act requires Digital Services Coordinators to cooperate with other national competent authorities, as well as with the Commission and the European Board for Digital Services which the instrument

([26]) Article 40, Recital 93 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p.1.

([27]) EDPS, Opinion 2/2021 on the Proposal for a Digital Market Act, issued on 10 February 2021. The same recommendation was given in the context of the DSA; EDPS, Opinion, 1/2021 on the Proposal for a Digital Services Act, issued on 10 February 2021.

([28]) Commission Decision of 23.3.2023 on setting up the High-Level Group for the Digital Markets Act C(2023) 1833 final.

establishes. Cooperation may, among others, be put in place through regular exchanges or specific cooperation mechanisms such as pooling of resources, joint task forces, joint investigations and mutual assistance mechanism ([29]). The Data Act ([30]) touches on several areas of EU law, including data protection and consumer protection, and requires relevant authorities to cooperate with each other in the enforcement of the regulation and the handling of complaints.

At a national level, several Member States have formalised cooperation among regulators. The Netherlands established in 2021 the Digital Regulation Cooperation Platform ('SDT'), made up by the Dutch Authority for Consumers and Markets, the Dutch Authority for the Financial Markets, and the Dutch Media Authority ([31]). More recently, Germany created the Digital Cluster, consisting of Federal Financial Supervisory Authority ('BaFin'), the Federal Office of Justice ('BfJ'), the BSI, the Federal Commissioner for Data Protection and Freedom of Information ('BfDI'), the Federal Cartel Office (Bundeskartellamt), and the Federal Network Agency ('BNetzA') ([32]); in late 2023, the French Competition Authority ('FRCA') and the French data protection agency ('CNIL') signed a joint declaration aiming to strengthen their already established cooperation ([33]); in Spain, the national Markets and Competition Commission's ('CNMC') and the Agencia Española de Protección de Datos ('AEPD') signed a general cooperation protocol ([34]). In 2020, the UK formed the Digital Regulation Cooperation Forum consisting of the Consumer and Markets Authority, the Information Commissioner's Office, the communications regulator OFCOM and the Financial Conduct Authority ([35]).

8. Conclusion

In the 10 years since the EDPS's Preliminary Opinion, there is now no disputing the need for coordination between data protection, competition and other authorities to make our society and market realities fairer, more just and equitable for everyone. This is happening at national level and has been formally mandated in several EU legal instruments.

([29]) Recital 110, and Articles 49 and 50 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 227, 27.10.2022, p. 1.

([30]) Recitals 107 and 108 and Articles 37(2) and 38(3) and Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L 2023/2854, 22.12.2023.

([31]) Authority for Consumers and Markets, Dutch regulators strengthen oversight of digital activities by intensifying cooperation, Press Release, 13 October 2021.

([32]) Bundeskartellamt, Digital Cluster Bonn: Sechs Bundesbehörden arbeiten bei der Digitalisierung enger zusamme, Press Release, 15 January 2024.

([33]) Autorité de la Concurrence, Data protection and competition: the CNIL and the Autorité de la concurrence sign a joint declaration, Press Release, 12 December 2023.

([34]) Agencia Española de Protección de datos, Protocolo general entre la comisión nacional de los mercados y la agencia española de protection de los datos, 26 July 2018.

([35]) DRCF, The Digital Regulation Cooperation Forum (DRCF) brings together four UK regulators to deliver a coherent approach to digital regulation for the benefit of people and businesses online.

Nonetheless, the uncomfortable but necessary question remains as to what has actually changed on the ground. Having a rule book in place is the easy part. Companies do not change successful business models voluntarily. Once the political momentum has moved on, enforcers have the unglamourous job of demanding paperwork, and dealing with the aggressive lawsuits and multiple delaying tactics of some of the most highly paid lawyers in the world. The court is swamped with litigation. Market logic will drive towards preserving lucrative practices for as long as they can convince enough people that they are lawful. The powerful will continue to safeguard their secrets from public scrutiny – whether it concerns a US president's tax returns or a CEO's choice of hotel accommodation ([36]) – while ordinary people's data continue to be broadcast across the Internet. Additionally, in today's tense geopolitical environment, where there are companies subject to laws in authoritarian states that operate personal data-hungry business models, the threat is as much to security as well as to individual freedom and rights.

For the long-term sustainability of data protection, the community may consider learning lessons from environmental law. In this area, policymakers have had to acknowledge that extractive industries and fossil fuels are themselves the obstacles to the sustainability of human population and its way of life. Erecting and patrolling 'guardrails' for these practices, where actors respect 'do's and don'ts' while carrying on regardless of the longer term externalities, are hopelessly insufficient. Instead, the EU like other regions is embarking on a radical transition away from these industries.

Sustainability in data protection may similarly require such a general transition. This would involve moving away from the monetisation of people as if they were objects to feed AI models, ensuring that that no single controller is powerful enough to pursue abusive practices with impunity, and avoiding a future where the rights to privacy and to data protection are a privilege for the wealthy. To succeed, it is likely to demand a whole-of-government approach to the dispersal of data power, the breaking up of 'monocultures' ([37]) represented by dominant business models. Data practices will need to be recognised for their impact not only on human dignity and broader individual rights but also on open markets, democracy and security. If there is to be a 'turn to enforcement' after the recent abundance of EU lawmaking, we might be looking at a period of more assertive use of existing tools, where enforcers coordinate their activities based on a common desired outcome. Data protection authorities will have to constantly turn to competition authorities and vice versa. Working together will be essential to prevent the grandfathering into the future of the present harmful abuses of power.

([36]) Dick Durbin United States Senator Illinois, Durbin Questions Facebook CEO Mark Zuckerberg, 4 October 2018.

([37]) Crooked Timber, Your platform is not an ecosystem, 8 December 2022.

16

Follow the (personal) data: positioning data protection law as the cornerstone of EU's 'Fit for the Digital Age' legislative package

Dr. Gabriela Zanfir-Fortuna

Follow the (personal) data: positioning data protection law as the cornerstone of EU's 'Fit for the Digital Age' legislative package

Dr. Gabriela Zanfir-Fortuna (*)

This contribution explores the relationship between existing EU data protection law, in particular Article 8 of the EU Charter of Fundamental Rights (the right to the protection of personal data) and the General Data Protection Regulation ([1]), with the EU's new digital rulebook, as announced in 2020 by the European Commission's 'Europe Fit for the Digital Age' plan. With most of those legislative initiatives now adopted and in force, this analysis advances the idea that EU data protection law is inevitably the cornerstone of all legal frameworks that purport regulating conduct in the digital economy and the digital space involving personal data. It relies on Opinions and Statements published primarily by the European Data Protection Supervisor, sometimes in conjunction with the European Data Protection Board, as well as on case law of the Court of Justice of the EU applying Article 8 Charter. This chapter

(*) Vice President for Global Privacy, Future of Privacy Forum, and former legal officer at the European Data Protection Supervisor. The opinions expressed are those of the author alone.

([1]) Acknowledging, nonetheless, that EU data protection law is broader than this, also encompassing the Law Enforcement Directive ('LED') (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89), the EUDPR (Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39), or the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2022, p. 37). For the purposes of this contribution, the analysis will focus on the Article 8 EU Charter and the GDPR.

shows that regardless of the number, complexity and depth of various legal acts focusing on conduct and relationships in the digital space, ultimately data protection law and the supervisory authorities entrusted with its enforcement remain at the core of protecting the fundamental rights of individuals and society from risks and systemic risks resulting from the use of any technology relying on processing of personal data, as well as from personal data sharing among businesses and public authorities.

1. Tilting a carefully negotiated balance

The new digital rulebook of the European Union is taking up much of the public attention since 2020, when the European Commission presented its 'Europe Fit for the Digital Age' initiatives in a series of White Papers and Communications ([2]). The Commission did so only two years after the General Data Protection Regulation ([3]) ('GDPR') became applicable and without waiting to see whether its strengths would change business models and data practices, or how it would strengthen people's awareness of how their personal data is used, strengthening control over their digital traces and digital self.

The legislative package announced four years ago soon became reality. The Digital Services Act ([4]) ('DSA'), the Digital Markets Act ([5]) ('DMA'), the Data Act ([6]), the Data Governance Act ([7]) ('DGA') are now adopted and most of them will become fully applicable in 2024. The EU's AI Act ([8]) ('AIA') is close to adoption, while other closely-linked initiatives, such as the Platform Workers Directive ([9]) and the European Health Data Space ([10]) are being advanced in their legislative journey. In an uphill battle during their legislative process, the European Data Protection Supervisor ('EDPS'), sometimes with the support of the European Data Protection Board ('EDPB'), pushed for cohesion of this regulatory juggernaut with the already established EU data protection law

([2]) European Commission, Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence, Press Release, issued on 19 February 2020.

([3]) Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119, 4.5.2016, p 1.

([4]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1.

([5]) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1.

([6]) Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 202/1828 (Data Act), OJ L 2023/2854, 22.12.2023.

([7]) Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, p. 1.

([8]) Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final.

([9]) Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM(2021) 762 final.

([10]) Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final.

and its governance structure, flagging early on the risk of confusion, legal uncertainty, and ineffective enforcement ([11]).

It was as early as 2017 when the EDPS expressed concerns related to the adoption of laws in the digital realm that overlap with the (then) recently adopted GDPR. '*Fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity*' ([12]), the EDPS wrote in its Opinion on the Proposal for a Directive on contracts for the supply of digital content. The same Opinion also clearly stated that '*[t]he EU should … avoid any new proposals that upset the careful balance negotiated by the EU legislator on data protection rules. Overlapping initiatives could inadvertently put at risk the coherence of the Digital Single Market, resulting in regulatory fragmentation and legal uncertainty. The EDPS recommends that the EU apply the GDPR as the means for regulating use of personal data in the digital economy*' ([13]).

The European Commission did not take this advice to heart. In subsequent Opinions related to the avalanche of new legislation proposed following the '*Europe fit for the digital age*' communications, the EDPS, sometimes in conjunction with the EDPB ([14]), highlighted concerns related to the legal uncertainty created by the overlap of the scope of application and rules of the GDPR with the proposed legislation and systematically called for rules that are aligned to the comprehensive legal framework already in place and applicable to all processing of personal data, across industries, public services and regardless of the size of the entities processing it.

Starting with the Opinion on the EU Strategy for Data in 2020, before the Commission published any of the legislative proposals that were to come, the EDPS recalled that '*the GDPR provides for a solid basis, also by virtue of its technologically neutral approach, for the development and implementation of the Strategy*' ([15]) and, optimistically, supported the '*Commission's commitment to develop the Strategy in full compliance with the GDPR*' ([16]).

([11]) See for example the EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), adopted on 4 May 2023, p. 2, stating '*with this joint Opinion, the EDPB and the EDPS aim to draw attention to a number of overarching concerns on the Proposal on Data Act and urge the co-legislature to take decisive action*'; or the EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, issued on 10 February 2021, p. 3, where the EDPS welcomed the legislative proposal, '*as it seeks to promote fair and open markets and the fair processing of personal data*', but also provided '*specific recommendations to help ensure that the Proposal complements the GDPR effectively, increasing protection for the fundamental rights and freedoms of the persons concerned, and avoiding frictions with current data protection rules*'.

([12]) EDPS Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, issued on 14 March 2017, p. 3.

([13]) EDPS Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, issued on 14 March 2017, p. 3.

([14]) In addition to the EDPB-EDPS Joint Opinions, see also the EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021.

([15]) EDPS Opinion 3/2020 on the European Strategy for Data, issued on 16 June 2020, paragraph 8.

([16]) EDPS Opinion 3/2020 on the European Strategy for Data, issued on 16 June 2020, paragraph 8.

Furthermore, in its Opinion on the White Paper on AI, the EDPS responded to the claims therein that transparency, traceability and human oversight of AI systems are not specifically covered under current legislation: the EDPS '*is of the view that the GDPR fully reflects the mentioned key requirements and it applies to both private and public sectors processing personal data*' ([17]). The EDPS specifically mentioned in this regard Article 5(1)(a) – the principle of lawfulness, fairness and transparency, Articles 12 to 14 – transparency requirements, including regarding the logic involved in automated decision-making, and more broadly Article 5(2) – accountability. '*Therefore, this does not seem an issue for the EU's data protection legislation*'([18]), the EDPS added.

As the legislative proposals for the DSA, DMA, DGA and AIA had been published by the end of 2021, and the proposed text of the Data Act was about to be published, the EDPB issued a sobering statement, saying that '*without further amendments, the proposals will negatively impact the fundamental rights and freedoms of individuals and lead to significant legal uncertainty that would undermine both the existing and future legal framework. As such, the proposals may fail to create the conditions for innovation and economic growth envisaged by the proposals themselves*' ([19]).

Why are the EDPS and EDPB so concerned with overlapping laws in the digital realm and the legal uncertainty this may create? And where does the adoption of this full suite of new laws leave the GDPR, data protection law and the role of Data Protection Authorities ('DPAs')? This contribution will provide some answers to these questions. The following section will look into the scope of application of the DMA, DSA, DGA, Data Act and AIA and will show how they all ultimately regulate processing of personal data and the entities engaging in it, overlapping thus with the GDPR and triggering its application in several, if not most, scenarios regulated by the new laws (Section 2). Next, it will be argued that due to this fact Article 8 Charter will likely also be triggered in the application of the new laws, foreseeing possible future challenges at the CJEU (Section 3). The fourth section will show how the new laws establish precedence of the GDPR in sometimes clear and sometimes less clear terms, positioning thus the GDPR as the cross-functional backbone of the Data Strategy laws (Section 4). Before drawing conclusions (Section 6), the enforcement framework proposed by the new laws will be briefly analysed, showing that the supervisory authorities entrusted with the application of data protection law do not have a clear role in the new EU digital rulebook, despite the significant role that processing of personal data has in defining its scope (Section 5).

([17]) EDPS Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust, issued on 29 June 2020, paragraph 18.

([18]) EDPS Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust, issued on 29 June 2020, paragraph 18.

([19]) EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 2.

2. The EU's New Digital Rulebook also regulates processing of personal data and the entities engaging in it

The GDPR applies to the 'processing' of 'personal data' wholly or partly by automated means (Article 2(1) GDPR) and to some non-automated processing, regardless of industries, business models, public services provided, contexts, nature or size of the entities processing the data. Both concepts of 'processing' and 'personal data' are broadly defined in Article 4 of the Regulation and have also been interpreted broadly by supervisory authorities, national courts and the CJEU ([20]). Both concepts refer to 'any information' that is related to an 'identified or identifiable natural person', and to 'any operation or set of operations' performed on such information.

Showing just how far-reaching the rules of the GDPR are, a case-law report on its Article 22 (the right not to be subject to automated decision-making), included cases involving the use of social media platforms, the use of facial recognition systems in schools and supermarkets, automated grading of students, automated assessing for distribution of social benefits by public authorities, management of gig workers through gig platforms, among many other scenarios ([21]). The entities bearing legal obligations under the GDPR are 'controllers' and 'processors'. Both of them can be any natural or legal person, as long as they establish the purposes and means of processing (controllers) or process personal data on behalf of an entity that does so (processors).

The DSA applies to intermediary services, including online platforms, offered to recipients of the service ([22]) and sets out a complex set of rules, from takedown of illegal content online, to forbidding profiling of minors for ad targeting, forbidding profiling based on sensitive data for ad targeting, to offering researchers access to data held by Very Large Online Platforms and Search Engines ('VLOPs/'VLOSEs'). As explained by the European Commission, the covered intermediary services may include online marketplaces, social networks, content-sharing platforms, app stores and online travel and accommodation platforms ([23]). For instance, the same entities ('providers of online platforms') that under the DSA have a prohibition to present ads to users stemming from 'profiling' them based on sensitive personal data ([24]) are also controllers under the GDPR whenever they engage in any type of profiling on their platforms.

The DMA applies to core platform services provided or offered by 'gatekeepers' to business users and end users ([25]). Its defined purpose is '*to contribute to*

([20]) See, for instance, CJEU Research and Documentation Directorate, Fact Sheet on Protection of Personal Data, November 2021, p. 12-19.

([21]) Zanfir-Fortuna, G., Barros Vale, S., *Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities*, Future of Privacy Forum, May 2022.

([22]) Article 2(1) DSA.

([23]) See European Commission, Sharing Europe's Digital Future, The Digital Services Act package.

([24]) Article 26(3) and Recital 68 of the DSA.

([25]) Article 1(2) DMA.

the proper functioning of the internal market by laying down harmonized rules ensuring for all businesses, contestable and fair markets in the digital sector' ([26]). The Commission explains that '*gatekeepers" are "digital platforms with a systemic role in the internal market that function as bottlenecks between businesses and consumers for important digital services*' ([27]). The rules of the DMA include obligations that specifically refer to processing personal data, such as a prohibition for gatekeepers to '*combine personal data from the relevant core platform service with personal data from any other services provided by the gatekeeper or with personal data from third-party services*' ([28]).

The Data Act lays down harmonised rules for a series of 'data operations', which often involve sharing or other types of processing of personal data, such as making available product data and related service data to the user of a connected product or a related service, or a vaguely worded '*making available of data by data holders to data recipients*' and 'to public sector bodies' ([29]). In Article 1(2), which defines its scope of application, the Data Act confirms that it '*covers personal and non-personal data*'.

The DGA lays down, among other things, conditions for the re-use of certain categories of data held by public sector bodies, rules for the provision of data intermediation services and a framework for voluntary registration of entities processing data '*made available for altruistic purposes*' ([30]). The DGA mentions both 'personal data' and 'non-personal data' in its provisions, usually involving 'sharing' or 'making available' such data as operations.

Finally, the AI Act lays down harmonised rules for the placing on the market, the putting into service and the use of AI systems and General Purpose AI models, as well as prohibitions of certain AI practices, specific requirements for high-risk AI systems and their operators, and transparency rules related to AI systems, among other issues ([31]). Certain type of scoring based on personal data, including inferred personal data, as well as real time facial recognition systems are among the prohibited AI practices ([32]). At the same time, providers of high-risk AI systems are under an obligation to process special categories of personal data as defined in Article 9 GDPR, 'to *the extent they are strictly necessary for the purposes of ensuring bias detection and correction*' ([33]).

Even briefly looking at the subject matter and scope of application of these legal acts, it is no surprise that the EDPB pointed out in its 2021 Statement on the Digital Package and Data Strategy that '*[p]rocessing of personal data already is or will be a core activity of the entities, business models and technologies regulated*

([26]) Article 1(1) DMA.
([27]) European Commission, Sharing Europe's Digital Future, The Digital Services Act package.
([28]) Article 5(2)(b) DMA.
([29]) Article 1(1)(a), (b) and (c) Data Act.
([30]) Article 1(1) DGA.
([31]) Article 1(1) AIA, as adopted by COREPER, see Council Doc. 8115/21, 26 January 2024.
([32]) Article 5 AIA, as adopted by COREPER, see Council Doc. 8115/21, 26 January 2024.
([33]) Article 10(5) AIA, as adopted by COREPER, see Council Doc. 8115/21, 26 January 2024.

by these proposals' ([34]). The EDPB was thus worried that '*[t]he combined effect of the adoption and implementation of the proposals will therefore significantly impact the protection of the fundamental rights to privacy and to the protection of personal data, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and in Article 16 of the Treaty on the Functioning of the European Union*' ([35]).

The amendments to these proposals that followed in the legislative process did not alleviate the concerns of legal uncertainty due to the significant potential overlap of their scope of application with that of existing data protection law. Wojciech Wiewiórowski, the European Data Protection Supervisor, highlighted in public remarks at the end of 2023, that '*even though each Act pursues its own objectives, several provisions explicitly regulate processing of personal data, sometimes even explicitly referring to GDPR definitions, concepts and obligations*' ([36]).

As shown in the following section, this fact is particularly relevant in the light of case-law of the Court of Justice of the EU ('CJEU') on the effective application of Article 8 of the EU Charter of Fundamental Rights on the right to the protection of personal data.

3. The EU's New Digital Rulebook includes interference with the fundamental right to the protection of personal data

In the seminal judgment of *Digital Rights Ireland*, which saw the 2006 Data Retention Directive ([37]) annulled in its entirety eight years after it was adopted, the CJEU established unequivocally that the whole Directive at issue '*constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the* ***Charter because it provides for the processing of personal data***' ([38]) (emphasis added). After finding, among other things, that the Directive '*does not lay down any objective criterion by which the number of persons authorized to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued*' ([39]), and that it '*does not contain any substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use*', ([40])

([34]) EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 1.

([35]) EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 1.

([36]) Wiewiórowski, W., Brussels Privacy Symposium on the EU Data Strategy, Opening Remarks, 14 November 2023.

([37]) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105, p. 54.

([38]) Judgement of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Seitlinger and others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 36.

([39]) *Digital Rights Ireland and Seitlinger and others*, paragraph 62.

([40]) *Digital Rights Ireland and Seitlinger and others*, paragraph 61.

the Court established that the Directive '*does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter*' ([41]), and it annulled the entire legal act ([42]).

The finding that a legal act merely providing for the processing of personal data constitutes an interference with Article 8 of the Charter was confirmed in subsequent case-law of the CJEU. In *Ligue des droits humains*, the CJEU restated that '*processing of PNR data as that covered by the PNR Directive also falls within the scope of Article 8 of the Charter* ***because it constitutes processing personal data within the meaning of that article, and, accordingly, must necessarily satisfy the data protection requirements laid down in that article***' ([43]) (emphasis added). Additionally, the Court confirmed that '*it is settled case-law that the* ***communication of personal data to a third party, such as a public authority****, constitutes an interference with the fundamental rights enshrined Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to those data with a view to their use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference*' ([44]) (emphasis added). Assessing the safeguards put in place, ultimately the Court ruled that the PNR Directive is consistent with the provisions of the Charter, including Article 8 ([45]).

All legal acts from the European Commission's 'EU fit for the digital age' package analysed in this chapter include at least some instances of clear obligations to process personal data for the actors covered, or lay down conditions for such processing, notwithstanding the overall potential overlap in scope of application with the GDPR and other EU data protection law. Understanding that the 'data' subject to the application of these laws include 'personal data' pursuant to their 'Definitions' clauses, there are obvious examples of such obligations:

- Article 40 of the DSA and its obligation for VLOPs/VLOSEs to provide access to the data necessary (i.e. 'making [personal] data available') to monitor their compliance with the regulation to competent authorities and vetted researchers;
- Article 6(9) of the DMA and its obligation for gatekeepers to '*provide end users and third parties authorized by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user … including by the provision of continuous and real-time access to such data*';

([41]) *Digital Rights Ireland and Seitlinger and others*, paragraph 65.
([42]) See also further the contribution by Kranenborg, H., 'The EDPS and the never-ending story of data retention', Chapter 6.
([43]) Judgment of the Court of Justice of 21 June 2022, *Ligue des droits humains*, in C-817/19, ECLI:EU:C:2022:491, paragraph 95.
([44]) *Ligue des droits humains*, paragraph 96.
([45]) *Ligue des droits humains*, paragraph 2 of the Executive part of the judgment.

- Article 4 of the Data Act, including obligations to make product data and related service data accessible to the user and Article 14 of the Data Act including an obligation to make data available to public sector bodies;
- Article 10(5) AIA, including an obligation for providers of high-risk AI systems to process special categories process special categories of personal data as defined in Article 9 GDPR '*to the extent they are strictly necessary for the purposes of ensuring bias detection and correction*' ([46]).

These are all provisions which constitute interference with the right to protection of personal data as provided by Article 8 Charter, to the extent that the data at issue includes personal data (which is more likely than not, given the nature of the regulated entities). Even though there is not an obvious instance where such interference is created directly by the DGA, that Regulation details conditions for re-use of data, including personal data, held by public sector bodies, as well as a framework for lawfully 'donating' personal data (making that data available to specific entities on the basis of consent), as well as a framework for recognising data intermediaries, explicitly dealing with requests from individuals that seek to make their personal data available and to exercise their rights under the GDPR. Regulating frameworks and procedures for sharing data including personal data, and for the exercise of the data subject rights under the GDPR is relevant for respecting the conditions of Article 8 Charter, especially taking into account its second paragraph which specifically refers to conditions of lawfulness for processing and to access and correction as data subject rights.

Assessing whether the interference with Article 8 of the Charter, stemming from the provisions summarised above is justified, as well as potentially other provisions of the 'EU fit for the digital age' legislative package, requires a detailed analysis of the law. The CJEU explained that law including interference with fundamental rights '*must itself define the scope of limitation on the exercise of the right concerned*' ([47]), even if flexible for different contexts and changing circumstances, and that, with regard specifically to interference with the right to the protection of personal data, the law '*in order to satisfy the proportionality requirement, … must lay down clear and precise rules governing the scope and application of the measures provided for and imposing minimum safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse*' ([48]). As the effects of this legislative package and its various provisions stimulating processing of personal data at varying scale will unfold, it should not be surprising if challenges of the validity of these provisions will be brought to the CJEU in the light of Article 8 EU Charter in the following years.

Notwithstanding the potential interference with the right to the protection of personal data created directly by some of these provisions, another fact should be taken into account: the material and personal scope of application defined

([46]) Article 10(5) AIA, as adopted by COREPER, see Council Doc. 8115/21, 26 January 2024.

([47]) *Ligue des droits humains*, paragraph 114.

([48]) *Ligue des droits humains*, paragraph 117.

by the laws analysed in this chapter (see in particular Section 2) will inevitably overlap with 'controllers' and 'processors' 'processing personal data' under the GDPR or other relevant EU data protection secondary law. The next section will briefly discuss how this conflict of law is being solved and point to some additional areas of uncertainty.

4. The EU's New Digital Rulebook applies without prejudice to the GDPR

Section 2 demonstrated that the legal acts of the Data Strategy package are also regulating the processing of personal data and the entities engaging in it. As a result, two questions arise: first, are the new laws consistent with the rules of the GDPR and other secondary data protection law, and second, if there are instances where they are not consistent, which of the two laws apply?

A survey of the EDPS and the EDPB-EDPS Joint Opinions on the legislative proposals of the new legislative acts shows that these questions are acute. Take, for instance, the Joint Opinion on the DGA, in which the EDPB and the EDPS considered that the Proposal raises significant inconsistencies with the GDPR, as well as with other Union law ([49]) and laid out five aspects where this happens, from broad issues like the '*subject matter and scope of the Proposal*', to specific issues like '*legal basis for the processing of personal data*' ([50]). Similarly, in their Joint Opinion on the Data Act, they considered that '*additional safeguards are necessary to avoid lowering the protection of the fundamental rights to the privacy and the protection of personal data in practice*' and urged the co-legislature to take 'decisive action' ([51]). Concrete examples of such inconsistencies included the obligation to make data available to public sector bodies, including Union bodies, in case of exceptional need, and the extension of a right to access data to entities other than the data subject, including businesses. They encouraged the Commission '*to ensure that data protection rules and principle shall prevail whenever personal data are being processed*' ([52]).

The EDPB-EDPS Joint Opinion on the EU AI Act proposal stressed that '*the Proposal has prominently important data protection implications*' ([53]) and specifically mentions that the GDPR, the EUDPR and the LED have to be '*considered as a prerequisite on which further legislative proposals may build upon without affecting or interfering with the existing provisions, including when it comes*

([49]) EDPB-EDPS Joint Opinion 3/2021 on the Proposal for a regulation the European Parliament and of the Council on European data governance (Data Governance Act), adopted on 10 March 2021, paragraph 24.

([50]) EDPB-EDPS Joint Opinion 3/2021 on the Proposal for a regulation the European Parliament and of the Council on European data governance (Data Governance Act), adopted on 10 March 2021, paragraph 25.

([51]) EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), adopted on 4 May 2022, Executive Summary, p. 2.

([52]) EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), adopted on 4 May 2022, paragraph 20.

([53]) EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), adopted on 18 June 2021, Executive summary.

to the competence of supervisory authorities and governance' ([54]). They also highlighted that the plea to ensure consistency with the data protection acquis '*is not only for the sake of legal certainty*', but *'also to avoid that the Proposal has the effect of directly or indirectly jeopardizing the fundamental right to the protection of personal data, as established under Article 16 of the TFEU and Article 8 of the Charter*' ([55]).

All these concerns were raised during the legislative process. They focused both on ensuring the precedence of the GDPR (and other data protection law acquis where needed) in the final text of the law, and on aligning the provisions on substance in instances where future conflict of laws seemed obvious or where there was a risk of non-compliance with the fundamental right to the protection of personal data.

Each of the five legal acts establish, without exception, the precedence of the GDPR (and other data protection acquis where necessary), some in clearer terms than others:

- The DSA, the DGA, and the Data Act include articles ([56]) establishing that they are 'without prejudice' to EU law on the protection of personal data, all quoting the GDPR, and some also additional data protection legislative acts.
- The DMA includes similar wording establishing the precedence of the GDPR, but only in a recital ([57]). It omits to include this language in the main text of the law, in Article 1 defining its scope which includes references to other law taking precedence over the DMA. However, the provision of the DMA establishing accountability of gatekeepers to ensure and demonstrate compliance with their main obligations in the Act (Article 8(1) DMA) also adds that the way in which gatekeepers implement those obligations must comply with all other applicable law, 'in particular' the GDPR, the ePrivacy Directive and a suite of additional laws, from consumer protection to product safety.
- The AI Act also defines the relationship between itself and EU data protection secondary law in an article, but uses more evasive language, saying that the Act 'shall not affect' the GDPR, the EUDPR, the ePrivacy Directive and the LED. The first part of the provision also states that EU data protection and privacy law *'applies to personal data processed in connection with the rights and obligations laid down in this Regulation*', which is a vague formulation since it does not seem to immediately include processing of personal data in relation to AI systems covered by the Act. A helpful recital further clarifies that the Act '*does not affect the obligations of providers and deployers of AI systems in their role as*

([54]) EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), adopted on 18 June 2021, paragraph 56.

([55]) EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), adopted on 18 June 2021, paragraph 57.

([56]) Article 2(4)(g) DSA, Article 1(3) DGA, and Article 1(5) Data Act.

([57]) Recital 12 DMA.

data controllers or processors stemming from national or Union law on the protection of personal data in so far as the design, the development or the use of AI systems involves the processing of personal data' ([58]).

Therefore, all these new legislative acts of the 'EU fit for the digital age' strategy acknowledge the potential of overlap between them and the GDPR (as well as other relevant data protection laws), by establishing rules for potential conflict of laws applying to the same material and personal scope delineated by (likely) processing of personal data as part of the conduit they regulate.

Despite establishing such precedence rules, avoiding divergence in interpreting and applying these new acts in conjunction with the GDPR and other data protection law will not be an easy task. Enforcement of the new rules is entrusted to a potentially very diverse set of new and old national regulators to be appointed by Member States, in addition to some core enforcement functions that the European Commission has.

5. The EU's New Digital Rulebook does not have a clear role for DPAs in its enforcement structure

The EDPS identified as significant the issue of enforcement of the new digital laws announced in the ambitious plans of the European Commission, starting with the Opinion on the Strategy itself, even before the texts of the proposals were published. '*The EDPS underlines that in the context of future governance mechanisms the competences of the independent supervisory authorities for data protection must be properly respected. (…) Cooperation and joint investigations between all relevant public oversight bodies, including data protection supervisory authorities, should be encouraged*' ([59]).

Despite this advice, the EU legislator opted to create a new web of digital enforcers and regulators, leaving it to the Member States to choose one or more enforcers for the new Acts, with the exception of the centralized enforcement powers given to the European Commission in the DMA, the DSA for VLOPs/VLOSEs, and the AI Act for General Purpose AI models. The AI Act also has a role for the EDPS as enforcer, in relation to EU agencies and bodies acting as AI operators. Little attention was paid in the legislative acts themselves to enforcement cooperation and the key role Data Protection Authorities ('DPAs') have whenever natural or legal persons – be them gatekeepers, providers of AI systems, online marketplaces, or public authorities, process personal data covered by EU data protection law.

([58]) 58The Recital is provisionally numbered 5aa in the text adopted by COREPER, see Council Doc. 8115/21, 26 January 2024. See also further the contribution by Smuha, N., 'The paramountcy of data protection law in the age of AI (Acts)', Chapter 17.

([59]) EDPS Opinion 3/2020 on the European Strategy for Data, issued on 16 June 2020, paragraph 64.

The EDPB succinctly described the problem in its 2021 Statement on the Data Strategy package:

> *'While the processing of personal data is central to the activities regulated by the proposals, data protection supervisory authorities are not designated as the main competent authorities. The EDPB recalls that, as far as the protection and free flow of personal data is concerned, Article 16(2) TFEU and Article 8(3) of the EU Charter require that the supervision of the processing of personal data be entrusted to independent data protection authorities'. ([60])*

Indeed, both Article 16(2) TFEU and Article 8(3) Charter provide that compliance with the rules related to the fundamental right to the protection of personal data '*shall be subject to the control of independent authorities*'. The two provisions do not specify exactly what authorities, but they are clear that the supervisory authorities enforcing rules related to processing of personal data in the application of this right must be independent. In fact, the independent supervision of the provisions related to processing of personal data is recognized as one of the key elements of the fundamental right to the protection of personal data ([61]). Notably, the main EU secondary legislation transposing Article 8 Charter, the GDPR, specifically recognizes DPAs as supervisory authorities for the enforcement of data protection law.

The EDPB also requested in the same 2021 Statement that '*each of the proposals clearly mentions data protection supervisory authorities among the relevant competent authorities with whom cooperation shall take place*'. ([62]) This message was re-emphasized with some variations in all of the EDPS and EDPB-EDPS Joint Opinions on each of the legislative proposals.

The final version of the legal texts analysed recognises some role for DPAs, with notable variations. For instance, after the Data Act grants each Member State the power to designate one or more competent authorities to be responsible for its application and enforcement, it specifies in Article 37(3) that DPAs '*shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned*'.

In turn, the DSA does not refer to DPAs in its chapter dedicated to enforcement, despite some of its key provisions relying on concepts defined in the GDPR, such as 'profiling', or involving obligations to process personal data, such as making personal data processed by platforms available to researchers. The DSA provides that Member States should designate one or more competent authorities ([63]), among which they should appoint a Digital Services Coordinator ('DSC'). Recital 44, in its last sentence, mentions that '*for any question requiring*

([60]) EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 3.

([61]) Gonzalez Fuster, G., *Study on the essence of the fundamental rights to privacy and to the protection of personal data (EDPS 2021/0932)*, 2022, p. 33 and 34.

([62]) EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 4.

([63]) Article 49 DSA.

an assessment of compliance with [the GDPR], the competent authority for data intermediation services should seek, where relevant, an opinion or decision of the competent supervisory authority established pursuant to [the GDPR]'.

The DSA empowers the European Commission to enforce its rules targeting VLOPs/VLOSEs. A question arises regarding independence of the DSA enforcers. The DSCs '*must perform their tasks … in an impartial, transparent and timely manner*' ([64]). The Act adds that '*when carrying out their tasks and exercising their powers in accordance with this Regulation, the [DSCs] shall act with complete independence*' ([65]). This may mean that the authority itself does not have to be an independent authority, but only that it must act with independence when carrying out its tasks under the DSA. This 'qualified' independence for national DSCs may be explained by the fact that the European Commission, the executive arm of the EU, is one of the enforcers of the DSA, and thus requiring independence similar to that of DPAs would be asymmetrical. However, creating more confusion, recital 112 provides context on the independence requirement generally for the competent authorities designated at national level – they should act in complete independence '*from private and public bodies, without the possibility to seek or receive instructions, including from the government, and without prejudice to the specific duties to cooperate with other competent authorities*'. Considering the significant role DSA enforcers have in enforcing how personal data is being processed ([66]) by online platforms, should they be required to meet the independence criteria that DPAs have to meet? Or should this conundrum be solved by involving DPAs formally in DSA's enforcement process?

The European Commission is also the enforcer of the DMA, one of the laws of the new legislative package that enshrines legal provisions related to the processing of personal data, including obligations for gatekeepers to process personal data in specific ways and relying on legally defined terms in the GDPR, such as 'consent'. The DMA vaguely refers in a recital to the fact that it is without prejudice to the GDPR, '*including its enforcement network, which remains fully applicable with respect to any claims by data subjects relating to an infringement to their rights under that Regulation*' ([67]). This wording suggests that DPAs would not have competence over claims made by data subjects relating to an infringement of the DMA, even where they act as 'data subjects', so therefore in relation to rights concerning processing of their personal data which would be governed by the GDPR.

Such a solution would be curious, especially following the recent Judgment of the CJEU in the *Bundeskartellamt* case. The CJEU was explicit when stating in that case that '*the examination by a competition authority of an undertaking's*

([64]) Article 50(1) DSA.

([65]) Article 50(2) DSA.

([66]) See, for instance, Zanfir-Fortuna, G., and Rovilos, V., EU Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR, *Future of Privacy Forum Blog*, 31 August 2023.

([67]) Recital 37 DMA.

conduct in the light of the provisions of the GDPR may entail the risk of divergences between that authority and the supervisory authorities in the interpretation of that regulation' ([68]).

The Court established two rules: First, competition authorities that must look into GDPR compliance in the exercise of their powers '*are required to consult and cooperate sincerely with the national supervisory authorities concerned or with the lead supervisory authority, all of which are then bound, in that context, to observe their respective powers and competences, in such a way as to ensure that the obligations arising from the GDPR and the objectives of that regulation are complied with while their effectiveness is safeguarded*' ([69]). Second, competition authorities must ascertain whether the conduct they are investigating has already been the subject of a decision by a competent DPA or the Court, and if that is the case, it '*cannot depart from it, although it remains free to draw its own conclusions from the point of view of the application of competition law*' ([70]).

Finally, the AI Act does not have a clear role for DPAs either, other than a couple of narrowly defined interventions. For instance, in the case of specific high-risk AI systems used for law enforcement purposes and other three specifically defined types of high-risk systems, Member States must designate as market surveillance authorities DPAs as established by the GDPR or the LED. The EDPS is designated to act as market surveillance authority where Union institutions, agencies and bodies fall within the scope of the AIA ([71]). Additionally, DPAs should be notified of each use of a real-time biometric identification system, together with the relevant market surveillance authority (Article 5 AIA).

Given how the EU legislator ended up building the enforcement edifice ([72]) of the new Data Strategy laws, the EDPS had a poignant message at the end of 2023, when the final text of most of the laws analysed here was already settled: '*one of the biggest challenges ahead for the EU's digital rulebook, in my view, is going to be its enforcement*', and, specifically, 'ensuring regulatory consistency' ([73]).

This analysis, even if brief, showed that there is a considerable disconnect between the 'personal data processing'-heavy scope of application of the EU's new Digital Rulebook, the mission of the DPAs as independent supervisory authorities entrusted with making sure that the fundamental right to the protection of personal data is respected in the EU, and the fairly marginal role DPAs have been specifically granted in the governance and enforcement of these new laws.

([68]) Judgement of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraph 55.

([69]) Meta Platforms a*nd others (Conditions générales d'utilisation d'un réseau social)*, paragraph 54.

([70]) Meta Platfor*ms and others (Conditions générales d'utilisation d'un réseau social)*, paragraph 56.

([71]) Article 63 AIA – market surveillance and control of AI systems in the Union market, as provisionally numbered in the text adopted by COREPER, see Council Doc. 8115/21, 26 January 2024.

([72]) Or 'labyrinth' as it was coined by Hajduk, P., 'A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research', 18th IFIP Privacy and Identity Management 2023, Sharing (in) a Digital World, Springer, forthcoming 2024.

([73]) Wiewiórowski, W., Brussels Privacy Symposium on the EU Data Strategy, Opening Remarks, 14 November 2023.

6. Conclusion

This chapter showed that data protection law, whose application is triggered whenever 'personal data' is 'processed', remains the cornerstone of EU's Digital Rulebook, regardless of whether it is explicitly recognized as such in these new positive laws.

First, it briefly looked into the scope of application of the DMA, DSA, DGA, Data Act and AIA and identified clear instances where processing of personal data and the entities engaging in it are being regulated by these new laws, while at the same time triggering the application of the GDPR (Section 2).

The following section (3) showed how several provisions of the Digital Rulebook are capable of directly engaging Article 8 EU Charter, in the light of established CJEU case-law that a legal measure which provides for processing of personal data amounts to an interference with Article 8. There was no assessment made regarding the lawfulness of any of the interference identified, as it sufficed to show for the purposes of this analysis that the right to the protection of personal data is at play in the Data Strategy legal framework.

Section 4 mapped provisions in each of the five laws analysed which established precedence of the GDPR (and sometimes other EU secondary data protection and privacy law), positioning it as the one common denominator cutting through the Digital Rulebook and engaging all of the new legal frameworks in various ways.

Finally, the last section (5) briefly discussed the enforcement architecture built by the EU legislator, observing that despite the significant role that processing of personal data has in the substance and material scope of the new digital rulebook, and despite the clear engagement with Article 8 Charter discussed earlier, DPAs do not have a well established role in the enforcement or governance of the EU's Digital Rulebook.

The journey through these arguments and analysis was accompanied by Opinions and Statements published in the past four years by the EDPS, sometimes jointly with the EDPB, analysing these legislative proposals and clearly showing areas of tension with existing legal frameworks and their enforcement.

These areas of tension indicate challenges ahead in the implementation of the EU's new Digital Rulebook. Such challenges can be overcome by coherent policymaking and governance, which could start by recognizing the central role data protection law has in the digital regulatory space, especially through the lens of Article 8 EU Charter. This would be translated into consistent involvement of DPAs and the existing data protection 'infrastructure' permeating all public sector and all industries after the adoption of the GDPR, the LED and the EUDPR, such as Data Protection Officers, in the coherent interpretation and application of the new rules. The opportunities brought by the new legislative package could thus be easier to grasp.

17

The paramountcy of data protection law in the age of AI (Acts)

Prof. Dr. Nathalie A. Smuha

The paramountcy of data protection law in the age of AI (Acts)

Prof. Dr. Nathalie A. Smuha (*)

Artificial Intelligence's data-driven nature renders it undeniably impactful on the rights to privacy and data protection. It is therefore no surprise that Europe's upcoming AI Act is entwined with regulation that seeks to protect those rights, amongst other EU values. In this article, I dive deeper into the relationship between the AI Act and European data protection law, and seek to unpack how the latter influences the former. I consecutively examine how data protection law grounds the AI Act, how it complements the Act, and how it enables an evaluation and a critique thereof. I conclude by arguing that, notwithstanding the AI Act's upcoming role and its new set of requirements, data protection law remains paramount to protect people against AI's adverse effects and to hold AI providers and deployers accountable.

1. Introduction

Over the past decade, few technologies managed to reach the level of hype attained by Artificial Intelligence ('AI'). Whenever AI was not making headlines for fascinating breakthrough applications, it was at any rate in the news for the substantial ethical and legal concerns it raises. AI systems require a large amount of data for their training and functioning, which typically also includes personal data. It is hence not surprising that many concerns relate to privacy and personal data protection, two fundamental rights that are significantly affected by AI systems ([1]). Moreover, the deployment of AI can also (in)directly impact numerous other fundamental rights (such as the right to non-discrimination and

(*) Assistant Professor, Department of International and European Law, KU Leuven Faculty of Law; Emile Noël Fellow, Jean Monnet Center, NYU School of Law.

([1]) See e.g. Manheim, K. and Kaplan; L., 'Artificial intelligence: Risks to privacy and democracy', *Yale Journal of Law & Technology*, 21, 2019, 106-188; Chamberlain, J., and Reichel, J., 'Supervision of Artificial Intelligence in the EU and the Protection of Privacy', *FIU Law Review* Vol. 17 No. 2, 2023, 267-285. On the relationship between both rights, see also González-Fuster,G., *The emergence of personal data p*rotection as a fundamental right of the EU, Springer, 2014.

the right to human dignity) and EU values (such as democracy and the rule of law) ([2]), bearing in mind that privacy and data protection often act as essential prerequisites for their enjoyment.

Initially, EU policymakers focused mostly on AI's strategic and economic potential, and were most concerned with being a 'leader' in the global race to AI, in which they sought to keep up with China and the United States ([3]). Their vision became gradually more comprehensive after scandals like the *Cambridge Analytica* saga ([4]), which involved large-scale AI-driven misuse of personal data for political and commercial ends, and put AI's risks more firmly on their radar. Yet despite the growing evidence of adverse effects associated with AI's irresponsible use, and of legal gaps that make it difficult to address them, the EU legislator for a long time remained hesitant to introduce new binding rules. One of the most prominent arguments against a new legislative initiative to better safeguard people's rights was – ironically enough – the General Data Protection Regulation (GDPR), which became applicable in 2018. At that time, it was believed that this new regulation ([5]), which also included provisions on automated data processing and algorithmic decision-making, offered sufficient protection to address the (new) threats posed by AI systems, and that additional legislation would merely stifle innovation ([6]).

This stance ultimately shifted in 2019 after yet more scandals ([7]), and after the European Commission's High-Level Expert Group published its *Ethics Guidelines for Trustworthy AI* and its *Policy Recommendations* ([8]), signalling in both documents that non-binding guidance can be useful but remains inadequate to protect fundamental rights, democracy and the rule of law

([2]) See e.g. Yeung, K., 'Why Worry about Decision-Making by Machine?', in Yeung, K., and Lodge, M., (eds), *Algorithmic Regulation*, Oxford University Press, Oxford, 2019; Mantelero, A., *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*, Springer, 2022; Smuha, N.A., *Algorithmic Rule by Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law*, Cambridge University Press, Cambridge, 2024. See also the EDPS Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments, issued on 23 October 2023, p. 6.

([3]) This is particularly visible in Europe's AI Strategy, proposed by the European Commission in April 2018. See European Commission, Artificial Intelligence for Europe, COM(2018) 237 final. In this regard, see also Smuha, N.A., 'From a "race to AI" to a "race to AI regulation": regulatory competition for artificial intelligence', *Law, Innovation and Technology*, Vol. 13, No. 1, 2021, p. 57-84; Bradford, A., *Digital empires: The global battle to regulate technology*, Oxford University Press, Oxford, 2023.

([4]) See Wylie, C., *Mindf* ck: Cambridge Analytica and the plot to break America*, Random House, 2019. See also Hinds, J., Williams, E.J. and Joinson, A. N., '"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal', *International Journal of Human-Computer* Studies 143, 2020.

([5]) The GDPR revised and repealed its predecessor, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

([6]) See in this regard also Smuha, N.A. and Yeung, K., 'The European Union's AI Act: beyond motherhood and apple pie' in Smuha N.A. (ed), *The Cambridge Handbook on the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press, 2024 (forthcoming).

([7]) Consider, for instance, Amazon's automated hiring tool that showed bias against women by ranking their applications with a lower score. See Dastin, J., Insight – Amazon scraps secret AI recruiting tool that showed bias against women, Reuters, 10 October 2018.

([8]) See High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, Brussels, issued on 8 April 2019; *Policy and Investment Recommendations for Trustworthy AI, Brussels*, issued on 26 June 2019.

– the EU's trinity of constitutional values – against AI's risks ([9]). In April 2021, the European Commission hence published a full-fledged proposal for a new regulation laying down harmonised rules on Artificial Intelligence, known as the AI Act ([10]), on which the European Parliament and the Council reached political agreement in December 2023.

The AI Act adopts a risk-based approach, categorising AI systems based on the level of risk they raise to health, safety and fundamental rights. Systems posing an unacceptable risk are prohibited, whereas those with a high risk are subjected to new requirements and a mandatory conformity assessment prior to their use or placement on the market. Providers of high-risk systems can opt to comply with (still to be developed) technical standards and benefit from a presumption of compliance. ([11]) The regulation also imposes new (transparency) obligations on providers of AI systems that pose a risk of deceit, and on providers of general-purpose AI ('GPAI') models. Enforcement will occur by independent national supervisory authorities and – for GPAI models posing a systemic risk – by a new AI office that will be set up at the European Commission. In addition, a European AI Board composed of representatives from national authorities – akin to the European Data Protection Board ('EDPB') – will coordinate Member States' approaches and facilitate their exchange of best practices. AI systems used by EU institutions will be supervised by the European Data Protection Supervisor ('EDPS'), which issued two opinions on the text during the political negotiations ([12]). Finally, an EU-wide database will be set up ([13]), in which certain providers and deployers of (high-risk) AI systems will need to register certain information about their system, which should facilitate monitoring and enforcement of the AI Act, and enhance public transparency.

The AI Act has many strengths and weaknesses, and will undoubtedly be the object of many future commentaries. In this article, I will solely focus on the AI Act's relationship with EU data protection law. With the latter, I intend to denote not only the Union's secondary legislation dealing with personal data protection rules, but also relevant primary legislation. This includes Article 8 of the EU Charter of Fundamental Rights ('CFR') which enshrines personal data protection as a fundamental right, and Article 16 of the Treaty on the Functioning of the

([9]) That same year, then-German Chancellor Angela Merkel called for a new regulation for AI, '*similar to the General Data Protection Regulation, that makes it clear that artificial intelligence serves humanity*', and Ursula von der Leyen, then-President Elect of the Commission, promised to follow suit in her Political Guidelines.

([10]) European Commission, Proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final.

([11]) See Article 40(1) of the AI Act.

([12]) See EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), issued on 18 June 2021; EDPS Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments, issued on 23 October 2023. See also EDPS Opinion 20/2022 on the Recommendation for a Council Decision authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law, issued on 13 October 2022, which does not pertain to the EU's AI Act but to the Council of Europe's negotiations on an international AI Convention.

([13]) See Article 71 of the AI Act, which establishes that the Commission, in collaboration with Member States, will set up and maintain an EU database containing information on high-risk AI systems.

European Union ('TFEU') which grants all individuals the right to the protection of their personal data, and which enables the EU legislator to '*lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law*'.

In what follows, I argue that the interrelationship between data protection law and the AI Act can be examined from (at least) three perspectives. First, data protection can be seen as an underlying *foundation* of the AI Act's content, both substantively (in terms of the protective measures it enshrines) and procedurally (in terms of the AI Act's legal basis). Second, the data protection framework can be seen as *complementary* to the AI Act, as the latter is to a large extent meant to fill the legal gaps left open by the former. Third, data protection law can also be used as a basis to *evaluate* the AI Act's aspirations and shortcomings, and to offer a critique on the protection it (fails to) offer for personal data and for fundamental rights more generally. I conclude by accentuating that, despite the coming into being of a new AI-specific regulation, data protection will remain of paramount importance to protect people against the adverse effects of AI systems, and to safeguard the EU's core values of liberal democracy.

2. Data protection as a foundation of the AI Act

The AI Act contains numerous references to its ambitions to protect fundamental rights and other EU values in the context of AI. Yet despite this lofty rhetoric, the AI Act is first and foremost a market harmonization instrument. Central to its approach is the idea that AI systems are regulatable 'products' and 'services', that it is beneficial to achieve a single European market for AI, and that the realization of such a market requires harmonizing measures to prevent obstacles to trade, particularly given the risk that Member States adopt diverging AI-requirements. The fact that these harmonizing measures seek to counter AI's harmful effects and ensure a '*high level of protection of health, safety and fundamental rights*' is important, but comes afterwards. Member States who would like to offer a higher level of protection are, for instance, generally barred from doing so (with only a few exceptions), since the Act's maximum approach to harmonization creates a ceiling of protection rather than a floor ([14]).

The AI Act's market-oriented approach also manifests itself in the chosen enforcement architecture, which is based on the New Legislative Framework ([15]). Providers of high-risk AI systems must for instance carry out a conformity

([14]) See Recital 1 of the AI Act, stating that '*This regulation ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.*'

([15]) The new legislative framework (NLF) is a package of EU measures that aim to improve market surveillance and boost the quality of conformity assessments in product legislation, while clarifying the use of CE marking. Its incorporation in the AI Act has also been criticised e.g. in Veale, M., and Zuiderveen Borgesius, F.J., 'Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach', *Computer Law Review International*, Vol. 22 No. 4, 2021, p. 111.

assessment to comply with a new set of mandatory requirements and affix a CE-mark to their system. Accordingly, AI systems are treated like washing machines or fridges which simply need to fulfil a list of technical criteria, despite being rather complex socio-technical systems that can lead not only to individual (physical) harm, but also undermine various collective and societal interests ([16]).

Against this background, the AI Act's reliance on Article 114 TFEU as its main legal basis is understandable, as it allows the Parliament and Council to adopt measures for the approximation of Member States' provisions which have as '*their object the establishment and functioning of the internal market*'. One could even argue that a product-oriented approach was the only way to adopt measures to better protect fundamental rights in the sphere of AI, given the absence of a more general EU legal basis enabling the protection of fundamental rights more directly ([17]). In this regard, it can be recalled that the GDPR's predecessor, Directive 95/46/EC ([18]), also had Article 114 TFEU as its legal basis; only later, the importance of the right to personal data protection became more acknowledged and resulted in a separate legal basis by means of Article 16 TFEU.

At the same time, it should be emphasised Article 114 TFEU does not necessarily mandate an approach that treats 'fundamental rights risks' at the same level as 'technical safety risks' and that seemingly pushes fundamental rights protection into a straitjacket of technical standards ([19]). Furthermore, given the intricate link between AI's risks, the right to data protection, and other fundamental rights, the EU legislator could have relied on Article 16 TFEU to adopt a rights-oriented rather than a risk-oriented approach to regulate AI (or even on Article 352 TFEU) ([20]) . Instead, the AI Act's reliance on Article 16 TFEU is minimal. Though it is mentioned as the regulation's second legal basis, this only extends to the provisions that regulate the use of AI for the '*purpose of law enforcement*', and only with regard to law enforcement's use of AI for remote biometric identification, for risk assessments of natural persons, and for biometric categorisation ([21]). This hence raises some questions on the relationship between the AI Act and already existing secondary legislation that seeks to safeguard the right to data

([16]) See in this regard also Smuha, N.A., 'Beyond the individual: governing AI's societal harm', *Internet Policy Review*, Vol. 10, No. 3, 2021, p. 5.

([17]) Indeed, it is not uncommon that a piece of legislation which is based on Article 114 TFEU has the goal to inter alia contribute to the protection of one or more fundamental rights.

([18]) See footnote 5.

([19]) For a more extended critique, see e.g. Veale, M. and Zuiderveen Borgesius, F.J., op. cit. (footnote 15); Smuha, N.A., and Yeung, K., op. cit. (footnote 6).

([20]) Article 352 TFEU enables the EU legislator to adopt measures '*if action by the Union should prove necessary, within the framework of the policies defined in the Treaties, to attain one of the objectives set out in the Treaties, and the Treaties have not provided the necessary powers*'. However, since this requires unanimous action by the Council, this provision is generally to be avoided when there is a risk that some Member States might disagree. It also only requires 'consent' from the European Parliament, which could raise concerns from a democratic representation perspective.

([21]) See Recital 3 of the AI Act. For the use of (remote) biometric identification systems and biometric categorization systems, Article 9 of the GDPR and Article 10 of the LED already provide a base layer of protection given the sensitivity of the data concerned.

protection based on Article 16 TFEU, including not only the GDPR, but also the Law Enforcement Directive ('LED') ([22]) and the Data Protection Regulation for EU institutions, offices, bodies and agencies ('EUDPR') ([23]).

In its preamble, the AI Act sought to express this relationship by stating – with regard to those three specific law enforcement applications – that the use of AI in this context must occur without prejudice to pre-existing data protection legislation, and that the AI Act's new safeguards come on top of it. In other words, Article 16 TFEU is the legal basis that justifies additional safeguards in the specific context of law enforcement. The AI Act, however, mentions many other AI systems and practices that raise personal data protection concerns, and for which Article 16 TFEU does not explicitly serve as a legal basis. This notwithstanding the fact that the additional safeguards the AI Act imposes elsewhere – from mandatory requirements for high-risk systems with fundamental rights implications, and the (limited) prohibition of certain data processing practices like social scoring, to the introduction of a right to an explanation – *also* contribute to data protection.

Consider, for instance, the AI Act's prohibition of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage. The reason for this prohibition is, according to the preamble, that '*this practice adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy*' ([24]). Moreover, in some cases, the AI act also seems to codify provisions that can at least in part be derived from data protection-related judgments of the Court of Justice of the EU ('CJEU'). The AI Act's new safeguards for post-remote biometric identification by law enforcement are a good example thereof, as they reflect the previously established case law that the untargeted (biometric) data processing by law enforcement without any link to a crime or threat is unlawful ([25]). In the context of AI-based biometric identification and categorisation, the AI Act also reiterates that the processing of biometric data is already prohibited by the data protection framework subject to limited exceptions, and that this framework in any case remains applicable as *lex specialis* ([26]).

([22]) Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

([23]) Regulation 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

([24]) See Recital 43 of the AI Act.

([25]) See e.g. Judgment of the Court of Justice of 21 June 2022, *Ligue des droits humains*, C-817/19, ECLI:EU:C:2022:491.

([26]) See Recital 38 of the AI Act. Furthermore, when it comes to real-time biometric identification by law enforcement in public places, the AI Act is also careful in stating that its provisions are not meant to provide a legal basis for the processing of such data under Article 8 of the LED.

In sum, data protection at least *implicitly* plays a role in the underlying rationale of imposing new safeguards and obligations in the AI Act. This is why, to avoid any misunderstanding, the AI Act's preamble has a more general recital stating that '*it does not seek to affect the application of existing Union law governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments*' ([27]). The regulation also explicitly '*does not affect the obligations of providers and deployers of AI systems in their role as data controllers or processors*' when it comes to the design, development and use of AI, and clarifies that '*data subjects continue to enjoy all the rights and guarantees awarded to them by such Union law*', including the rights related to automated individual decision-making and profiling. It is, however, one thing to include this language in the preamble, and another thing to actually implement the AI Act in a way that does not run counter to the existing data protection framework. In this respect, it should be noted that the EDPS' suggestion to make national data protection authorities the default national supervisory authorities for the AI Act ([28]) – in light of the numerous overlaps with data protection law requirements – was not upheld by the EU legislator ([29]). Hopefully, the above recitals can however at the very least offer guidance to courts who will likely be faced with questions on the AI Act's interpretation and its relationship with data protection law.

3. Data protection as complementary to the AI Act

In addition to normatively underpinning the AI Act, data protection law can also be seen as complementary to it. As the above recitals demonstrate, the AI Act should not be considered as a *lex specialis* that deviates from data protection rules, but rather as a supplement to fill in the legal gaps that the GDPR, the LED, the EUDPR and other pieces of EU legislation did not yet satisfactorily cover. The AI Act hence serves as a protective layer *on top* of existing data protection rules. In other words: AI system providers and deployers must comply with the

([27]) See Recital 10 of the AI Act.

([28]) See EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), issued on 18 June 2021, p. 14-15. The EDPS reiterated this suggestion in its EDPS Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments, issued on 23 October 2023, p. 20.

([29]) This means that Member States have the liberty to designate other authorities as the supervisory authority for the purpose of the AI Act. That said, in some instances (e.g. in the context of regulatory sandboxes processing personal data, as per Article 57(10) of the AI Act), the regulation does provide that the national competent authorities must associate the national data protection authorities to the operation of the AI regulatory sandbox and involve them in the supervision of the personal data related aspects. It can also be noted that representatives of the national supervisory authorities will constitute the European AI Board, in which the EDPS will sit as an observer, pursuant to Article 65(2) of the AI Act.

data protection framework *and* with the AI Act ([30]). Rather than overlapping, the provisions of the aforementioned frameworks are meant to be complementary, which is evident from several of the AI Act's provisions.

A good example is Article 27 of the AI Act, which deals with the obligation to undertake a fundamental rights impact assessments ('FRIAs') ([31]). Prior to deploying a high-risk AI system, certain AI deployers – namely bodies governed by public law, private operators providing public services, and banking and insurance entities – will need to assess the impact of their system's use on fundamental rights (based on a template that the AI Office will develop) ([32]). The Article's fourth paragraph specifies that if any of the obligations laid down in this article are already met through the data protection impact assessment ('DPIA') conducted pursuant to Article 35 GDPR or Article 27 of LED, the FRIA shall be conducted in conjunction with that DPIA. In its 'Analysis of the final compromise text' of the AI Act of 26 January 2024, this was explained by the Council as implying that the FRIA '*will need to be carried out only for aspects not covered by other legal obligations, such as Data Protection Impact Assessment under the GDPR and will be procedurally aligned with existing processes in order to eliminate any overlap and additional burden*' ([33]).

Another way in which the AI Act complements the data protection framework is through its aim to '*strengthen the effectiveness of [such] existing rights and remedies by establishing specific requirements and obligations, including in respect of transparency, technical documentation and record-keeping of AI systems*'. Undoubtedly, the enhanced transparency that the AI Act engenders, both externally (e.g. through the newly established database) and internally (e.g. through the imposition of documentation obligations that can later serve in investigations), can also contribute to better data protection. One manifestation of this interplay can be found in the provisions on the new EU database of high-

([30]) See in this regard Recital 9 of the AI Act, which explicitly states that the AI act is complementary to existing Union law, notably on data protection. Recital 69 also states that the right to privacy and to the protection of personal data must be guaranteed throughout the entire lifecycle of the AI system, and reiterates the principles of data minimisation and data protection by design and by default, which apply whenever personal data is being processed in AI-context.

([31]) This obligation made its way into the regulation through the European Parliament's mandate, thanks to the pressure exerted by a large number of human rights- and civil society organisations. Most notably, the EU's Fundamental Rights Agency already called upon such assessments in 2020 in its report '*Getting the future right – Artificial intelligence and fundamental rights*', which was also noted by the EDPB and the EDPS in their Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), issued on 18 June 2021, p. 9.

([32]) The assessment must also be notified to the relevant market surveillance authority. An exception is foreseen in Article 46(1) of the AI Act, which allows any market surveillance authority to '*authorise the placing on the market or putting into service of specific high-risk AI systems within the territory of the Member State concerned, for exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets*'.

([33]) EU Presidency, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts: Analysis of the final compromise text with a view to agreement, 5662/24, Brussels, 26 January 2024, p. 4.

risk systems, in which providers and certain deployers must register certain information. As part of that information, the AI Act now mandates deployers to register '*a summary of the data protection impact assessment*' they had to carry out in accordance with Article 35 GDPR or Article 27 LED, '*where applicable*' ([34]). Furthermore, Article 13 of the AI Act obliges AI providers to offer specific information about their high-risk system to AI deployers, and Article 26(9) mandates deployers to use this information to comply with their obligation to carry out a DPIA.

More critically, Article 86 of the AI Act also provides a 'right to an explanation' for those who are subjected to high-risk AI systems. Indeed, anyone who is '*subject to a decision which is taken by the deployer on the basis of the output from an high-risk AI system … and which produces legal effects or similarly significantly affects him or her in a way that they consider to adversely impact their health, safety and fundamental rights shall have the right to request from the deployer clear and meaningful explanations on the role of the AI system in the decision-making procedure and the main elements of the decision taken*'. For those who consider that the GDPR already affords data subjects with a 'right to an explanation', this Article may seem superfluous, despite the controversy on whether and to which extent such right exists ([35]). The EU legislator however seemingly sought to avoid this controversy by adding that '*this Article shall only apply to the extent that the right … is not already provided for under Union legislation*' ([36]), hence being complementary to any existing explanation-rights that already exist under the data protection framework. Moreover, since this Article does not use the term 'data subject' but rather 'affected person', the right to an explanation can also be invoked by non-data subjects.

In other instances, the AI Act creates a legal basis for the processing of personal data. Let me offer two examples. Article 10 sets out a data quality requirement for high-risk systems, including the requirement to '*detect, prevent and mitigate possible biases*'. However, testing whether an AI system is biased against people with a certain protected characteristic may necessitate the processing of data about those characteristics in the first place. Article 10(5) therefore specifies that '*to the extent that it is strictly necessary for the purposes of ensuring bias detection and correction in relation to the high-risk AI systems, the providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons*'. It also subjects the reliance on this legal

([34]) See Annex VIII of the AI Act, Section C, 5.

([35]) See in this regard e.g. Wachter, S., Mittelstadt, B., and Floridi, L., 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law*, 7(2), 2017, p. 76–99; Selbst, A.D., and Powles, J., 'Meaningful information and the right to explanation', *International Data Privacy Law*, Vol. 7, No. 4, 2017, p. 233–242; Casey, B., Farhangi, A., and Vogl, R., 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise', *Berkeley Technology Law Journal*, 34, 2019, p. 143-188.

([36]) See Recital 171 of the AI Act.

basis to a set of conditions, such as the fact that this goal cannot be effectively fulfilled by processing other data (such as synthetic or anonymised data), and that such data cannot be transmitted, transferred or otherwise accessed by other parties ([37]).

The AI Act also creates a legal basis in the context of regulatory sandboxes, a vehicle that is meant '*to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring compliance of the innovative AI systems*' with existing Union and national rules ([38]). Concretely, Article 59 of the AI Act provides that (prospective) AI providers can use personal data that was lawfully collected for other purposes to develop, train and test certain AI systems in the sandbox when a set of cumulative conditions are met ([39]). This includes, amongst others, the fact that the systems must be developed to safeguard a substantial public interest, that there are effective monitoring mechanisms to identify if any high risks to the rights and freedoms of the data subjects can arise, and that logs of the processing of such personal data are kept for the duration of the sandbox participation.

That said, and notwithstanding the examples above, the complementary relationship between the AI Act and the data protection framework is not always clearcut. In their Joint 5/2021 Opinion, the EDPB and the EDPS for instance asked the EU legislator to better explain what the AI Act understands with a 'risk-based approach', and whether and how this concept encompasses risks to fundamental rights ([40]). The AI Act's final version, however, does not fully clarify this matter. Instead, the concept of risk is defined in Article 3(2) as '*the combination of the probability of an occurrence of harm and the severity of that harm*'. This can be criticised, as the infringement of a fundamental right does not necessarily require any 'harm' to ensue: the very infringement of a fundamental right, regardless of any proof of harm, is what matters ([41]).

Furthermore, one of the implications of this complementarity is the fact that the lawfulness of an AI system's development and deployment cannot be assessed by looking at the AI Act alone. This is something the AI Act does make explicit. For instance, as regards the list of prohibited AI practices, the relevant provision in the AI Act states that it '*shall not affect the prohibitions that apply where an artificial intelligence practice infringes other Union law*'. The preamble also clarifies that '*practices prohibited by Union legislation,*

([37]) Arguably, these conditions already exist in the current data protection framework, yet the EU legislator likely sought to include them in this Article to prevent the potential unlawful reliance on this legal basis.

([38]) See Recital 139 of the AI Act. Interestingly, in Article 57(3), the AI Act provides that the EDPS may also establish an AI regulatory sandbox for the EU institutions, bodies and agencies.

([39]) This article can however not be used as a legal basis in the meaning of Article 22(2)(b) of Regulation (EU) 2016/679 and Article 24(2)(b) of Regulation (EU) 2018/1725, which is explicitly carved out.

([40]) See footnote 12, p. 8.

([41]) See in this regard Hildebrandt, M., 'Beyond the GDPR: The Fundamental Issues with the Harms-Based Approach', Utrecht University, 22 September 2023, p. 11.

including data protection law' are not affected by this regulation and hence remain prohibited, despite their absence from this list. ([42]) Accordingly, at least in theory, the AI Act does not exclude incompatibilities between AI systems that are not listed among the prohibited AI practices and data protection law (or other fundamental rights). This also means that national legislators should not be precluded from adopting domestic legislation that prohibits certain AI practices based on such incompatibility, nor should the AI Act prevent people to argue that certain AI systems are unlawful and should be prohibited in light of their rights-infringing nature.

However, in practice, in the absence of such an explicit domestic rule, this argument would need to be brought before a court to have any meaningful effect, since the AI Act now does set the tone for AI 'red lines' in the European Union. While judges will still be able to assess AI applications based on their compatibility with data protection law and fundamental rights more generally, they might be more reluctant to do so, or might at least rely on the EU legislator's assessment as codified (or not) in the AI Act.

The possibility to challenge the lawfulness of AI systems theoretically also exists when it comes to high-risk AI systems. In this regard, the AI Act clarifies ([43]) that the fact that a system is classified as high-risk should not be interpreted as indicating that its use is lawful under other acts of Union law (or national law implementing Union law), '*such as on the protection of personal data, the use of polygraphs or the use of emotion recognition systems*'. However, given the AI Act's explicit intention to comprehensively regulate AI systems that pose a risk to fundamental rights, it may be challenging to argue that AI systems which are included in the high-risk list are nevertheless unlawful. At the very least, the burden of proof on the side of the claimant will be very high, and is likely to only be reached if there is a detailed domestic rule that designates a particular AI system or practice as unlawful due to its incompatibility with data protection law. Moreover, even in that case, that domestic rule could still be challenged by the AI system's provider on internal market-based grounds, in light of the regulation's maximum approach to harmonisation. The AI provider could argue that the domestic regulator imposed an unlawful market restriction on AI products and services by inappropriately 'balancing' the free movement of goods with the right to data protection, despite its good intentions. And given the EU's broad protection of 'market access', as also acknowledged by the CJEU, the provider could in theory try to strike such a domestic rule down ([44]).

([42]) See Recital 45 of the AI Act.

([43]) See Recital 63 of the AI Act.

([44]) For an overview of the (at times difficult) interplay between internal market law and fundamental rights, see also e.g. Reynolds, S., 'Explaining the constitutional drivers behind a perceived judicial preference for free movement over fundamental rights', *Common Market Law Review* Vol. 53, 2016, p. 643–678.

4. Data protection as critique of the AI Act

This brings me to the third type of relationship I wish to discuss, which focuses on the role that the data protection framework can play in evaluating and critiquing the AI Act. It can be recalled that the right to personal data protection, enshrined in Article 8 CFR alongside the right to privacy in Article 7 CFR, is first and foremost a fundamental right, constituting a higher norm with which all EU secondary legislation must comply. This evidently also includes the AI Act. Accordingly, these rights can serve as a basis to assess the AI Act's aptness in protecting and avoiding undue interference with fundamental rights, and enables us to formulate a critique where it falls short of those aspirations.

When comparing the European Commission's original proposal for an AI Act of April 2021 with its final version in 2024, there are several sections where the EU legislator has come a long way in improving the legal safeguards it contains. This is in part due to the feedback that was received on this original proposal, and the strong criticism on the fact that it neglected to properly consider those adversely affected by AI systems, and merely focused on obligations on and between AI providers and deployers ([45]). The abovementioned opinions of the EDPS also played a pivotal role in enhancing the regulation's protection, by pointing to numerous provisions in the proposal that were inadequate to safeguard fundamental rights generally, and the right to data protection more specifically. While the EU legislator seemed to have listened to this feedback, it did so only in part, and several concerns remain.

It goes beyond the scope of this article to provide an extensive critique of the AI Act's text, so let me merely mention a few points that were raised by the EDPS in its feedback, but that were not duly addressed. In Opinion 5/2021, various AI practices were identified that merit being prohibited altogether, in light of the unacceptable risks they pose to fundamental rights. One of these entails the use of AI systems to '*categorise individuals from biometrics […] into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination prohibited under Article 21 of the Charter*' ([46]). The final version of the AI Act, however, does not include such a prohibition. Instead, it only prohibits biometric categorisation systems that are used to deduce or infer an individuals' political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation ([47]). All

([45]) For an extensive critique, see Smuha, N.A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., and Yeung, K., *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, SSRN, 2021.

([46]) EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), issued on 18 June 2021, p. 13.

([47]) See Article 5(1)(g) of the AI Act.

other applications of biometric categorisation are treated 'merely' as a high-risk application and are subjected to mandatory requirements ([48]), and to the transparency requirements of Article 50 ([49]).

Likewise, despite the fierce criticism on this application ([50]), the AI Act only subjects emotion recognition systems to a very limited ban, namely in the areas of workplace and education institutions and with exceptions where the system is used for 'medical or safety' reasons. Other applications fall under the list of high-risk systems (which is already an improvement though, as the original proposal did not even classify them as high-risk). Furthermore, the EU legislator did not include a full ban on real-time remote biometric identification like the EDPB and EDPS requested, but retained exceptions that are similar to the original draft ([51]). This means that, despite the additional safeguards the AI Act sought to put in place, public spaces will increasingly be equipped with facial recognition cameras to ensure they can be used 'in case' an exception arises ([52]), inevitably increasing surveillance concerns and risks of abuse. Despite all these concerns, the AI Act is now final and expected to shape the use of AI in the EU for years to come.

What, then, can be undertaken by those who believe that the AI Act woefully underperforms in its aspiration to protect EU values? When it comes to high-risk systems, there is still a possibility to (re-)assess AI systems in the future and to add them to the list, pursuant to the procedure set out in Article 7 of the AI Act ([53]). Yet when it comes to the list of prohibited systems, no such flexibility is foreseen. Instead, it will be the task of EU institutions and Member States to ensure that, when they implement the AI Act's provisions, they do so in a way that ensures compatibility with the Charter and Treaties. It will be the task of courts to ensure that, when they interpret the AI Act – which they will undoubtedly be called upon to do sooner rather than later – this occurs in a way that secures alignment with fundamental rights. And it will be the task of citizens, civil society organisations and public interest groups to remain vigilant and ensure those actors carry out their respective task in a rights-protecting

([48]) See Annex III(1)(b) of the AI Act.

([49]) Of course alongside, as discussed above, the existing requirements under data protection legislation.

([50]) See EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), issued on 18 June 2021, p. 12, where the EDPB and EDPS suggested a ban on emotion recognition systems '*except for certain well- specified use-cases, namely for health or research purposes*' and '*always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation*'.

([51]) See Article 5(1)(h). These exceptions concern the use of real-time biometric recognition for the targeted search for specific victims or missing persons; the prevention of an imminent threat to someone's life or physical safety or of a terrorist attack; and the localisation or identification of someone suspected of having committed a specific criminal offence.

([52]) See also the criticism in Smuha, N.A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., and Yeung, K., op. cit. (footnote 45).

([53]) Concretely, the Commission is empowered to adopt delegated acts to amend Annex III by adding or modifying use cases of high-risk AI systems where two conditions are fulfilled: (a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III; (b) the AI systems pose a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

manner. Finally, in a more drastic scenario, one could in theory also conceive of pursuing an action for annulment against sections of the AI Act that fail to protect the right to personal data protection and the interlinked right to privacy to a satisfactory degree. While it is difficult to assess the feasibility (or necessity) of such an action, it is important to remain aware of the fact that this is, at least in theory, a possibility. After all, as the CJEU reminded us in the *Digital Rights Ireland* case, all secondary EU legislation must comply with primary law, including the fundamental right to data protection, or it runs the risk of being invalidated ([54]).

5. Conclusion

In this article, I dived into the relationship between the EU data protection framework and the forthcoming AI Act. Having discussed the foundational, complementary and evaluating role that data protection can play in the context of AI, the above analysis leads me to conclude that data protection rules remain essential to protect individuals against AI's risks, and to safeguard their rights. The fact that a new AI-specific regulation will soon kick in, and that its provision seek to protect '*health, safety and fundamental rights*', does not alter the paramountcy of data protection law in the age of AI (Acts). In fact, unintuitively perhaps, I would argue that this new regulation's maximum approach to harmonization, and the numerous concerns it unfortunately leaves untouched, render the data protection framework more important than ever.

That said, many of the AI Act's provisions explicitly refer to data protection rules, and offer interpretative guidance to ensure that its implementation does not undermine those rules, but rather reinforces them and enhances their reach. It will hence be essential for the authorities that will implement, monitor and enforce the regulation, and for the courts interpreting it, to rely on this guidance and ensure that the AI Act not only fills the legal gaps of the data protection framework, but that the data protection framework is also used to fill the legal gaps of the AI Act.

([54]) Judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Seitlinger and others,* C-293/12 and C-594/12, ECLI:EU:C:2014:238.

18

The future of effective data protection enforcement

Dr. Lisette Mustert

The future of effective data protection enforcement

Dr. Lisette Mustert (*)

The first years of experience with the GDPR have shown serious deficiencies in the system of enforcement, resulting inter alia from the highly integrated but overly complex administrative procedures regulating enforcement. This chapter explores three possible solutions to these deficiencies and argues that harmonisation of administrative procedural laws will only have an added value if it covers a broad range of aspects to overcome all the structural problems. Therefore, this chapter argues that brave thinking regarding the design of the enforcement system itself is needed. This will most likely result in an increased role for an EU authority, either as a strong coordinator in the enforcement network or as an authority responsible for direct supervision of the very large data controllers and processors.

1. Introduction

The General Data Protection Regulation ('GDPR') aims to lay down a strong and coherent data protection framework, backed by strong enforcement ([1]). While strong enforcement was supposed to be realised by a novel system of shared enforcement ([2]), the first cracks within this system began to show not long after the entry into force of the GDPR. In principle, enforcement of the GDPR is arranged alongside complex decentralized procedures, where national supervisory authorities address cross-border GDPR violations in a type of co-decision making process ([3]). Involvement of an EU body – the European Data Protection

(*) Lisette Mustert is an Assistant Professor of administrative law at Utrecht University, the Netherlands, and affiliated to the Utrecht Centre for Regulation and Enforcement in Europe ('RENFORCE').

(1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 216 on the protection of natural persons with regard to the processing of personal data on the free movement of such data and repealing Directive 95/46 (General Data Protection Regulation), OJ L 119/1, 4.5.2016, p. 1, recital 7.

(2) See for a definition of 'shared enforcement' Karagianni, A.M., *The Protection of Fundamental Rights in Composite Banking Supervision Procedures*, Europa Law Publishing, Zutphen, 2022, p. 21 and 23.

(3) Chapter VII, section 1 GDPR.

Board ('EDPB') – occurs only where correct and consistent enforcement requires the EDPB to intervene ([4]). This highly integrated but complex administration ([5]), leads to structural problems in the GDPR's enforcement mechanism resulting in unexplained delays or refusals to act upon complaints at all, mostly in the context of cross-border data processing ([6]). This chapter aims to discuss the future of effective data protection enforcement by exploring ways for improvement either by means of increased harmonization of enforcement procedures in EU law ([7]), or by an increased role for a centralized node in the enforcement network ([8]). In order to do so, this chapter briefly introduces the GDPR's system of cross-border enforcement and, secondly, explores the lessons learnt so far. Hereafter the chapter turns to a discussion of several solutions to the deficits in the EU's data protection enforcement mechanism.

2. Enforcement of the GDPR: a national affair

Enforcement of the EU's data protection rules is, in principle, a national affair where Member States establish completely independent supervisory authorities ('SAs') responsible for monitoring and enforcing the GDPR ([9]). This means that the EU is highly dependent upon the Member States for effective data protection enforcement. It can, therefore, not be excluded that large differences in enforcement approaches and strategies exist, not only because Member States' legal systems differ, but also due to the differences in perception of the importance of enforcement of the EU rules ([10]). For that reason, the EU has increasingly intervened in enforcement processes in the Member States, which aimed at bringing about an intensification and a certain degree of uniformity in enforcement of EU law within the Member States ([11]). First, it is now settled case law that national enforcement measures must fulfil legal requirements such as equivalence, effectiveness, proportionality and dissuasiveness, based on the Member States' duty of sincere cooperation ([12]). Secondly, the EU has increasingly adopted legislative instruments in which the EU legislature lays down procedural rules for enforcement, and the requirement of cooperation

([4]) Chapter VII, section 2 GDPR.

([5]) See for a definition of the EU's integrated administration Hofmann, H.C.H., Rowe, G.C., and Türk, A.H., *Administrative Law and Policy of the European Union*, Oxford University Press, Oxford, 2011, p. 12.

([6]) As addressed by the EDPS, see EDPS speech at the "Future of Data Protection: Effective Enforcement in the Digital World" conference, 16-17 June 2022.

([7]) As proposed by the EU Commission, see Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM(2023) 348 final.

([8]) Either by an increased role in coordinating decentralized enforcement procedures, or by granting an EU body direct enforcement powers with regard to the supervision of large data controllers and processors, see section 3.2 and 3.3.

([9]) Article 52(1) GDPR. See for a clarification of the meaning of 'complete independence' the Judgment of the Court of Justice of 9 March 2010, Commission / Germany, C-518/07, ECLI:EU:C:2010:125, paragraph 30.

([10]) Jans, J.H., Prechal, S., and Widdershoven, R.J.G.M., *Europeanisation of Public Law*, Europa Law Publishing, Zutphen, 2015, p. 266.

([11]) *Ibid*, p. 266.

([12]) See e.g., Judgment of the Court of Justice of 21 September 1989, *Commission v Greece (Greek Maize),* C-68/88, ECLI:EU:C:1989:33921, paragraph 24.

between the Member States aimed at promoting effective enforcement of transnational violations of EU law ([13]). The GDPR forms an illustrative example where procedural rules and cooperation procedures, brought together in one legislative instrument, aim to increase both effectiveness and consistency in enforcement.

2.1. Effective and consistent enforcement of the GDPR

The GDPR lays down several enforcement tasks for the national SAs, accompanied with procedural rules. Generally, independent SAs are responsible for monitoring and enforcing the GDPR ([14]). A data subject has the right to complain to these SAs if she or he believes that the processing of her or his personal data infringes the GDPR. The submission of complaints must also be facilitated by the SAs ([15]). SAs are, furthermore, under an obligation to *handle* these complaints, and to *investigate* them to the extent appropriate ([16]). In order to do so, the GDPR offers the SAs a similar set of investigative and corrective powers ([17]), and sets out the conditions relevant for determining whether to impose an administrative fine and deciding on the amount of it ([18]).

Besides harmonizing enforcement procedures, the EU legislature requires SAs to cooperate with each other where alleged GDPR violations affect several jurisdictions within the EU ([19]). Hence, SAs shall exchange all relevant information with each other, provide mutual assistance, organize joint operations, and reach consensus on the draft decision (and every other step in the enforcement procedure) ([20]). Such cooperation among SAs aims to ensure consistency in the application and enforcement of the GDPR ([21]), and is supposed to offer a high level of protection of data subjects. While SAs shall cooperate to enforce transnational GDPR violations, one SA shall take the lead in this procedure in accordance with the one-stop-shop procedure ([22]). This prominent role of the lead SA is believed to increase the efficiency in enforcement ([23]), while the cooperation procedure prevents the lead SA from adopting a go-it-alone

([13]) Jans, J.H., Prechal, S., and Widdershoven, R.J.G.M., op. cit. (footnote 10), p. 266.

([14]) Articles 51(1) and 57(1)(a) GDPR.

([15]) Articles 77(1) and 57(2) GDPR.

([16]) Article 51(1)(f) GDPR.

([17]) Article 58(1)(2) GDPR.

([18]) Article 83 GDPR.

([19]) Articles 51(2) and 57(1)(g) GDPR.

([20]) Articles 60 to 62 GDPR.

([21]) Martinius, E. and Mastenbroek, E., 'Fit for purpose? Assessing Collaborative Innovation in the European Network for Prosecutors for the Environment', *European Journal of Risk Regulation*, Vol. 10, 2019, p. 488.

([22]) Article 56(1) GDPR.

([23]) Because this lead SA is able to develop a strong body of knowledge and expertise about the processing operations of these data controllers or processors who locate their main establishment on its territory, which is relevant for determining the appropriate enforcement approach or response to this company.

attitude ([24]). In other words, proximity is ensured by enabling every SA to protect its data subjects via the cooperation procedure ([25]) – e.g., by opposing a lead SA's draft measure ([26]) – also if these data subjects are affected by data processing that physically takes place outside the SA's territory.

While GDPR enforcement is organized mainly alongside decentralized procedures, the EU legislature established the EDPB as centralized node in the enforcement network ([27]). The EDPB is supposed to function as a guardian of correct and consistent enforcement by means of the adoption of, *inter alia*, guidelines, opinions, and (urgent) binding decisions ([28]). While guidelines and opinions aim to provide non-binding guidance to the SAs regarding the correct application and enforcement of the GDPR ([29]), the EDPB's binding decisions addressed to the SAs in individual cases either aim to settle disputes among the national authorities on the correct enforcement approach, or to settle urgent matters ([30]).

2.2. Experiences with cross-border GDPR enforcement

The design of the GDPR's cross-border enforcement system sounds promising, however, the current reality is different due to several reasons. First, while the GDPR at first sight seems to harmonize enforcement procedures to a large extent, many aspects of the enforcement procedure remain unregulated and are, therefore, determined by national procedural laws and strategies([31]). This discretion leads to unequal enforcement of the GDPR among the Member States – e.g. regarding the admissibility of complaints, whether or not to commence formal investigations, the scope of investigations, or the choice for softer or stronger corrective measures. The application of national procedural law also leads to notable differences in the level of procedural protection of data subjects and data controllers and processors under investigation. An illustrative example forms the definition of 'parties' and the right to be heard for complainants. Some Member States recognize the complainant as party to the

([24]) Council Doc. 10139/14 of 26 May 2014, p. 4.

([25]) Council Doc. 15656/1/14 REV 1 of 28 November 2014, p. 5.

([26]) This is what Li and Newman call a horizontal channel of 'peer accountability' where concerned SAs exercise supervision of the lead SAs enforcement actions by reviewing the draft decisions and raising potential objections. See Li, S. and Newman, A.L., 'Over the shoulder enforcement in European regulatory networks: the role of arbitrage mitigation mechanisms in the General Data Protection Regulation', *Journal of European Public Policy*, Vol. 29, No. 10, 2022, p. 1705.

([27]) Article 70(1)(a) GDPR.

([28]) Articles 64 to 66 GDPR.

([29]) See Article 70(1)(d)(f)-(m) GDPR.

([30]) Article 65(1)(a)(b)(c) GDPR.

([31]) See for a comprehensive overview Mustert, L., *Cross-border enforcement of the GDPR by independent administrative authorities*, PhD dissertation, University of Luxembourg, 2023.

procedure and, hence, she or he is being heard before an enforcement decision is taken ([32]). In other Member States, however, this right for complainants is limited to situations where the complaint is being dismissed or rejected, which right can even be restricted further for efficiency reasons ([33]). Further differences among the Member States exist, *inter alia*, with regard to the right to access the file, the right to careful and fair decision-making, the duty to give reasons, or timely decision-making ([34]).

Secondly, the system established in the GDPR to overcome such differences in enforcement – by means of establishing so-called 'peer pressure' among the SAs in the cooperation procedure ([35]) – does not live up to its promises. Experiences with the one-stop-shop and cooperation mechanism reveal two main causes which hinder concerned SAs from meaningful participation in enforcement procedures. First, the cooperation procedure is defined in minimal terms, allowing SAs to interpret their cooperative duties as it may fit national strategies and interests ([36]). Therefore, the lead SA can bar other concerned SAs from participating, for instance, by failing to provide relevant information to the other SAs ([37]). In such cases, SAs may lack a thorough understanding of the case, which is crucial for meaningful participation in the process of consensus finding on the appropriate course of action ([38]). Secondly, several SAs may have difficulties – or may even be prevented – combining their duties stemming from national procedural laws with those under the cooperation mechanism. An illustrative example are the strict time limits for opening an investigation in one Member State applicable to the lead SA, which may have expired before other concerned SAs can comment on the need to open an investigation or the scope of it. ([39]) Where meaningful participation of both the lead and all concerned SAs in the enforcement procedure is not guaranteed, peer pressure avenues are not being employed to the best effect, which is detrimental to correct and consistent enforcement throughout the EU. Connected to this are the concerns expressed by multiple

([32]) As is the case for instance in Luxembourg where the SA is required '*to arrange the broadest possible participation of individuals in administrative decision-making*'. See the Luxembourgish Law on Administrative Procedures (*Loi de 1er décembre 1978, Réglant la procédure administrative non contentieuse*), Mém. A n° 87 of 27 December 1978, p. 2486, Article 1.

([33]) See, e.g., the Dutch Administrative Law Act (*Algemene wet bestuursrecht*), 4 June 1992, Stb. 1992, 315, Articles 4:11 and 4:12.

([34]) See Mustert, L., op. cit. (footnote 31).

([35]) Opinion of Advocate General Bobek of 13 January 2021, Facebook Ireland and others, C-645/19, ECLI:EU:C:2021:5.

([36]) Hofmann, H.C.H., and Mustert, L., Op-Ed: "Procedures Matter – What to Address in GDPR reform and a new GDPR Procedural Regulation", EU Law Live, 30 May 2023.

([37]) See Gentile, G., and Lynskey, O., 'Deficient by Design? The Transnational Enforcement of the GDPR', *International and Comparative Law Quarterly*, Vol. 71, No. 4, 2022, p. 800.

([38]) As is required by Article 60 GDPR.

([39]) See for example the strict time limits imposed to the Belgian SA in accordance with Article 96 of the Act Establishing the Belgian Data Protection Authority (*Wet betreffende de oprichting van een Gegevensbeschermingsautoriteit*), 3 December 2017, numac: 2017031916.

SAs regarding their lack of sufficient resources to effectively carry out their enforcement tasks ([40]), which also raises relevant questions regarding the financial independence of SAs ([41]).

The concerns expressed in this section do not only influence horizontal cooperation among the SAs, but also vertical cooperation with the EDPB when the latter exercises its dispute resolution or urgent decision-making powers. Especially because the EDPB has no competence to collect information or conduct investigations and is, therefore, highly dependent upon whether it receives a complete file for decision-making from the national SAs ([42]).

3. The way forward: solutions to under-enforcement of the GDPR

'*The desperate need for stronger enforcement*' ([43]), as recalled by the European Data Protection Supervisor, Wojciech Wiewiórowski, gave rise to the organization of the EDPS conference in 2022 on the future of data protection enforcement ([44]). This milestone in the ongoing discussion on how the promises of the GDPR can be better delivered, brought together key actors in the data protection community. Not only were structural limitations to the GDPR's enforcement model discussed, but also potential solutions to the identified problems. While the EDPS has been critical to the solution of increased harmonization of administrative procedural law, he appraised the solution of a pan-European data protection enforcement model to ensure a consistently high level of protection of the fundamental right to the protection of personal data across the EU ([45]). The following sub-sections reflect on both solutions, and discuss a third (middle-ground) solution of increased coordination of national enforcement action by an EU body in section 3.2.

([40]) See e.g., concerns expressed by the Dutch SA, Miljoenennota: Geen verhoging budget AP, September 2021 and EDPS speech, op. cit. (footnote 6).

([41]) Scholten, M., *The Political Accountability of EU and US Independent Regulatory Agencies*, Brill Nijhoff, Leiden, 2015.

([42]) See for a further discussion of the role of the EDPB section 3.2 and 3.3 of this chapter.

([43]) EDPS speech at the "Future of Data Protection: Effective Enforcement in the Digital World" conference, 16-17 June 2022, p. 2.

([44]) See the EDPS Conference Report 2022 – The future of data protection: effective enforcement in the digital world, issued on 10 November 2022.

([45]) See EDPS speech at the "Future of Data Protection: Effective Enforcement in the Digital World" conference, 16-17 June 2022, p. 5.

3.1. Procedural harmonization

Since many concerns regarding GDPR enforcement stem from the application of national procedural laws in the cross-border enforcement procedure, a possible solution to the GDPR's enforcement deficit is increased procedural harmonization ([46]). From a practical point of view, this constitutes an appealing solution because it does not require to re-open the GDPR ([47]). After a period of reflection on the appropriate response to the concerns expressed regarding GDPR enforcement, amongst others in the EDPB's 'wish-list' ([48]), the Commission published its Proposal for a Regulation laying down additional procedural rules relating to the enforcement of the GDPR in July 2023 ([49]).

The Commission Proposal focusses on harmonising procedural laws particularly with regard to the treatment of complaints, the cooperation and dispute resolution procedures, procedural rights of parties under investigation and, to a certain extent, of complainants. Concretely, this means that the Commission's proposal aims, *inter alia,* to remove the fragmented approaches to the concept of a complaint by providing a common complaint form ([50]), and that the right to be heard and the right to access the administrative file are being harmonized for the parties under investigation ([51]). Complainants are purposively treated different than parties under investigation in the Proposal and, therefore, complainants enjoy significantly less procedural rights – e.g., they do not have generalised access to the file, while data controllers and processors would enjoy such right ([52]). With regard to streamlining cooperation, the Commission proposal requires from the lead SA to actively engage concerned SAs by regularly updating these authorities about the investigation at the earliest convenience with all relevant information available ([53]), and, more specifically, by sharing the preliminary views of the main issues in the investigation ([54]). Such information exchanges aim to increase the chances of SAs to meaningfully impact the course of the enforcement procedure.

([46]) Brito Bastos, F., and Pałka, P., 'Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?' *European Constitutional Law Review*, Vol. 19, 2023, p. 504.

([47]) *Ibid*, p. 504.

([48]) EDPB Letter to the EU Commission on Procedural Aspects, adopted on 10 October 2022.

([49]) COM(2023) 348 final.

([50]) *Ibid*, Recital 4 and Article 3(1).

([51]) *Ibid*, Recitals 22 to 23 and Articles 14(2)(5), 17 and 20(1).

([52]) *Ibid*, Recital 26 and Article 15. See also EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, adopted on 19 September 2023, paragraph 78.

([53]) COM(2023) 348 final, Article 8(1).

([54]) *Ibid*, Article 9(1).

While the Commission's initiative seems a welcome development at first sight – and it certainly addresses important aspects in need of clarification – the proposed Regulation may not substantially improve cross-border enforcement of the GDPR for three reasons. First, while the Proposal entails detailed rules on particular steps in the enforcement procedure, legal concepts such as 'draft decision', 'resolved cases', or 'interested parties' are only occasionally defined in the Proposal and will often require a national interpretation ([55]). Secondly, many concerns regarding the GDPR's cross-border enforcement procedure and procedural protection of individuals remain unaddressed, meaning that the Proposal falls short of remedying fundamental deficits in the GDPR's enforcement model ([56]). Lastly, particular aspects of the Commission's proposal seem to worsen some of the shortcomings in enforcement that it aims to improve – i.e., the outsized role of the lead SA is not mitigated but instead entrenched ([57]). In 2022, the EDPS already emphasized that the harmonisation of administrative procedural laws will only have an added value if it covers a broad range of aspects ([58]). Limited harmonisation – as now proposed by the Commission – will not radically improve the functioning of the cross-border GDPR's enforcement procedure, as it will not overcome all the structural differences. In the words of the EDPS '*harmonisation might help, but it is by no means a silver bullet*' ([59]).

3.2. The EDPB as stronger network coordinator

It is often argued that concentrating authority in a central body in enforcement networks will reduce the administrative complexity, and thereby, enhance the speed and efficiency of enforcement procedures ([60]). In that regard, especially large networks – such as the GDPR's enforcement network – benefit from a centralized form of governance ([61]). Hence, already during the preparation of the Commission's GDPR proposal, the need for a centralized node in the enforcement network was considered essential. While the proposal to set up

([55]) Brito Bastos, F., and Pałka, P., op. cit. (footnote 46), p. 506.

([56]) E.g., regarding admissibility criteria of complaints, guaranteeing a meaningful role for concerned DPAs in enforcement, and establishing further legal deadlines in the enforcement procedure. See for relevant examples also EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, adopted on 19 September 2023.

([57]) Particularly because the concerned SAs' relevant and reasoned objections to draft decisions prepared by the lead SA are significantly more restricted in their scope in comparison to how they are framed in the GDPR. See COM(2023) 348 final, Article 18.

([58]) EDPS speech at the "Future of Data Protection: Effective Enforcement in the Digital World" conference, 16-17 June 2022, p. 5.

([59]) *Ibid*, p. 5.

([60]) Van Kreij, L., 'Towards a comprehensive framework for understanding EU enforcement regimes', *European Journal of Risk Regulation*, Vol. 10, 2019, p. 447.

([61]) Provan, K.G., and Lemaire, R.H., 'Core Concepts and Key Ideas for Understanding Public Sector Organizational Networks: Using Research to Inform Scholarship and Practice', *Public Administration Review*, Vol. 72, No. 5, 2012, p. 640 and 643.

an EU Data Protection *Agency* was dismissed ([62]), the European Data Protection *Board* was established as an independent 'body of the Union' with legal personality, composed of the head of one SA of each Member State and the EDPS ([63]). The EDPB is supported by its secretariat, provided by the EDPS ([64]). While the EDPB's role is crucial for coordinating complex decentralized enforcement procedures, for which it has a broad legal basis in the GDPR, its role turns out to be limited in practice.

First, the Board's coordinating competences do not reach as far compared to other agencies with a supportive role in enforcement. Agencies such as Eurojust or the European Fisheries Control Agency, for example, do not merely have a task in promoting common training programmes and facilitating personnel exchanges, but instead concretely support and coordinate national investigations in which these agencies' officials may even participate ([65]). Such role for the EDPB in steering and/or participating in national investigations does not exist. Secondly, the EDPB's guidance documents – i.e., guidelines, recommendations and best practices – in which the EDPB can clarify both substantive and procedural aspects of the GDPR, do not fill the gap that the lack of procedural harmonization in the GDPR creates. Although the Board's guidance lacks inherent legally binding force ([66]), the guidance documents could nevertheless have established more concrete legal effects – e.g., meaning that the documents are generally perceived as binding and, therefore, lead to changes in the behaviour of its addressees ([67]). While it exceeds the scope of this chapter to discuss the reasons for this uncertainty regarding the legal effects of EDPB guidance in detail, it should be noted that the GDPR is completely silent on the effects that guidance documents aim to produce. One way to increase the potential legal effects of EDPB documents could be to establish a so-called 'comply or explain' mechanism ([68]). Such a mechanism indicates that compliance with guidance of an EU authority is expected, unless there are good reasons not to do so.

([62]) EU Commission, Commission Staff Working Paper: Impact Assessment – Accompanying the document […] General Data Protection Regulation […]', SEC(2012) 72 final, p. 72 and 81.

([63]) Article 68(3) GDPR.

([64]) Article 75 GDPR.

([65]) Scholten, M., op. cit. (footnote 41), p. 51.

([66]) It follows from the EU Treaties that only the instruments that have as such been attributed legally binding force can have *general and inherent legally binding force*, which are Directives, Regulations or Decisions as laid down in Article 288 of the Treaty on the Functioning of the EU. See further Senden, L., *Soft law in EU Community law*, Hart Publishing, Oxford, 2004, p. 246.

([67]) Petropoulou Ionescu, D. and Eliantonio, M., 'Words are Stones: Constructing Bindingness through Language in EU Environmental Soft Law', *The Legal Effects of Soft Law: Theory, Language and Sectoral Insights into EU Multi-Level Governance,* Edward Elgar, Cheltenham, 2023. See for a comprehensive analysis of the legal effects of the EDPB's guidance Mustert, L., op. cit. (footnote 31).

([68]) Van Rijsbergen, M., *Legitimacy and Effectiveness of ESMA's Soft Law*, Edward Elgar, Cheltenham, 2021.

Lastly, the EDPB is empowered to adopt legally binding decisions under the dispute resolution mechanism or the urgency procedure on an exceptionally broad range of topics, meaning that it can, in theory, push for advancement in individual cases. Hence, the EDPB could function as a backstop where decentralized enforcement risks paralysis. However, the effects of this competence are limited due to several reasons. First, the EDPB is highly dependent upon the loyal cooperation of the SAs. Hence, it is up to the SAs to refer a matter to the EDPB and the SAs shall determine the scope of the matter brought to the EDPB for decision-making. Furthermore, the EDPB holds no powers to collect information by itself and is, therefore, dependent upon the SAs for the referral of a *complete* file required for decision-making. However, in all disputes brought before the EDPB so far, the Board was incapable to decide on all aspects brought before it due to insufficient information in the file ([69]). Such decisional interdependence of EU agencies is not unique ([70]), however, most EU agencies with decision-making powers can somehow interfere when national authorities fail to sincerely cooperate. The European Security and Markets Authority (ESMA), for example, can initiate its dispute resolution competence by itself where a disagreement among national supervisory authorities is *presumed* – amongst others, if a joint decision is not being taken within the time limits as set out in the Regulation ([71]). Additionally, ESMA may directly address an information request to the financial market participant where the national supervisory authority does not provide the required information for dispute resolution ([72]) and is, therefore, less dependent upon the sincere cooperation of national supervisory authorities compared to the EDPB. Granting the EDPB similar powers would be a response to many problems its dispute and urgency procedures currently face. A last concern relates to the fact that the Board's binding decisions addressed to the SAs often leave broad discretion to the SAs when implementing the EDPB's decision addressed to the data controller, processor or complainant ([73]). Hence, national interests are not per se flattened out where the EDPB interferes by exercising its binding decision-making powers. Combined with the lack of control over the actual (correct) implementation of the EDPB's decision, the effects of dispute resolution or urgent decision-making remain uncertain. In this regard, inspiration for improvement can be found in the area of banking supervision where the Single Resolution Board (SRB) can directly enforce its decisions upon financial institutions, insofar the national authorities did not comply with the SRB's decision in their implementing decision ([74]).

([69]) See for an analysis e.g., Mustert, L., 'The EDPB's Second Article 65 Decision – Is the Board Stepping up its Game?', *European Data Protection Law Review*, Vol. 7, No. 3, 2021.

([70]) Majone, G., 'The credibility crisis of community regulation', *Journal of Common Market studies*, Vol. 38, No. 1, 2000.

([71]) Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), OJ L 331, 24.11.2010, p. 84, Article 19(1).

([72]) *Ibid*, Article 35(6).

([73]) Article 65(6) GDPR.

([74]) See Timmermans, J., and Chamon, M., 'Controlling the SRB's resolution powers', in *Controlling EU Agencies: The Rule of Law in a Multi-jurisdictional Legal Order*, Edward Elgar, Cheltenham, 2020, p. 301.

While the role of the EDPB is crucial in coordinating a large enforcement network as established under the GDPR, the Board's current role is rather limited compared to other EU agencies pursuing similar aims. Problems mainly stem from deficiencies in the design of the GDPR and the lack of detailed procedures applicable to the EDPB. In order to improve the position of the EDPB as a stronger network coordinator, inspiration can be found in the design of tasks and powers of many other EU agencies as briefly discussed above. In this regard, it is important to note that changes regarding the position of the EDPB as network coordinator as discussed in this section, would not require the reopening of the GDPR, as such changes would add to the existing legal framework without amending it.

3.3. A dual-approach: direct enforcement by an EU authority

In the above section two solutions to the GDPR's enforcement deficits were explored. While harmonisation might help only to a certain extent, increasing the role of the EDPB as network coordinator may have its downsides too – as it would, for example, not per se make the enforcement system and information puzzle less complex. Therefore, it is worth exploring a pan-European approach where direct enforcement powers are exercised by an EU agency or body, as has been considered as a valuable solution by the EDPS ([75]). Such an approach is particularly preferred where a relatively small and/or homogenous group of actors operates across the EU, whose violations require a single solution ([76]). Placing this group of actors under direct control of an EU agency or body mitigates the problems of combining procedural laws and strategies of too many SAs in one procedure, and it flattens out national interests ([77]). Since the GDPR aims to regulate a very diverse market including both small and very large data controllers and processors, a dual-approach is preferred where only the large, systemic or serious cases are transferred to the EU level. This small group of very large data controllers and/or processors would then be subject to direct control by an EU agency or body – e.g., the EDPB. Such a dual-approach is already established in other areas of law which contain a diverse market of small and large participants. Hence, centralized supervision and enforcement exists, for example, for large banks ([78]), large online platforms ([79]), or aircraft types instead of individual aircrafts ([80]).

([75]) EDPS speech at the "Future of Data Protection: Effective Enforcement in the Digital World" conference, 16-17 June 2022, p. 5.

([76]) Van Kreij, L., op. cit. (footnote 60), p. 447.

([77]) Karagianni, A.M., op. cit. (footnote 2), p. 24.

([78]) Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions, OJ L 287, 29.10.2013, p. 63, Article 6(4).

([79]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act),OJ L 277, 27.10.2022, p. 1, Article 56(2)(3).

([80]) Regulation (EU) 2018/1193 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 , OJ L 212, 22.08.2018, p. 1, Article 77(1).

4. Concluding remarks

The first years of experience with the GDPR have shown serious deficiencies in the system of enforcement, resulting *inter alia* from the highly integrated but overly complex administrative procedures regulating enforcement. While the Commission now aims to address these concerns by means of procedural harmonization, research has shown that the harmonisation of administrative procedural laws will only have an added value if it covers a broad range of aspects. Limited harmonisation will not radically improve the functioning of the cross-border GDPR's enforcement procedure, as it will not overcome all the structural differences. Therefore, this chapter rethought the design of the enforcement model and the role of a centralized node in the GDPR's networked enforcement structure. While an increased role for the EDPB as strong network coordinator could certainly prove beneficial, and inspiration for such a role was found in the design of tasks and powers of other EU agencies, the need for a dual-approach was also explored. While the latter solution would require the re-opening of the GDPR, this should not be a taboo. Instead, as the EDPS rightly stated, '*closer integration is needed if we are serious about protecting EU citizens' personal data across the EU*' ([81]).

([81]) EDPS speech at the "Future of Data Protection: Effective Enforcement in the Digital World" conference, 16-17 June 2022, p. 6.

19

Data protection at the Court of Justice of the EU

Christopher Docksey

Data protection at the Court of Justice of the EU

Christopher Docksey (*)

This chapter considers some of the most significant trends in the case law of the Court of Justice of the EU, following the entry into force of the EU Charter. In a series of landmark cases, the Court has underpinned the architecture and governance of European data protection law and its relationship with national law, and balanced the fundamental rights of privacy and data protection with other fundamental rights. It has developed an accountability approach, which ensures that those processing personal data may be held responsible for such processing, by following a broad approach to the material scope of the data protection legislation and a strict approach to the exceptions thereto.

1. Introduction

This chapter discusses some of the most significant trends in the case law of the Court of Justice of the European Union ('CJEU') based on a number of landmark cases, each at the centre of a constellation of rulings and pending cases around the same issue. National supervisory authorities and the EDPS ('DPAs') have played an important role in many of these cases, as a party or intervenor.

1.1. The Lisbon Treaty and the EU Charter

The entry into force of the Lisbon Treaty in December 2009 had two key implications for EU data protection law.

First, it gave treaty status to the Charter of Fundamental Rights of the European Union ('Charter'), which provided the Court with a firm legal basis for a vigorous interpretation and application of fundamental rights to EU and national law and international treaties ([1]).

(*) Honorary Director General, EDPS.

([1]) See Iglesias Sánchez, S., 'The Court and the Charter: the impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights', CML Rev, Vol. 49, 1565, p. 1569-1573.

Second, Lisbon provided a specific legal basis for data protection legislation, Article 16(2) of the Treaty on the Functioning of the European Union ('TFEU'), which put an end to the discussion of the scope and implications of the internal market legal base ([2]) used for the Data Protection Directive ('DPD') ([3]).

Following Lisbon, the Court has handed down a number of seminal rulings, dating from *Google Spain* in 2014 to *Meta Platforms* and *CRIF* in 2023. This chapter will discuss the main points of these rulings together with their associated cases, save for those on data retention and international transfers, which are discussed in other chapters in this book.

Many of these landmark cases preceded the GDPR, which was adopted in 2016 under the new Lisbon legal basis and entered into application in 2018. Since then it has underpinned the growth of the case law over the current third decade of data protection law in which we find ourselves today. The new legislative framework has been described as a 'tipping point' for a 'new and more effective era of data protection' ([4]), which has undergone a qualitative change, and is now established as a policy field in its own right ([5]).

1.2. The massive growth of data protection case law

Since the adoption of the GDPR, litigation at national level has increased, resulting in a commensurate number of references for preliminary rulings. Over the first decade of the century there was barely one CJEU ruling a year, constituting only about 10% of the present total of rulings. In the second decade there were about five cases a year, amounting to about 47% of the total. In the present decade, over the first four years, 2020-2023, the tempo has risen to an average of some 12 rulings a year ([6]), amounting to some 43% of the total ([7]). The tempo is likely to increase, together with the number of direct actions before the General Court.

This significant growth of the case law at national level underlines the need for a common interpretation by the CJEU.

([2]) See most recently the judgment of the Court of Justice of 9 July 2020, *Land Hessen*, C-272/19, EU:C:2020:535, paragraph 66.

([3]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.1.1995, p. 31.

([4]) Docksey, C., and Hijmans, H., 'The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law', EDPL, Vol. 5, No. 3, 2019, p. 300 at p. 316. This chapter, by one of the authors, takes up some of the same themes.

([5]) Opinion of Advocate General Szpunar of 17 December 2020, *Latvijas Republikas Saeima (*Penalty points*)*, C-439/19, ECLI:EU:C:2020:1054, point 52.

([6]) Rising to over 20 rulings in 2023.

([7]) Rough calculations by the author using the Court's search form. The vast majority of these rulings were preliminary rulings. In addition there were two Advisory Opinions by the EFTA Court in 2020.

2. The architecture and governance of the GDPR

Many of the powerful novelties in the GDPR are about architecture and governance – the consistency mechanism and one-stop-shop, the powers of the EDPB, the enforcement powers of DPAs, and the representation of data subjects. This new institutional framework is giving rise to its own questions before the Court.

2.1. Consistency and cooperation: the one-stop shop and the growth of litigation

The general rule for the jurisdiction of supervisory authorities is laid down in Article 55, which provides that *'each supervisory authority shall be competent …on the territory of its own Member State'* ([8]).

This rule does not apply, however, where a controller processes personal data in more than one EEA Member State, in which case the 'one-stop-shop' rule under Article 56 GDPR applies to supervision of cross-border processing. The DPA of the main establishment of the cross-border controller becomes the 'lead supervisory authority' ('LSA') and assumes competence as *primus inter pares* ([9]) for any complaints against that controller, regardless of the jurisdiction in which a complaint is made. The application of the one-stop-shop triggers the Consistency Mechanism under Article 60 GDPR whereby the LSA is required to cooperate with any other supervisory authority concerned ('CSA') and any persistent divergences of views are resolved by the European Data Protection Board ('EDPB') in the dispute resolution procedure under Article 65 GDPR.

These provisions were first tested in the *Facebook Ireland* ([10]) case, which concerned an investigation against Facebook Belgium by the Belgian DPA. This commenced under the DPD but was still pending when the GDPR came into application in 2018, at which point the Data Protection Commissioner of Ireland ('DPC') became the LSA. The CJEU was asked in essence whether the LSA had sole competence to go to court, or, more specifically, whether the local DPA should at least be able to continue with a case that it had started before the GDPR entered into application.

([8]) See judgment of the Court of Justice of 16 January 2022, *Österreichische Datenschutzbehörde*, C-33/22, ECLI:EU:C:2024:46, paragraphs 61 to 63.

([9]) Opinion of Advocate General Bobek of 13 January 2021, *Facebook Ireland and others*, C-645/19, ECLI:EU:C:2021:5, point 111. See Hijmans, H., 'Article 56', in Kuner, C., Bygrave, L.A., and Docksey, C. (eds.), *The EU General Data Protection Regulation: A Commentary*, Oxford University Press, Oxford, 2020, p. 917-918.

([10]) Judgment of the Court of Justice of 15 June 2021, *Facebook Ireland and others*, C-645/19, ECLI:EU:C:2021:483.

The Court held that a local DPA may continue to bring a case only up to the date that the DPD was repealed by the GDPR, that is, 25 May 2018 ([11]). Thereafter the one-stop-shop rule under Article 56(1) GDPR confers competence on the LSA ([12]), in effect a *lex specialis* ([13]). However the Court stressed that Article 56(1) requires '*close, sincere and effective cooperation*' between the DPAs concerned and that the LSA '*cannot eschew essential dialogue with and sincere and effective cooperation with the other supervisory authorities concerned*' ([14]). The Advocate General emphasised the need to ensure consistency and prevent the risk of fragmentation under the DPD whereby various DPAs take different approaches with regard to cross-border processing ([15]).

This was a difficult case for the Court, as witness strong doubts expressed at the hearing ([16]), and it is clear that it finally decided to give the consistency mechanism a chance to work. Advocate General Bobek pointed out that the mechanism is 'still in its infancy' ([17]) and should be given the 'benefit of doubt' for the time being. However, he added that the Court would not 'turn a blind eye' to any gap in effective protection by regulators which might emerge ([18]).

The ability to challenge the dispute resolution procedure under Article 65 GDPR was considered in *WhatsApp Ireland* ([19]). Following 'relevant and reasoned' objections by CSAs, the EDPB decided that the DPC acting as LSA should increase its proposed fine from €30-€50m to €225m. WhatsApp Ireland challenged the Board's decision before the General Court, which dismissed it as inadmissible. Applying settled law, the General Court found that the decision of the Board addressed to the DPC was not of individual or direct concern to the company concerned. It was solely addressed to the DPC, the body which would adopt the final decision, which could be challenged before its national courts. The ruling has been appealed to the CJEU ([20]), but it is likely that the General Court's ruling will be upheld. It avoids parallel proceedings before the European and national courts, and a national court may send a reference to the CJEU.

([11]) *Ibid*, paragraph 104.

([12]) *Ibid*, paragraph 50.

([13]) Opinion of Advocate General Bobek in *Facebook Ireland and others*, see footnote 9, point 59, affirming the EDPB Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment, adopted on 9 July 2019, paragraph 20. It is '*not … an exclusive competence, but … a structured way of cooperating with other locally competent supervisory authorities*.' Hustinx, P., 'EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation', in Cremona, M. (ed.), *New Technologies and EU Law*, Oxford University Press, Oxford, 2017, p. 123.

([14]) *Facebook Ireland and others*, see footnote 10, paragraph 63. See also judgment of the Court of Justice of 24 September 2019, *Google (*Territorial scope of de-referencing*)*, C-507/17, ECLI:EU:C:2019:772, paragraph 68: '*the various national supervisory authorities concerned must cooperate… in order to reach a consensus*'.

([15]) Opinion of Advocate General Bobek in *Facebook Ireland and others,* see footnote 9, points 76-80. See also the Opinion of Advocate General Saugmandsgaard Øe of 19 December 2019, in *Facebook Ireland and Schrems,* C-311/18, ECLI:EU:C:2019:1145, point 155, pointing out the inherent risk of fragmentation under the previous DPD.

([16]) Manancourt, V., Top EU court judges clash with Commission over GDPR enforcement model, *Politico Pro*, 6 October 2020.

([17]) Opinion of Advocate General Bobek in *Facebook Ireland and others,* see footnote 9, point 125.

([18]) *Ibid*.

([19]) Order of the General Court of 7 December 2022, *WhatsApp Ireland v EDPB*, T-709/21, ECLI:EU:T:2022:783.

([20]) Pending Case *WhatsApp Ireland v EDPB*, C-97/23 P.

The second challenge was lodged in *DPC v EDPB*. The Board decided that the DPC should carry out an additional investigation into WhatsApp's processing operations in order to determine matters omitted from the original investigation (such as special categories of personal data and data for the purposes of behavioural advertising), and to issue a new draft decision ([21]). The DPC has requested the General Court to annul the relevant paragraphs of the Board's decision on the grounds that the EDPB has exceeded its competence under Article 65(1)(a) GDPR in purporting to instruct it to carry out a new investigation, and issue a new draft decision ([22]). However the DPC has previously argued that it is unacceptable to open the scope of an existing inquiry, lest it jeopardise '*the entirety of the inquiry*' on the grounds of 'procedural unfairness' ([23]). If neither enlarging the original investigation nor ordering a fresh investigation are possible, this would leave a gap in protection of data subjects, and it is hoped that the prediction by Advocate General Bobek that the EU courts will not turn a 'blind eye' is correct.

In the meantime the Board wrote to the Commission with a 'wishlist' of procedural law changes to improve the functioning of the system, for example by setting deadlines for different procedural steps in the handling of a one-stop-shop case ([24]). In response, the Commission has proposed a regulation to set clear procedural rules for LSAs and CSAs dealing with cross-border investigations ([25]). At least three of its provisions demonstrate the failure by DPAs to respect the Court's mandate to cooperate in *Facebook Ireland* ([26]).

2.2. Enforcement by independent data protection authorities

A pending case brought by the EDPS illustrates the significance of the enforcement powers conferred on supervisory authorities by EU law and the case law of the court on DPA independence.

First, Chapter VI of the GDPR has afforded specific tasks and duties to DPAs, in contrast to the illustrative list in Article 28 DPD. In addition, Article 83 GDPR

([21]) EDPB Binding Decision 5/2022 on the dispute submitted by the Irish SA pursuant to Article 65 GDPR on WhatsApp Ireland Limited, adopted on 5 December 2022, paragraph 326. See also paragraph 222.

([22]) Case *Data Protection Commission v EDPB*, T-111/23, lodged 24 February 2023.

([23]) EDPB Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR, adopted on 9 November 2020, paragraph 64.

([24]) Letter of 12 October 2022 from Andrea Jelinek, President of the EDPB, to Commissioner Didier Reynders suggesting a number of procedural law changes to improve enforcement, including deadlines to start an investigation, to communicate the information on the case to CSAs and to issue a draft decision, p. 5.

([25]) Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM(2023) 348 final. See also further the contribution by Mustert, L., 'The Future of Effective Data Protection Enforcement', Chapter 18.

([26]) Article 8 COM(2023) 348 final requires the LSA to regularly update the other CSAs about an investigation and provide them, *at the earliest convenience*, with all relevant information once available. Article 9 requires the LSA, once it has formed a *preliminary view on the main issues*, to send a *summary of key issues* the CSAs, identifying the main elements of the investigation and its views on the case, thus allowing CSAs to provide their views early on. Finally Article 10(3) requires the LSA to engage with CSAs on basis of their comments in an endeavour to *reach a consensus*.

provides for competition-law style fines. These provisions are mirrored in the EUDPR ([27]), which applies to the EU institutions, bodies and agencies and establishes the EDPS as their DPA.

Whilst fines are possibly the headline innovation of the GDPR, they are not necessarily the most effective means of imposing compliance, which may be better achieved in some cases by the use of corrective powers ([28]) such as ordering the controller or processor to bring processing operations into compliance or suspension, imposing a temporary or definitive ban on processing, or ordering the rectification or erasure of personal data ([29]).

Second, the CJEU has developed a consistent and demanding standard for the independence of DPAs, higher than that for regulators on other areas ([30]) and similar to that applied to the judiciary ([31]). Independence is grounded on the fundamental principle of independent supervision enshrined, exceptionally, in both Article 8(3) of the Charter and Article 16(2) TFEU. The Court has stressed that the high level of independence of DPAs is not a *right* enjoyed by DPAs but rather a *means* to ensure that they can support individuals most effectively ([32]).

In *Commission v Germany* ([33]), the Court held that DPAs must be free from any external influence, direct or indirect, not only from supervised bodies but also from government itself, referring to the status of *Land* authorities which were independent of the companies they supervised but formed part of the organisation of State government. As the EDPS pointed out in its intervention, government authorities have their own financial, economic and political strategies and priorities, quite different to ensuring compliance, and the regulator should not be subject to any such influence ([34]).

The Court further developed its approach in *Commission v Austria* ([35]), where it held that DPAs must remain above all *suspicion* of partiality and that their organisation should not permit any pressure for *prior compliance*. The EDPS

([27]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

([28]) See Lintvedt, M.N., 'Putting a price on data protection infringement', *IDPL*, Vol. 12, No. 1, 2022, p. 11.

([29]) Article 58(2)(d), (f) and (g) GDPR and Article 58(2)(e), (g) and (h) EUDPR.

([30]) Judgment of the Court of Justice of 19 October 2016, *Ormaetxea Garai and Lorenzo Almendros*, C-424/15, ECLI:EU:C:2016:780.

([31]) See judgment of the Court of Justice of 24 March 2022, *Autoriteit Persoonsgegevens*, C-245/20, ECLI:EU:C:2022:216. See also the criticism by Balthasar, A., 'Complete Independence of National Data Protection Supervisory Authorities', *Utrecht Law Review*, Vol. 9, No. 3, 2013, p. 31.

([32]) Judgment of the Court of Justice of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 25.

([33]) *Commission v Germany,* see footnote 32. This case preceded Lisbon and was based on the notion of 'complete independence' in Article 28(1) DPD, now Article 52(1) GDPR and Article 55(1) EUDPR.

([34]) EDPS pleading at the hearing of the Court in Case C-518/07 (Commission v Germany), 26 November 2008, paragraph 59.

([35]) Judgment of the Court of Justice of 16 October 2012, *Commission v Austria*, C-614/10, ECLI:EU:C:2012:631.

had noted that the Commissioner and staff of the Austrian DPA were career officials in the Chancellor's Office, and thus open to influence from within the government ([36]).

Finally, the Court has laid down in *Commission v Hungary* ([37]) that data protection commissioners cannot be replaced before the end of their mandate outside the procedures laid down, even if the dismissal is by way of legislation with the status of a Fundamental Law. The EDPS intervened to warn that the arbitrary termination of a mandate may have a 'chilling effect on the activities of any subsequent heads of the supervisory authority' ([38]) and Advocate General Wathelet characterised the 'paralysing risk' that a Commissioner's term in office might be prematurely terminated as a 'sword of Damocles' ([39]).

There was a similar problem of lack of independence in the area of international transfers in Opinion 1/15 (*EU-Canada PNR*). The CJEU found that the 'impartial' administrative body integrated within the executive in Canada which was responsible for supervising processing of EU citizens' PNR data was not fully independent within the meaning of Article 8(3) of the Charter ([40]). The EDPS had intervened to advise that the administrative body was only an 'internal review mechanism' which could at best be compared with the function of the internal Data Protection Officer ([41]), and Advocate General Mengozzi had added that the administrative body continued to be '*under the direction of the responsible Minister*' and '*subject to any direction given by the Minister*' ([42]).

The ruling of the General Court in *EDPS v Parliament and Council* has to be seen in light of the above ([43]). In 2020, the EDPS found that there had been infringements of the initial Europol Regulation, since large volumes of data concerning individuals with no established link to a criminal activity had been continuously stored by Europol. The EDPS admonished Europol for the continued storage of such data, posing a risk to individuals' fundamental rights, in particular with regard to failing to comply with the principles of data minimisation and data retention. In January 2022, the EDPS adopted a decision ordering Europol to delete data concerning individuals with no established link to a criminal activity according to a certain timetable, with the aim that Europol would no longer retain data about people who have not been linked to a crime or a criminal activity for long periods with no set deadline.

([36]) EDPS pleading at the hearing of the Court in case C-614/10 (Commission v Austria), 25 April 2012.

([37]) Judgment of the Court of Justice of 8 April 2014, *Commission v Hungary*, C-288/12, ECLI:EU:C:2014:237.

([38]) EDPS pleading at the hearing of the Court in Case C-288/12 (Commission v Hungary), 15 October 2013.

([39]) Opinion of Advocate General Wathelet of 10 December 2013, *Commission v Hungary,* C-288/12, ECLI:EU:C:2013:816), point 83.

([40]) Opinion of the Court of Justice of 26 July 2017, *EU-Canada PNR Agreement*, C-1/15 Opinion, ECLI:EU:C:2017:592, points 230-231.

([41]) EDPS pleading at the hearing of the Court in C-1/15 Opinion (EU-Canada PNR Agreement), 5 April 2016.

([42]) Opinion of Advocate General Mengozzi of 8 September 2016, *EU-Canada PNR Agreement,* ECLI:EU:C:2016:656, point 315 and fn 118.

([43]) Order of the General Court of 6 September 2023, *EDPS v Parliament and Council*, T-578/22, ECLI:EU:T:2023:522.

In June 2022, the European Parliament and the Council amended the Europol regulation, inserting two transitional provisions ([44]) at the last moment in the trilogue which, according to the EDPS, retroactively legalised Europol's contested data retention practices and de facto annulled the decision of 3 January 2022. The EDPS took the view that the transitional provisions infringed his enforcement powers under Article 55 EUDPR and his independence under Article 8(3) of the Charter, read in conjunction with Article 43(1) and (3)(e) of the amended Europol regulation ([45]), and lodged an application for annulment of those transitional provisions.

However the EDPS was faced with the standard hurdle of proving standing to bring an action for annulment under Article 263 TFEU. This requires an applicant to be a privileged applicant (an EU institution under Article 13(1) TEU) or to be directly and individually concerned by those provisions. The General Court found that the EDPS did not meet the requirements of Article 263 TFEU and rejected the action as inadmissible. First, the Court found that the EDPS did not have privileged standing before the EU Courts in order to seek the annulment of an EU act, since the transitional provisions did not affect the EDPS' prerogatives so as to affect the institutional balance ([46]). Second, the Court found that the EDPS was not directly concerned since those provisions did not change the way in which he can lawfully exercise his powers, nor did they automatically override the EDPS' decision but instead conferred a discretion on Europol to decide when it is necessary to process the data in question. The Court dismissed the argument that the mere fact of conferring a discretion directly undermines the EDPS' decision, which was definitive and contained no such discretion.

At the heart of the ruling were two issues: that the transitional provisions do not directly affect the EDPS' legal situation, and that '*the independence in which the EDPS must carry out his duties in practice is not intended to limit the powers of the EU legislature*' ([47]). The order has been appealed in Case C-698/23 P. It remains to be seen whether these findings with regard to the EU DPA will be affirmed by the CJEU in the light of its powerful case law on the independence of supervisory authorities.

([44]) Articles 74(a) and 74(b) of Regulation (EU) 2016/794.

([45]) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968, OJ L 135, 24.5.2016, p. 53, as amended by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, OJ L 169, 27.6.2022, p. 1.

([46]) In the sense of the judgment of the Court of Justice of 22 May 1990, *Parliament v Council*, C-70/88, EU:C:1990:217.

([47]) *EDPS v Parliament and Council*, see footnote 43, paragraph 48.

2.3. Enforcement by bodies acting under consumer protection and competition law

In 2014, the EDPS adopted a path-breaking opinion which recognised the common goals of EU policies on data protection, competition and consumer protection and called for a closer dialogue between regulators across these policy boundaries in order to aid enforcement of the rules ([48]). The opinion 'kick-started' the discussion of the interplay between these policies ([49]), which has been developed in a number of recent rulings.

First, the Court has considered the right to collective representation under Article 80 GDPR of the rights under Articles 77 to 79 GDPR to complain to a DPA, to complain against a DPA, and to seek a judicial remedy. Article 80(1) directly empowers data subjects to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of data protection to lodge complaints on their behalf and exercise the rights referred to in Articles 77 to 79 on their behalf. Article 80(2) goes further, and permits Member States to provide standing for such a representative body in the absence of a specific mandate from an individual.

In *Fashion ID* ([50]), it was argued that the DPD then in force did not specifically provide for standing of such associations, and indeed precluded such representation until the advent of Article 80(2) GDPR. The Court recalled that one of the 'underlying objectives' of the data protection legislation is '*to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy*' ([51]), and held that the fact that Article 80(2) GDPR expressly authorises Member States to allow associations to bring representative proceedings does not mean that Member States could not grant them that right under the DPD, but '*confirms, rather, that the interpretation of that directive in the present judgment reflects the will of the EU legislature*' ([52]).

Notwithstanding these dicta, Article 80(2) was the main item in *Meta v Verbraucherzentrale Bundesverband* ([53]). The German federal consumer association sought an injunction against Meta concerning a section on Facebook that allows users to access free games provided by third parties, claiming that the information provided was unfair. The association was on the

([48]) EDPS Preliminary Opinion on Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, issued in March 2014. See also further the contribution by D' Cunha, C. and Colaps, A., 'A clear imbalance between the data subject and the controller': Data protection and competition law', Chapter 15.

([49]) Lynskey, O., 'At the crossroads of data protection and competition law: time to take stock', *IDPL*, Vol. 8, No. 3, 2018, p. 179.

([50]) Judgment of the Court of Justice of 29 July 2019, *Fashion ID,* C-40/17, ECLI:EU:C:2019:629.

([51]) *Ibid*, paragraph 50.

([52]) *Ibid*, paragraph 62.

([53]) Judgment of the Court of Justice of 28 April 2022, *Meta Platforms Ireland*, C-319/20, ECLI:EU:C:2022:322.

list of entities under German law with standing to bring consumer cases without a specific mandate and German consumer law already allowed consumer associations to take legal action against an alleged infringer of data protection law. However the defendant challenged whether such prior legislation with regard to consumer protection was consistent with Article 80(2) GDPR.

The Court ruled that Article 80(2) is an *opening clause*: consumer associations may bring actions for violation of the data protection rules, so long as they have standing under national law, their objective is to ensure observance of GDPR rights, and such standing does not undermine its content and objectives. The Court underlined that the defence of collective interests of consumers by consumer associations undoubtedly contributes to ensuring a high level of protection ([54]). Advocate General Richard de la Tour pointed out the '*complementarity and convergence of the law relating to the protection of personal data with other areas of law, such as consumer law and competition law*'… and concluded that the '*effective application of the [GDPR] cannot but be strengthened as a result*' ([55]). Finally, the Court noted that the right under Article 80(2) is not subject to the existence of a specific infringement, it is sufficient that the entity concerned 'considers' that the rights of a data subject laid down in that regulation have been infringed as a result of the processing of their personal data ([56]).

A third case, *Meta Platforms v Bundeskartellamt* ('BKA') ([57]) affirmed the complementarity of enforcement in the competition field. Access to Facebook was conditional on consent to Meta's data and cookies policies, which provided for the 'central element' ([58]) of pooling by Meta of the personal data harvested by Meta's various apps for profiling and advertising. The BKA, the German national competition authority, found that Facebook's data processing terms did not comply with the GDPR and constituted an abuse of Meta's dominant position on the German social network market for private users. It prohibited

([54]) *Ibid*, paragraph 74, see also paragraphs 80 to 81 where the Court noted that its interpretation is supported by the fact that Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, OJ L 409, 4.12.2020, p. 1, specifically refers to the GDPR in recitals 13 and 15 and Annex I paragraph 56.

([55]) Opinion of Advocate General Richard de la Tour of 2 December 2021, *Meta Platforms Ireland*, C-319/20, ECLI:EU:C:2021:979, point 84.

([56]) *Meta Platforms Ireland*, see footnote 53, paragraphs 70-72. See d'Ath, F., 'Meta v. BVV: The CJEU Clarifies The Scope of the Representative Action Mechanism of Article 80(2) GDPR Whereby Not-for-Profit Associations Can Bring Judicial Proceedings Against a Controller or Processor', *EDPL*, Vol. 8, No. 2, 2022, p. 323. A fresh reference has been submitted concerning the same case at national level with regard to the requirement that a representative action under Article 80(2) should concern the infringement of the rights of a data subject '*as a result of the processing*.' In his Opinion of 25 January 2024, Advocate General Richard de la Tour has concluded that it is sufficient to specify actual, not hypothetical, processing which is linked to the specific infringement alleged: Pending Case, *Meta Platforms Ireland Limited*, C-757/22, ECLI:EU:C:2024:88, paragraphs 48 and 56.

([57]) Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (*General terms of use of a social network*)*, C-252/21, ECLI:EU:C:2023:537.

([58]) Opinion of Advocate General Rantos of 20 September 2022, *Meta Platforms and others (*General terms of use of a social network*)*, C-252/21, ECLI:EU:C:2022:704, point 10.

Meta from processing data under FB's terms of service and imposed measures to stop Meta from continuing.

The CJEU held, first, that a competition authority may, in order to establish whether there has been an abuse of a dominant position under competition law, examine whether an undertaking's conduct complies with other rules, such as the data protection rules in the GDPR ([59]). Advocate General Rantos felt that compatibility with the GDPR could be taken into account as an 'incidental question' ([60]) but the Court went further, and added that compliance or not with the GDPR may be a 'vital clue' whether a certain practice amounts to a breach of the competition rules ([61]).

Second, the Court ruled that a competition authority does not have primary competence to assess compliance with the GDPR, which is reserved to the DPAs concerned, whom it must inform and consult and seek their cooperation under the duty of sincere cooperation in Article 4(3) TEU. If there is any decision or investigation by the competent CSA, LSA or court, the competition authority cannot depart from it, although it remains free to draw its own conclusions from the point of view of the application of competition law ([62]).

This case law has affirmed the complementarity of data protection, consumer protection and competition law first put forward in 2014, and answered some of the initial questions on how such cooperation should function in practice and respect the independence of DPAs.

2.4. Relationship with national law

In cases where national law is clearly inconsistent with the Charter or secondary data protection law, the Court has not hesitated to interpret and apply EU law ([63]). Otherwise where there is no specific EU rule precluding a national rule and where it furthers the objectives of the GDPR, the Court has deferred to national law, particularly with regard to the principle of procedural autonomy. Underlying the Court's approach, two themes can be discerned: increasing the level of protection of the fundamental right to protection of personal data, and deferring where appropriate to more specific or more protective national rules.

([59]) *Meta Platforms and others (*General terms of use of a social network*)*, see footnote 57, paragraphs 43 and 47.

([60]) Opinion of Advocate General Rantos in *Meta Platforms and others (*General terms of use of a social network*)*, see footnote 58, point 22.

([61]) *Meta Platforms and others (*General terms of use of a social network*)*, see footnote 57, paragraph 47.

([62]) *Ibid*, paragraphs 56 to 60. In the event, the BKA had consulted in advance of its decision the two CSAs concerned and the LSA, which had raised no objections.

([63]) See the case law on data retention, surveillance and international transfers discussed in respectively the contributions by Kranenborg, H., 'The EDPS and the never-ending story of data retention', Chapter 6 and Kuner, C., 'International Data Transfers and the EDPS: Current Accomplishments and Future Challenges', Chapter 7.

This dual approach can be seen in the cases on collective representation and administrative competence discussed earlier in this section. It is also present in a number of cases on data protection officers ('DPOs') and compensation for non-material harm.

A. Dismissal of Data Protection Officers

In *Leistritz* ([64]) the head of the legal department ([65]) and internal data protection officer was dismissed with one month's notice on the grounds of a 'corporate restructuring measure,' under which both functions were outsourced. The Court had to reconcile the second sentence of Article 38(3) GDPR, whereby the DPO '*shall not be dismissed or penalised by the controller or the processor for performing his tasks,*' with Article 6(4) of the German federal law on data protection, which offered a higher level of protection and provided that a DPO can only be dismissed if '*there are facts that give the public body just cause to terminate without notice*.'

In effect, the dismissal was valid under EU law, because it was not related to carrying out the function of DPO, but invalid under national law, because a restructuring measure does not constitute just cause for dismissal ([66]). As in *Fashion ID* and *Bundesverband*, the question arose whether EU law precluded or permitted the national rule.

Both the Court and Advocate General Richard de la Tour felt that Article 38(3) GDPR is only intended to ensure a DPO's *functional independence*, and not to govern the overall employment relationship between a controller or a processor and staff members. However they differed on the outcome. The Advocate General implicitly characterised Article 38(3) second sentence as another opening clause ([67]). In contrast, the Court concluded that the employment relationship of the DPO and the employer, and the determination of the rules on protection against termination of the DPO's employment contract, falls outside the scope of data protection and within the scope of social policy, and hence is governed by national law. Under Article 4(2)(b) TFEU, the EU and Member States have a shared competence in the field of social policy, for the purposes of Article 2(2) thereof. Moreover Article 153(1)(d) specifies that the EU is to support and complement Member States' activities in the field of the protection of workers in cases where their employment contract is terminated ([68]).

([64]) Judgment of the Court of Justice of 22 June 2022, *Leistritz*, C-534/20, ECLI:EU:C:2022:495.

([65]) The issue of conflict of interest that may arise from the combining of these two rules was considered in the subsequent judgment of the Court of Justice of 9 February 2023, *X-FAB Dresden*, C-453/21, ECLI:EU:C:2023:79.

([66]) At EU level Article 44(8) EUDPR adds the consent of the EDPS as an additional protection.

([67]) *Leistritz*, see footnote 64; Opinion of Advocate General Richard de la Tour of 22 January 2022, *Leistritz*, C-534/20, ECLI:EU:C:2022:62, point 39, footnote 28.

([68]) *Leistritz*, see footnote 64, paragraph 32. The Court added that Article 153(2)(b) TFEU provides that the EU may lay down minimum requirements for employment protection of workers in directives, not in regulations, *Leistritz*, see footnote 64, paragraph 33.

Under both analyses, national legislation may impose stricter dismissal conditions so long as they do not undermine GDPR objectives, thus both approaches would have been equally reassuring for Member States with a higher level of protection than the GDPR ([69]). However the approach of the Court was more sensitive to the boundaries between EU and national law under the Treaties. The Court added that '*the mere fact that domestic measures come, as is the situation in the present case, within an area in which the European Union has powers cannot bring those measures within the scope of EU law*' ([70]).

B. Compensation for non-material damage

Article 82(1) GDPR provides that '*(a)ny person who has suffered material or non-material damage as a result of an infringement of [the GDPR] shall have the right to receive compensation from the controller or processor for the damage suffered*.' This provision is different to its predecessor in the DPD in one specific respect: it specifically adds the right to 'non-material' damage ([71]). Recital 146 adds that '*the concept of damage should be broadly interpreted' and that 'data subjects should receive full and effective compensation*.' The legislation itself, therefore, suggests that the addition of non-material damage was intended as a significant change.

A series of cases have been referred to the CJEU which raise three issues: the nature of compensation for non-material damage under Article 82(1), the burden of proof, and the criteria for the assessment of damage. The Court's analysis of the nature of compensation and the assessment criteria shows at the same time its insistence on autonomous EU law guaranteeing protection of the fundamental right and its deference to national law when this does not undermine the fundamental right.

The landmark ruling in this area is *Österreichische Post* ([72]). The Austrian Post Office ('ÖPAG') collected information on its customers without their knowledge or consent, and used an algorithm based on socio-demographic criteria to calculate their political affinities and sell this information to parties advertising elections. An Austrian attorney discovered that the algorithm had concluded that he was likely to vote for a far-right party. On the one hand he had suffered no material harm because both he and a number of other plaintiffs had obtained interim relief from the Austrian courts, and because he had entered his details in a mailing black list, so that the ÖPAG had not sold his personal data to anyone.

([69]) In addition to Germany, Belgium and Spain have chosen to supplement Article 38(3), see Opinion of Advocate General Richard de la Tour in *Leistritz*, see footnote 67, point 46, footnote 34.

([70]) *Leistritz*, see footnote 64, paragraph 44.

([71]) Contrast the United States, where the Supreme Court has ruled that only those that can show concrete harm have standing to seek damages against private defendants, *TransUnion LLC v. Ramirez*, 594 U.S. ___ (2021).

([72]) Judgment of the Court of Justice of 4 May 2023, *Österreichische Post (*Non-material damage resulting from unlawful processing of data*)*, C-300/21, EU:C:2023:370.

On the other hand, in the wording of the court, '*he felt great upset, a loss of confidence and a feeling of exposure due to the fact that a particular affinity had been established between him and the party in question*.' He therefore claimed €1,000 compensation for non-material damage. His claim was dismissed because it was below a "materiality" threshold for damage under national law, which did not provide for compensation for mere discomfort and feelings of unpleasantness.

On the three issues, Advocate General Sánchez-Bordona took a conservative approach, on the basis that a broad interpretation of Article 82 was unnecessary to protect individuals' rights. Hence compensation should not be available in the absence of damage and, based on the distinction in national systems between damage and mere inconvenience, Article 82 imposes a *de minimis* 'threshold of seriousness.' Finally EU law does not impose any requirements for the assessment of compensation, save for the standard principles of equivalence and effectiveness ([73]).

On the first issue, the Court found that a GDPR infringement does not give rise *per se* to a right to damages, since it is only the first limb of three cumulative conditions governing the right to compensation ([74]). As to the nature of the right to compensation, the Court contrasted it with the punitive purpose of administrative fines and other penalties under Articles 83 and 84, which are not conditional on the existence of individual damage. However, the Court added that these different categories of provisions under Article 82 and Articles 83 and 84 are also complementary in encouraging compliance with the GDPR, because the individual right to seek compensation for damage '*reinforces the operational nature*' of the GDPR *'and is likely to discourage the reoccurrence of unlawful conduct*' ([75]).

On the second issue, the Court noted that the concepts of 'damage' and 'non-material damage' within the meaning of Article 82 '*must be given an autonomous and uniform definition specific to EU law*' ([76]). In contrast to the Advocate General ([77]), it held that the GDPR does not contain any reference to '*any threshold of seriousness*' and it would be contrary to the legislator's broad conception of 'damage' to impose such a threshold, in view of the context of Article 82, the third sentence of recital 146, and the objective of the GDPR,

([73]) Opinion of Advocate General Campos Sánchez-Bordona of 6 October 2022, *Österreichische Post (*Non-material damage resulting from unlawful processing of data*)*, C-300/21, ECLI:EU:C:2022:756.

([74]) *Österreichische Post (*Non-material damage resulting from unlawful processing of data*),* see footnote 72, paragraph 32. In addition, there must be material or non-material damage resulting from that infringement and, third, a causal link between the damage and the infringement.

([75]) *Österreichische Post (*Non-material damage resulting from unlawful processing of data*)*, see footnote 72, paragraphs 38 to 40. See also judgment of the Court of Justice of 21 December 2023, *Krankenversicherung Nordrhein*, C-667/21, EU:C:2023:1022, paragraph 85.

([76]) *Österreichische Post (*Non-material damage resulting from unlawful processing of data*),* see footnote 72, paragraph 44.

([77]) Opinion of Advocate General Campos Sánchez-Bordona in *Österreichische Post (*Non-material damage resulting from unlawful processing of data*)*, see footnote 73, who found that, based on the distinction in national systems between damage and mere inconvenience, Article 82 imposes a *de minimis* 'threshold of seriousness.'

set forth in recital 10, to ensure a consistent and high level of protection ([78]). However the Court insisted that a plaintiff alleging negative consequences still bears the burden of proving that '*those consequences constitute non-material damage within the meaning of Article 82*.' To understand this caveat, there are two clues earlier in the judgment, based on the order for reference. First the Court noted that it is '*apparent from the order for reference that no harm other than those adverse emotional effects of a temporary nature has been established*' ([79]). Second, the Court summarised the view of the [referring court] that '*non-material damage must be compensated … if it is tangible, even if it is minor. By contrast, such damage should not be compensated if it appears to be completely negligible, as would be the case for the merely unpleasant feelings that are typically associated with such a breach*' ([80]).

On the third issue, following its dual approach, the Court entrusted the criteria for assessment to the detailed rules in each national legal system. While this approach may be criticised as reducing the level of harmonisation, the Court added three significant riders to this finding which should be taken into account by the national courts. First, it described the domestic rules as rules for '*actions intended to safeguard of the rights which individuals derive from the GDPR*.' Second, it subjected the criteria for assessment of compensation under those rules to the principles of equivalence and effectiveness ([81]). Finally, it underlined the 'compensatory function' of the right to compensation under the GDPR and emphasised that the GDPR '*seeks to ensure full and effective compensation for the damage suffered*.' These criteria may ensure an acceptable standard of interpretation of the right to compensation across the EU and allay fears that the absence of an EU criteria for assessment would lead to a lower standard of enforcement. Taken as a whole, the ruling has given full force to the intention of the legislator whilst at the same time deferring to the principle of procedural autonomy.

Subsequently the Court has clarified and confirmed the three issues: the nature of compensation under Article 82(1) is full compensation but no more ([82]); there is no threshold of seriousness but the data subject must show tangible non-material harm rather than a mere fear of possible misuse ([83]); the burden is on the controller to disprove liability for harm caused, and the assessment

([78]) *Österreichische Post (*Non-material damage resulting from unlawful processing of data*)*, see footnote 64, paragraphs 45 to 49.

([79]) *Ibid*, paragraph 12.

([80]) *Ibid*, paragraph 19.

([81]) Affirmed in the judgment of the Court of Justice of 25 January 2024, *MediaMarktSaturn*, C-687/21, ECLI:EU:C:2024:72, paragraphs 48 and 54; and *Krankenversicherung Nordrhein*, see footnote 75, paragraphs 86 and 87.

([82]) *MediaMarktSaturn*, see footnote 81, paragraph 54.

([83]) *Österreichische Post (*Non-material damage resulting from unlawful processing of data*)*, see footnote 72, paragraphs 42 and 50; judgment of the Court of Justice of 14 December 2023, *Natsionalna agentsia za prihodite*, C-340/21, ECLI:EU:C:2023:986, paragraph 84; judgment of the Court of Justice of 14 December 2023, *Gemeinde Ummendorf*, C-456/22, EU:C:2023:988, paragraphs 21 and 23; and *MediaMarktSaturn*, see footnote 81, paragraphs 60 and 68.

of damage has no relation to the gravity of the violation ([84]) and must rely on the domestic rules of each Member State relating to the extent of pecuniary compensation ([85]), subject to the principles of equivalence and effectiveness ([86]).

3. Accountability and the GDPR – meaning and burden of proof

The principle of accountability is one of the most significant innovations of the GDPR and one of its central themes ([87]). In place of the ineffective 'notify and forget' approach under Articles 18 and 19 DPD, which placed responsibility on DPAs to receive notifications from controllers, it shifts the burden of data protection to the controller, who must take proactive action to ensure compliance and to be ready to demonstrate that compliance. It can be found in Articles 5(2) and 24 GDPR, which taken together require controllers to ensure and demonstrate compliance. Controllers must take responsibility for their processing of personal information, assess and implement appropriate and effective measures to ensure compliance, and be able to demonstrate that they have the appropriate systems in place to ensure compliance[88]. The Court has made it clear that it will hold to account those who process personal data for the processing for which they are responsible ([89]).

The case law of the CJEU has analysed the principle, laid down specific consequences for the burden of proof, and underpinned a positive approach to the interpretation of the legislation.

First, the Court has accepted that the principle runs through both Articles 5(2) and 24 GDPR. At first there was a tendency to refer only to Article 5(2) ([90]), which, to be fair, bears the title of 'accountability' ([91]). In some of its more recent rulings the Court has referred to both Articles. This development is important,

([84]) *Österreichische Post (*Non-material damage resulting from unlawful processing of data*)*, see footnote 72, paragraph 51*;* *Natsionalna agentsia za prihodite*, see footnote 83, paragraph 78*;* *Gemeinde Ummendorf*, see footnote 83, paragraph 16; and *MediaMarktSaturn*, see footnote 81, paragraph 52.

([85]) *MediaMarktSaturn*, see footnote 81, paragraph 53.

([86]) For a discussion of the principle of 'minimum effectiveness' required by Article 47 of the Charter, see Mulders S., *The relationship between the principle of effectiveness under Art. 47 CFR and the concept of damages under Art. 82 GDPR*, 13 IDPL (2023) p. 169 at p.175.

([87]) Lenaerts, K., The EU General Data Protection Regulation Five Months On speech by CJEU President Lenaerts at the 40th International Conference of Data Protection and Privacy Commissioners, 25 October 2018.

([88]) See generally on accountability Docksey, C., 'Article 24', in Kuner, C., Bygrave, L.A. and Docksey, C. (eds.), op. cit. (footnote 9), p. 555-570.

([89]) *Fashion ID*, see footnote 50, paragraph 74.

([90]) Judgment of the Court of Justice of 24 February 2022, *Valsts ieņēmumu dienests (*Processing of personal data for tax purposes*)*, C-175/20, ECLI:EU:C:2022:124, paragraph 77; judgment of the Court of Justice of 4 May 2023, *Bundesrepublik Deutschland*, C-60/22, ECLI:EU:C:2023:373, paragraph 53; *Meta Platforms and others (General terms of use of a social network)*, see footnote 57, paragraph 95.

([91]) For the legislative history showing how the labels attached to Article 5(2) (*accountability*) and Article 24 (*responsibility*) ended up the wrong way round, see Docksey, C., 'Article 24' in Kuner, C., Bygrave, L.A., Docksey, C. (eds.), *The EU General Data Protection Regulation: A Commentary, Update of Selected Articles,* Oxford University Press, Oxford, 2021, p. 115–116.

because it avoids the danger of emphasising the demonstration of simple compliance under Article 5(2) ([92]) rather than the taking of appropriate technical and organisational measures required under Article 24 and the mandatory use of other accountability tools such as privacy by design and default under Article 25 and security of processing under Article 32. The leading case is now *Natsionalna agentsia za prihodite*, in which the Court referred to '*the principle of accountability of the controller, set out in Article 5(2) of the GDPR and given expression in Article 24 thereof*' ([93]), following Advocate General Pitruzzella's explanation that the '*principle of accountability … places the responsibility on the controller to take proactive measures to ensure compliance of the processing operation … and to be able to demonstrate such compliance*' ([94]).

Second, the principle of accountability has shifted the burden of proof onto controllers, as a consequence of the obligation to 'stand ready to demonstrate compliance when called upon to do so' ([95]). In *SIA 'SS'* the Latvian tax authorities asked an online sales website for information on its advertisements and sales, including identifiable personal data such as car chassis numbers and telephone numbers. The Court '*emphasised that, in accordance with the principle of accountability set out in Article 5(2) [GDPR], the controller must be able to demonstrate compliance with the principles relating to the processing of personal data set out in paragraph 1 of that article*.' In consequence the burden of proof lay with the tax authorities ([96]).

4. Accountability and scope: narrow exceptions and broad definitions

The CJEU has followed a broad approach when interpreting the scope and the definitions of the EU data protection rules, on the basis that Article 2(1) GDPR gives a '*very broad definition of the material scope of that regulation*' ([97]). In particular, it has developed the notion of joint controllership under the DPD, in advance of Article 26 GDPR, in order to '*ensure, through a broad definition … ,*

([92]) See for example the judgment of the Court of Justice of 7 December 2023, *SCHUFA Holding (*Scoring*)*, C-634/21, ECLI:EU:C:2023:957, paragraph 67.

([93]) *Natsionalna agentsia za prihodite*, see footnote 83, paragraph 57 and ground 3 of the ruling; see also *MediaMarktSaturn*, see footnote 81, paragraph 43.

([94]) Opinion of Advocate General Pitruzzella of 27 April 2023, *Natsionalna agentsia za prihodite*, C-340/21, ECLI:EU:C:2023:353, point 21.

([95]) Van Alsenoy, B., 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation', *JIPITEC*, Vol. 7, No. 3, 2017, p. 271, paragraph 43.

([96]) *Valsts ieņēmumu dienests (*Processing of personal data for tax purposes*)*, see footnote 90, paragraphs 77, 78 and 81. See also *Meta Platforms and others (General terms of use of a social network)*, see footnote 57, paragraph 152; *MediaMarktSaturn*, see footnote 81, paragraph 43.

([97]) Judgment of the Court of Justice of 22 June 2021, *Latvijas Republikas Saeima (*Penalty points*)*, C-439/19, EU:C:2021:504, paragraph 61.

effective and complete protection of the persons concerned' ([98]). The President of the Court, Koen Lenaerts, has characterised this case law as confirming the Court's attachment to 'high levels of accountability' of individuals that process personal data, in light of the 'central theme' of accountability in the GDPR ([99]). This "accountability" approach may be applied more generally to the case law on scope, definitions and exceptions, that is, to the cases where the Court wishes to ensure that there is responsibility for the processing of personal information.

Similarly, the exceptions to the material scope of the GDPR are set forth in 'exhaustive terms' ([100]) in Article 2 paragraphs 2 and 3 thereof, and must be interpreted strictly ([101]).

The definitions and exceptions are important because they define the scope of the data protection legislation, and hence have often been employed in order to avoid accountability under those rules (usually unsuccessfully) ([102]).

4.1. Processing in the course of an activity which falls outside the scope of Union law

In *Land Hessen* a citizen submitted a subject access request to the Petitions Committee of the Parliament of the State of Hessen, which was refused on the basis that parliamentary activity falls outside the scope of the GDPR.

The Court held that Article 2(2)(a) GDPR must be interpreted restrictively because it constitutes an exception to the wide definition of the scope of the GDPR set out in Article 2(1). It refers to activities which are, in all circumstances, activities of the State, such as public security, defence, State security and activities in the areas of criminal law and it applies only to those activities or those which can be classified in the same category (*ejusdem generis*) ([103]).

Whilst the activities of the Petitions Committee of the Land Parliament are incontestably public activities, they are political as much as administrative, there is no specific exception for parliamentary activities under Article 23 GDPR, they do not correspond to the activities mentioned in Article 2(2)(b) and (d) GDPR, nor could they be classified in the same category ([104]).

([98]) Judgment of the Court of Justice of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraph 28; judgment of the Court of Justice of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 66; *Fashion ID*, see footnote 50, paragraph 66.

([99]) Lenaerts, K., op. cit. (footnote 87).

([100]) *Österreichische Datenschutzbehörde*, see footnote 8, paragraph 34.

([101]) *Ibid*, paragraph 62 and the case law cited.

([102]) See for example the argument concerning the definition of personal data in the judgment of 18 June 2020 *Commission v Hungary (*Transparency of associations*)*, C-78/18, ECLI:EU:C:2020:476, paragraphs 109 and 126.

([103]) *Land Hessen*, see footnote 2, paragraphs 68 to 69, referring to the interpretation of Article 3(2), first indent, of the predecessor DPD in the judgment of the Court of Justice of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraphs 43 and 44. For more recent case law on Article 2(2)(a) see *Österreichische Datenschutzbehörde*, see footnote 8, paragraph 18.

([104]) *Land Hessen*, see footnote 2, paragraphs 68 to 72.

More recently, *Österreichische Datenschutzbehörde* considered whether the activities of a different parliamentary committee, set up to scrutinise whether there had been any political influence over the Austrian national security authorities, fell within the exception. The Grand Chamber of the CJEU affirmed the ruling of the Third Chamber in *Land Hessen* on the narrow scope of the exception excluding parliamentary activities. In particular, it approved the observation by Advocate General Szpunar that the exception refers only to categories of *activities* which, by their nature, fall outside the scope of Union law, and not to categories of *persons* ([105]).

Second, it applied a strict interpretation to the notion of '*activities intended to safeguard national security or … which can be classified in the same category… which encompass, in particular, those that are intended to protect essential State functions and the fundamental interests of society*' ([106]). When a parliamentary committee scrutinises the activities of the intelligence community which are necessary for safeguarding national security, that activity falls within the exception; however the '*mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable*' ([107]). In the present case, the specific task of investigation of political influence over the intelligence community was not itself an activity intended to safeguard national security and hence fell outside the exception.

4.2. Processing by a natural person in a purely personal or household activity

The scope of the household activity limb of this exception, formerly Article 3(2) DPD, was considered in *Ryneš* ([108]), where a householder installed a video camera outside his house to photograph and prosecute vandals breaking the windows of his house. Although he had a valid reason for the processing, the DPA found that he had collected the personal data of persons in the street and the house opposite without their consent or informing them, and had failed to notify DPA of this processing. The underlying problem in this case was that Czech law was based on informational self-determination, so that consent was normally required as the lawful basis for processing. He therefore had to find another means of defence, and argued that the filming of the vandals fell within the household exception, so that the data protection rules did not apply.

([105]) *Österreichische Datenschutzbehörde,* see footnote 8, paragraph 41, referring to the Opinion of Advocate General Szpunar of 11 May 2023, ECLI:EU:C:2023:397, point 84.

([106]) *Österreichische Datenschutzbehörde,* see footnote 8, paragraphs 37, 45 and 46 and case law cited.

([107]) *Ibid*, paragraph 50 and case law cited. This venerable approach is long established, see e.g. judgment of the Court of the Justice of 15 May 1986, *Johnston v Chief Constable of the Royal Ulster Constabulary*, C-222/84, ECLI:EU:C:1986:206, paragraph 26.

([108]) Judgment of the Court of Justice of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428.

The Court noted that this was an exception to a fundamental right and hence must be narrowly construed. It found that the exception excludes anything that covers, even partially, a *public space* and is accordingly '*directed outwards from the private setting of the person processing the data*' ([109]).

The scope of the personal activity limb of this exception was interpreted equally narrowly in *Buivids*, together with the broad statutory derogation for journalism ([110]). In this case, a person who was interviewed in a police station took the opportunity to video the police officers carrying out their duties around him and post the video on YouTube. The Court affirmed that exceptions must be interpreted strictly and found that this was not a purely personal activity, since the posting on the website permitted access to the personal data to an indefinite number of people ([111]). The Court also approved two important points raised by Advocate General Sharpston. Austria had argued that the act of recording a video of police officers in the public performance of their duties fell outside the scope of the Directive, because officials carrying out their duties have to accept that they operate in the public arena and that their actions may be subject to scrutiny. However there is no exception to the scope of the Directive for the processing of personal data of public officials ([112]). Moreover, the Court recalled, the fact that information is provided as part of a professional activity does not mean that it cannot be characterised as 'personal data' ([113]).

We should now turn to the broad approach to definitions.

4.3. Personal data – any information relating to an identified or identifiable person

This short phrase, formerly Article 2(a) DPD, contains four distinct elements, each of which has been considered in the extensive case law on this definition.

The words '*any information*' mean that personal data is not limited to any particular medium, but may be contained in non-verbal media such as photographs and videos ([114]). On the other hand, the Court has stressed that legal '*persons*' do not fall within the definition ([115]), unless the name of a company contains the name of an identifiable natural person ([116]).

([109]) *Ibid*, paragraph 33. The same approach was applied to video cameras in common areas of an apartment block in the judgment of the Court of Justice of 11 December 2019, *Asociația de Proprietari bloc M5A ScaraA*, C-708/18, ECLI:EU:C:2019:1064.

([110]) See Kranenborg, H., 'Article 85', in Kuner, C., Bygrave, L.A. and Docksey, C. (eds.), op. cit. (footnote 9), p.1207-1209.

([111]) Judgment of the Court of Justice of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 43.

([112]) *Ibid*, paragraphs 44 to 45, referring to the Opinion of Advocate General Sharpston of 27 September 2018, ECLI:EU:C:2018:780, C-345/17, point 30.

([113]) *Ibid*, paragraph 46, referring to the judgment of the Court of Justice of 16 July 2015, *ClientEarth and PAN Europe/EFSA*, C-615/13 P, EU:C:2015:489, paragraph 30.

([114]) *Ibid*, paragraph 39.

([115]) Judgment of the Court of Justice of 10 December 2020, *J & S Service,* C-620/19, ECLI:EU:C:2020:1011, paragraph 46. See recital 14 GDPR.

([116]) Judgment of the Court of Justice of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 53.

The words '*relating to*' were definitively considered in *Nowak* ([117]). A trainee accountant who failed an accountancy exam made a subject access request, inter alia, for his examination script. The Court held that it was personal data, which covers both objective and subjective data (i.e. opinions and assessments) and has a wide scope ('any information'), which is not limited to sensitive or private personal data in that case.

In 2007, the Article 29 Working Party ('WP29'), the predecessor of the EDPB, laid down three alternative tests, any one of which is sufficient to show that information 'relates to' a natural person ([118]). The Court applied these criteria to find that data may be personal in view of their *content* (the examination script related to the knowledge of the applicant, and for some potential employers the handwriting may reveal character), their *purpose* (the assessment of the candidate) or their *effect* (on the candidate's career). In the event, all three criteria were met in this case, but any one would have been sufficient to establish that the examination paper constituted the personal data of the candidate ([119]). In the same way, the comments by the examiner were also the personal data of the examiner.

Two further issues arose from the ruling in *Nowak*. First, it established that subjective opinions can constitute personal data. In the earlier ruling of *YS* the Court had found that legal opinions about the status of asylum applicants did not relate to them, and were only a legal analysis of their situation. Only the objective facts about the applicants constituted personal data in that case.

Second, *Nowak* opened the way for the development of the case law on the right of subject access under Article 15(3) GDPR. The underlying reason for the restrictive approach in *YS* was to limit the scope for subject access requests. The Court had feared that if legal opinions constituted personal data, the right of subject access would serve the purpose of guaranteeing a right of public access to administrative documents, which is not the purpose of the data protection rules ([120]).

However the right of access has been characterised as a 'cornerstone' for meaningfully exercising other data protection rights ([121]), and this enabling role has now been given full effect by the First Chamber of the CJEU in a trio of rulings in 2023.

([117]) Judgment of the Court of Justice of 20 December 2017, *Nowak*, C-434/16, ECLI:EU:C:2017:994. See Podstawa K., 'Peter Nowak v Data Protection Commissioner: You Can Access Your Exam Script, Because It Is Personal Data', *EDPL* Vol. 4, No. 2, 2018, p. 252-259.

([118]) Article 29 Working Party Opinion 4/2007 on the concept of personal data, WP136, adopted on 20 June 2007.

([119]) They are not cumulative, as in the English Court of Appeal ruling in *Durant v Financial Services Authority* [2003] EWCA Civ 1746; [2004] FSR 28. This led to the opening of an infringement proceeding by the Commission which was resolved by House of Lords guidance in *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47.

([120]) Judgment of the Court of Justice of 17 July 2014, YS and others, C-141/12 and C-373/12, ECLI:EU:C:2014:2081, paragraph 46. See also the Opinion of Advocate General Sharpston of 12 December 2013 in this case, ECLI:EU:C:2013:838, point 61.

([121]) Ausloos, J., Veale M., and Mahieu, R., 'Getting Data Subject Rights Right', *JIPITEC*, Vol. 10, No. 3, 2019, p.283, paragraph 17.

In *CRIF* (*Österreichische Datenschutzbehörde*) ([122]) the Court considered whether the right to obtain a copy of the personal data undergoing processing under Article 15(3) GDPR means that the data subject must be given not only a copy of those *data*, but also a copy of *documents* which contain those data. The applicant requested a credit reference agency, CRIF, for access to his personal data and for a copy of the documents containing that data, namely emails and database extracts. CRIF provided some of the information requested in an aggregated form, and in a summary. The requested documents were not provided.

The Court found that data subjects have the right to obtain a faithful reproduction of their personal data that are processed by the controller in the form of a 'copy' which contains all the personal data undergoing processing. The right under Article 15 must enable data subjects to ensure that the personal data relating to them are correct and are being processed in a lawful manner, and enable them to exercise their other rights under the GDPR, namely the rights to rectification, erasure and restriction of processing as well as the rights to object and right of action where they suffer damage ([123]). The Court relied in particular on the principle of transparency enshrined in Article 12(1) GDPR, which requires that the information sent to the data subject must be concise, easily accessible and easy to understand, and formulated in clear and plain language. As a result, the copy of the personal data must reproduce those data fully and faithfully in an intelligible presentation. On this basis, the Court concluded that it may be essential to provide a copy of extracts from documents or even entire documents or extracts from databases which contain, inter alia, the personal data undergoing processing.

The Court then addressed the balancing of rights required under Article 15(4), where the rights and freedoms of others are affected. Such rights include '*trade secrets or intellectual property and in particular the copyright protecting the software*', per recital 63 GDPR, together with the right to the protection of personal data of third parties. In *Nowak*, for example, the comments on the examination paper were also the personal data of the examiner. Closely following Advocate General Pitruzzella ([124]), the Court ruled that a balance has to be struck between the rights in question, for example by communicating the personal data in a way that does not infringe the other rights at issue, bearing in mind the caveat in recital 63 that '*the result of those considerations should not be a refusal to provide all information to the data subject*'.

Finally, the Court ruled that the concept of 'information' in Article 15(3) GDPR, understood in context, is limited to the personal data of which the controller must provide a copy under that provision.

([122]) *Österreichische Datenschutzbehörde*, see footnote 8.

([123]) *Ibid*, paragraph 35 and the case law cited.

([124]) Opinion of Advocate General Pitruzzella of 15 December 2022, *Österreichische Datenschutzbehörde*, C-487/21, ECLI:EU:C:2022:1000, point 61.

In consequence, it will be necessary in any particular case to consider whether it is sufficient to provide aggregated data or a summary, for example where the personal data processed are mostly the data subject's name, address and contact details. In cases where a document is solely about the data subject, or the information being processed is also factual or evaluative, or where the document contains empty fields, which in context may convey further information, the most effective way of ensuring the right of access would be to provide a copy of the document or part of the document containing that information.

In *Österreichische Post* ([125]) and *Pankki S* ([126]) the Court further developed its approach to the right of access. It stressed that the right of access is '*characterised by the broad scope of the information that the controller must provide to the data subject*,' and underlined that the rights under Articles 12(1) and 15(3) are both part of transparency, an important element of the GDPR ([127]). In *Österreichische Post* the Court found that where personal data have been or will be disclosed to recipients, the controller is obliged to provide the data subject, on request, with the actual identity of recipients. Only in cases where it is not (yet) possible to identify those recipients may the controller only indicate categories of recipients (as well as cases where the controller demonstrates that the request was manifestly unfounded or excessive). In *Pankki S* the Court added that the employees of a controller acting under its instructions are not recipients themselves. In consequence there is no right to know their identities unless that information is essential in order to enable data subjects to exercise their rights effectively.

It can seen that the Court has progressed from a cautious and restrictive approach in *YS* to one which regards the right under Article 15, albeit a procedural rather than a substantive right, as a significant guarantee of data subjects' rights under the GDPR and Article 8(2) of the Charter ([128]).

In this context the First Chamber handed down a fourth ruling on information and access to personal data in *SCHUFA*. An application for credit was refused by a bank on the basis of a credit score provided by SCHUFA, a credit scoring agency. A score estimates the probability of the future behaviour of a person in terms of for example repayment of a loan. The applicant asked SCHUFA for information on her personal data and was informed of her score and, in broad terms, of the methods for calculating the scores. However, referring to trade secrecy, SCHUFA refused to disclose the various elements taken into account and their weighting. The Court held that, even though the bank and not SCHUFA made the actual contractual decisions, the score by SCHUFA amounted to a 'decision' for the purposes of establishing automated decision-making under Article 22 GDPR ([129]).

([125]) Judgment of the Court of Justice of 9 June 2022, *Österreichische Post (*Information regarding the recipients of personal data*)*, C-154/21, ECLI:EU:C:2023:3.

([126]) Judgment of the Court of Justice of 22 June 2023, *Pankki S,* C-579/21, ECLI:EU:C:2023:501.

([127]) *Ibid*, paragraphs 49 and 50.

([128]) *Österreichische Post (*Information regarding the recipients of personal data*)*, see footnote 125, paragraph 44.

([129]) *SCHUFA Holding (*Scoring*)*, see footnote 92.

There were two reasons motivating the Court's approach. First, as pointed out by the referring court, if SCHUFA did not fall under Article 22 GDPR, there would be a lacuna in legal protection: the controller with the necessary information, such as SCHUFA, would not be required to provide access to that information, whereas the controller making the decision on the basis of the score, such as the bank, would not have that information to provide. Second, it was common ground that SCHUFA's activity consists of 'profiling' under Article 4(4) of the GDPR, which, combined with automated processing, generates 'particular risks' to data subjects' rights and freedoms. In this context, if Article 22 applies, a data subject has the right to additional information under Article 13(2)(f) and Article 14(2)(g) GDPR and to extra, 'meaningful' information on the processing under Article 15(1)(h) GDPR. In addition, the controller has the obligation to adopt suitable safeguard measures under Article 22(3), such as human intervention. In such circumstances, the Court made it clear that its broad interpretation of Article 22(1), in particular the concept of 'decision' therein, '*reinforces the effective protection intended by that provision*' whereas a restrictive interpretation would have left a lacuna in legal protection ([130]).

In his lecture in 2018, CJEU President Lenaerts underlined that the fundamental rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter should protect people in particular against the undesired effects of profiling. His lecture presciently underlined the significance of the case law in this area, especially in view of the increasing pace of technological change in areas such as artificial intelligence. For example, in the present case SCHUFA stated at the hearing that it did not use self-learning algorithms at the time but that it may do in the future ([131]). The ruling in this case is a landmark for the application of Article 22 GDPR in the age of algorithms and artificial intelligence.

Finally, returning to the discussion of personal data, the CJEU has interpreted the expression '*identified* ([132]) *or identifiable person*.' An 'identifiable person' is defined in Article 4(1) GDPR as a person '*who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier …*', and is further extensively explained in recitals 26 and 30 GDPR.

Recital 26 GDPR states that, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person. It also discusses identification in the context of pseudonymisation and anonymisation. If a person may be identified using additional data together with pseudonymised data, those data are all personal data. In contrast, if a person can no longer be identified because their personal data have been anonymised, the data are no

([130]) *Ibid*, paragraphs 60 to 61.

([131]) Häuselmann, A., The ECJ's First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber, *European Law Blog*, 20 February 2023.

([132]) For a discussion of 'identification' and the merits of defining it as '*distinguishing a person from a Group*' see Purtova, N., 'From knowing by name to targeting: the meaning of identification under the GDPR', *IDPL*, Vol. 12, No. 3, 2022, p. 166.

longer personal data. In view of these criteria the WP29 has taken the view that anonymisation should make it *impossible* to re-identify a person, as opposed to the situation where a data controller does not delete the identifiable data but merely masks it ([133]).

Recital 30 consolidates in part the case law of the Court in *Promusicae* ([134]) and *SABAM* ([135]), where internet service providers ('ISPs') held both the IP addresses used at a specific time to download copyright material and the identity of the user of that IP address at that time. As a result, although the IP address does not itself identify a person, it does relate to a person who is identifiable by the ISP.

The case law was affirmed in *Breyer*, which also considered the dividing line between anonymous data and personal data. The applicant complained that when he visited German government websites, they kept a log of accesses, including the IP addresses of the devices from which the websites were visited. They replied that they needed this information to prevent cyber-attacks and to prosecute hackers. Unlike the previous case law, the government websites only knew their users' IP addresses, they did not have the information to link an IP address with a website user's name. Only the ISP concerned, a third party, could connect the IP address to a name and identify the website visitor, and German law did not allow the ISP to provide the website with the additional data necessary to identify the data subject.

The Court recalled the reference to 'any other person' in recital 26, and confirmed that it is not required that all the necessary identification information be in the hands of one person ([136]). Moreover, the CJEU found that 'legal channels' existed in the event of cyber attacks which could reasonably be used to identify the data subject, namely a competent authority could require the ISP to provide the additional information with a view to criminal proceedings. As a result, the dynamic IP addresses registered by a website could qualify as personal data ([137]).

The Court further noted, following the Advocate General, that there may be situations where identification is not feasible '*if the identification of the data subject was* ***prohibited by law*** *or* ***practically impossible*** *[because] it requires a disproportionate effort in terms of time, cost and man-power, so that the* ***risk of identification*** *appears in reality to be* ***insignificant*** ([138]) (emphasis supplied).

([133]) Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques, WP 216, adopted on 10 April 2014, p. 6 and 9.

([134]) Judgment of the Court of Justice of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 45.

([135]) Judgment of the Court of Justice of 16 February 2012, *SABAM*, C-360/10, ECLI:EU:C:2012:85, paragraph 51.

([136]) Judgment of the Court of Justice of 19 October 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779, paragraphs 42-43. See most recently judgment of the Court of Justice of 9 November 2023, *Gesamtverband Autoteile-Handel v Scania* (Access to vehicle information), C-319/22, ECLI:EU:C:2023:837, paragraph 45.

([137]) *Breyer*, see footnote 136, paragraphs 44 and 47.

([138]) *Ibid*, see footnote 136, paragraph 46.

The academic literature has underlined that this relative 'risk-based' approach by the Court is more flexible than the 'strict' approach of the WP39 noted above ([139]). On the facts of the case, however, the result was the same.

Two subsequent rulings by the General Court, both on appeal to the CJEU, have reopened this discussion.

In *OC*, the applicant was found by OLAF to have committed fraud and the file was passed to her national police. An OLAF press release enabled two journalists specialising in fraud to quickly identify the applicant. She claimed €1.1 million Euro damages under Article 268 TFEU to compensate for the non-material harm allegedly suffered as a result of the unlawful publication of her personal data.

The General Court held that the first limb of a damages claim had not been satisfied, a sufficiently serious breach of the fundamental right to protection of personal data, because the press release did not contain personal data ([140]). According to the court, the information in the OLAF press release was not sufficient to identify the applicant to an 'average or likely reader,' and the ability of the journalists to identify her was dismissed on the basis of their having specialised knowledge ([141]). However neither of these criteria are present in the case law of the CJEU ([142]), and it appears that the information in the press release, combined with information available online, would be sufficient to establish her identity ([143]).

It may be that the General Court introduced its new criteria because it did not wish to address the question of awarding compensation for non-material harm to an unworthy applicant.

The second ruling by the General Court appealed to the CJEU was *Single Resolution Board v EDPS* ([144]). In this case, the Single Resolution Board ('SRB') decided to place a Spanish bank under resolution ([145]) and contracted with a consultant firm to assess whether the bank's creditors and shareholders would have been treated more favourably under an insolvency procedure. These

([139]) See Weitzenboeck, E.M., Lison, P., Cyndecka, M., and Langford, M., 'The GDPR and unstructured data: is anonymization possible?', *IDPL*, Vol. 12, No. 3, 2022, p. 184 at p.194-195, and Groos, D., and van Veen, E-B., 'Anonymised Data and the Rule of Law', *IDPL*, Vol. 12, No. 4, 2022, p. 498 at p. 501-502. Cf. Zuiderveen Borgesius, F.J., 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition', *EDPL*, Vol. 3, No. 1, 2017, p. 130 at p.135.

([140]) Within the meaning of Article 3(1) EUDPR, *ibid,* Article 4(1) GDPR.

([141]) Judgment of the General Court of 4 May 2022, *OC v Commission*, T-384/20, ECLI:EU:T:2022:273.

([142]) Paun, M., 'OLAF's Press Release no. 13/2020 Does Not Contain Personal Data: On 'Identifiability' and Action for Damage', *EDPL*, Vol. 8, No. 3, 2022, p. 439-440.

([143]) *Ibid*, p. 440-441. the CJEU found that the General Court erred in finding that the identifiers in the press release did not reasonably allow the appellant to be identified and was wrong to hold that the information contained in the press release was not covered by the concept of 'personal data,' see judgment of the Court of Justice of 7 March 2024, OC v Commission, C-479/22 P, ECLI:EU:C:2024:215.

([144]) Judgment of the General Court of 26 April 2023, *SRB v EDPS,* T-557/20, ECLI:EU:T:2023:219.

([145]) Decision SRB/EES/2017/08 concerning a resolution scheme in respect of Banco Popular Español, SA, adopted on the basis of Regulation (EU) No 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit institutions and certain investment firms in the framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No 1093/2010, OJ L 225, 30.7.2014, p. 1.

parties were requested to provide information to the SRB, which pseudonymised that information, in the sense of Article 4(5) GDPR, by removing their identifying details, and transmitted the pseudonymised information to the consultants for analysis.

Five of the parties complained to the EDPS that the SRB had failed to inform them that the data collected through their responses to the SRB would be transmitted to the consultants, in violation of the obligation under Article 15(1)(d) EUDPR ([146]) to provide them with information concerning the recipient of the personal data. After a lengthy procedure, the EDPS adopted a revised decision which concluded that the SRB had infringed its statutory obligation to provide information to the complainants and that the SRB should ensure that such an infringement is not repeated in its privacy statements.

The General Court found that the data transmitted were not personal data for two reasons, both in effect, in the view of the Court, due to a failure of due diligence by the EDPS. First, the EDPS had failed to specifically consider and apply the *Nowak* tests to the facts of the case. Since the EDPS had not examined whether the information transmitted to the consultants related to a particular person by virtue of its content, purpose or effect, the EDPS could not conclude that that information related to a natural person within the meaning of Article 3(1) EUDPR ([147]). Second, the EDPS had failed to consider the situation of the recipients, as opposed to that of the *SRB*, and whether the possibility of combining the pseudonymised information with the additional information held by the SRB constituted a means likely reasonably to be used by the recipients to identify the parties ([148]). Since the EDPS had failed to consider whether these two tests for personal data were satisfied, it had infringed Article 3(1) EUDPR by deciding that the information transmitted to the consultants constituted the complainants' personal data. Like the ruling in *OC*, the Court may have been disinclined to find in favour of an unworthy party which it felt had not carried out the necessary assessment of the situation.

Two questions arise from this emphasis on procedure. First, as noted in section 3 above, the principle of accountability enshrined in Articles 5(2) and 24 GDPR has shifted the burden of proof onto the controller to stand ready to demonstrate its compliance. This would suggest, with regard to procedure, that the controller is obliged to demonstrate that a purported anonymisation is effective, to permit the DPA to assess whether there has been an infringement of the data protection rules.

Second, with regard to substance, the ruling fails to take account of the specific role played by pseudonymisation in its role as an 'important data protection

([146]) Drafted in the same terms as Article 13(1)(d) GDPR.

([147]) *SRB v EDPS*, see footnote 144, paragraphs 68 to 74.

([148]) *Ibid*, paragraphs 99 to 105.

safeguard' ([149]). An accountable controller in the situation of SRB would typically use pseudonymisation to protect the personal data of the parties prior to transmission to external consultants. In contrast, anonymised data fall out of scope, having been stripped of sufficient elements to ensure that there is no significant risk of identification, whether by the former controller, recipients or third parties.

In this respect, SRB clearly remained a controller with regard to the personal data of the parties, and thus subject to the corrective powers of the regulator. In addition the facts seem to provide a significant risk of re-identification by the consultants. The SRB could provide them with the additional identifying information upon request, if necessary for a legitimate purpose, and notably there was no contractual term prohibiting such disclosure. Finally, as the Court itself noted, '*similar but not identical comments based on the same sources [were] available on the Internet*' ([150]) which suggests that any 'reasonably competent person' (or 'motivated intruder') ([151]) would also have been able to identify the data subjects.

The consequences of the confusion between pseudonymised and anonymised data are serious for the scope of the data protection rules and for the accountability of controllers, both the sender and the recipient. If pseudonymised data automatically become anonymous once they are transferred, there would be no obligation to carry out fair and lawful processing, to provide transparency to the individuals concerned on the processing of their data, or to take appropriate measures under Chapter IV GDPR. In particular there would be no obligation to respect the GDPR's security and data breach requirements, which would seriously lower the protection of data subjects against unlawful identification by hackers or fraudsters. Finally, there would be no obligation for a recipient of pseudonymised data to respect the rules relating to international transfers under Chapter V GDPR. In light of this significant gap in protection it is fortunate that this decision has also been appealed ([152]).

4.4. Sensitive data

Articles 9 and 10 GDPR, formerly article 8 DPD, afford an enhanced level of protection to personal data '*which are, by their nature, particularly sensitive*,' per recital 51 GDPR. The case law of the CJEU, following on from an earlier ruling of the ECtHR ([153]), makes it clear that controllers should be particularly careful when processing this type of data.

([149]) See Tosoni, L., 'Article 45', in Kuner, C., Bygrave, L.A., Docksey, C. (eds.), op. cit. (footnote 91), p. 35.
([150]) *SRB v EDPS*, see footnote 144, paragraph 17.
([151]) Weitzenboeck, E.M., Lison. P., Cyndecka, M., Langford, M., op. cit. (footnote 139), p.192.
([152]) Pending Case, ED*PS v SRB*, C-413/23 P.
([153]) ECtHR judgment of 17 July 2008, *I v. Finland*, C-20511/03.

In *V. v European Parliament* ([154]), the Civil Service Tribunal of the Court of Justice found that casual sharing of information about the complainant between the doctors of two EU institutions violated both the ECHR and the EU data protection rules. The Court condemned the European Parliament to pay the complainant damages of €25,000, made up of €5,000 for loss of earnings and €20,000 for non-material damage, the first time such damages had been awarded against an EU institution. As a result, the EU institutions became much more careful how they handled health data.

The CJEU has confirmed the higher level of protection required for sensitive data. In its ruling on the draft *EU-Canada PNR* Agreement, the Court ruled that an additional, specific legal basis would be required to ground the transfer of sensitive data to the Canadian authorities ([155]). In *G.C. et al v CNIL,* it held that a search engine is required to immediately dereference sensitive data from search results when it receives a request to dereference ([156]). Most recently the Court has clarified that sensitive data may only be processed in compliance with Article 9 GDPR if it is based on one of grounds for lawful processing set forth in the 'exhaustive' list in Article 6(1) GDPR ([157]).

Finally, the ruling in *OT v VTEK* has emphasised the need to ensure that information which is not sensitive per se does not permit sensitive information to be *inferred*. In this case, the applicant and their partner were required to lodge declarations of private interests with the national Ethics Commission. In violation of the principle of data minimisation, the name of the applicant's partner was required, in addition to the relevant financial details, and the declarations of private interests were automatically placed online by the Ethics Commission.

The CJEU found, first, that the publication of such financial information on the Ethics Commission's website was disproportionate and exposed OT to a number of risks, including targeted advertising and even criminal behaviour ([158]). Publication to a smaller group of people would have been equally effective. Moreover the Court found that collecting and disclosing the spouse or partner's name could reveal ([159]) the sexual orientation of the persons concerned, and hence fell within Article 9 GDPR ([160]). The Court has also found

([154]) Judgment of the Civil Service Tribunal of 17 July 2008, *V v European Parliament*, F-46/09, ECLI:EU:F:2011:101.

([155]) *Opinion 1/15*, see footnote 40.

([156]) Judgment of the Court of Justice of 24 September 2019, *GC and others (*De-referencing of sensitive data*)*, C-136/17, ECLI:EU:C:2019:773.

([157]) *Krankenversicherung Nordrhein*, see footnote 75, paragraph 75. The ruling has put an end to the debate on whether the two provisions are cumulative, see Opinion of Advocate General Campos Sánchez-Bordona of 25 May 2023, *Krankenversicherung Nordrhein*, C-667/21, ECLI:EU:C:2023:433, paragraph 60.

([158]) *Vyriausioji tarnybinės etikos komisija*, see footnote 143, paragraphs 102-105 and 112. See also judgment of the Court of Justice of 22 November 2022, *Luxembourg Business Registers*, C-37/20 and C-601/20, EU:C:2022:912, discussed below.

([159]) Whilst Article 9(1) GDPR refers to information 'concerning' special categories of data, rather than information 'revealing' such data, this distinction was dismissed as contrary to the context, objective and purpose of the legislation, *Vyriausioji tarnybinės etikos komisija*, see footnote 143, paragraphs 121 to 127.

([160]) *Vyriausioji tarnybinės etikos komisija*, see footnote 143, paragraph 128.

that sexual orientation may be inferred from visits to certain websites or apps, the identity of which may reveal sensitive data ([161]). These rulings confirm the need to take great care in handling sensitive data.

4.5. Controller and joint controller

In the same way as the definition of personal data, the definition of controller is crucial for ensuring accountability for processing personal data.

In *Google Spain* ([162]), the search engine argued that it was based in California, outside the scope of EU law. However the CJEU found, following the Opinion of Advocate General Jääskinen, that Google operated an 'establishment', a branch or subsidiary in Spain, to sell advertising, which directed its *commercial activities* at the inhabitants. Processing in California was therefore covered by EU law because it was 'in the context of the activities' of the establishment in Spain ([163]).

Second, the Court found that Google was a 'controller' within the meaning of Article 2(d) DPD, now Article 4(7) GDPR, which defines 'controller' as the entity '*which, alone or jointly with others, determines the purposes and means of the processing of personal data*'. Google had argued that the controller with regard to information in search results is the original publisher of the information. However the Court noted that a search engine indexes such information automatically, stores it temporarily and, finally, makes it available to internet users according to a particular order of preference ([164]). Since the search engine determines the purposes and means of processing ([165]), the Court found that it is a controller in its own right, carrying out an activity additional to that of the original publisher, a newspaper, which remained a separate controller with regard to the original information in the newspaper.

Advocate General Jääskinen had advised a different approach on these points. He was generally uneasy with the '*wide interpretation given by the Court to the fundamental right to private life in a data protection context*', which he thought would '*expose any human communication by electronic means to the scrutiny by reference to this right.*' He urged the Court to '*apply a rule of reason, in other words, the principle of proportionality, in interpreting the scope of the Directive*

([161]) *Meta Platforms and others (*General terms of use of a social network*)*, see footnote 57, paragraphs 68-72. Moreover, it cannot be inferred from the mere visit to such a website or app that a user has manifestly made public the sensitive data so inferred, *Meta Platforms and others (General terms of use of a social network),* see footnote 57, paragraph 79. An 'affirmative act' by the data subject is required, '*and that he or she realised that this would be the result.*' Georgieva, L., and Kuner, C., 'Article 9. Processing of Special Categories of Personal Data', in Kuner, C., Bygrave, L.A. and Docksey, C. (eds), op. cit. (footnote 9), p. 378. In *Buivids*, see footnote 111, for example, the police were merely going about their duties, they had not posted a video themselves.

([162]) Judgment of the Court of Justice of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317.

([163]) See EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, adopted on 12 November 2019, p. 8. Revenue raising in the EU by a local establishment may be sufficient for EU law to apply.

([164]) *Google Spain and Google*, see footnote 162, paragraph 41.

([165]) It was long known that search engines make choices – see for example, Pariser, E., *The Filter Bubble: What the Internet Is Hiding from You*, Penguin, 2012.

in order to avoid unreasonable and excessive legal consequences.' In this respect he felt that the search engine was not a 'controller' within the material scope of the DPD because it is simply carrying out passive relaying.

The Court responded that the processing of personal data by a search engine '*can be distinguished from and is additional to*' that carried out by the source websites. The Court emphasised that search engines play a '*decisive role in the overall dissemination of personal information*', which internet users would not otherwise have without knowing the original web page on which those data are published. Crucially, the Court pointed out that processing by search engines is liable to affect significantly the fundamental rights to privacy and the protection of personal data, enabling any internet user to establish through search results a '*more or less detailed profile*' of the data subject concerned ([166]).

The Court therefore concluded that search engines are controllers, responsible for meeting the requirements of the Directive, in order that '*the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved*' ([167]).

For the same reason, the Court has developed the concept of joint controllership. In *Wirtschaftsakademie* ([168]), a local business academy in Germany provided educational and training services. In order to give it an internet presence and market its services, it set up a 'fan page' on Facebook. This allowed the academy to use a tool known as 'Facebook Insights' which installs Facebook behaviour tracking cookies onto users' devices and permitted the academy to receive anonymised data on users' habits and preference. It also allowed Facebook to track users of the fan page and to target advertisements at them. Neither the academy nor Facebook informed users that their personal data was being collected and used for tracking and profiling. On this basis, the Schleswig-Holstein DPA ordered the academy in November 2011 to deactivate its fan page. The order was dismissed by the German lower courts on the grounds that Facebook, not the academy, was the controller.

The CJEU ruled that the academy and Facebook were joint controllers, jointly responsible for the processing of data of visitors to the fan page. Facebook was a controller because it primarily determined the purposes and means of processing the personal data of Facebook users and other persons visiting the

([166]) *Google Spain and Google*, see footnote 162, paragraphs 36-38 and 80.

([167]) For the same reason, the CJEU found that national law had determined, at least implicitly, the purposes and means of the processing of personal data performed by the national official journal, judgment of the Court of Justice of 11 January 2024, *Etat Belge (*Processing of data by an Official Journal*)*, C-231/22, ECLI:EU:C:2024:7, paragraphs 28, 30 and 32. See also the judgments of the Court of Justice of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, paragraph 29, and of 5 December 2023, *Deutsche Wohnen*, C-807/21, EU:C:2023:950, paragraph 40 and the case-law cited.

([168]) *Wirtschaftsakademie Schleswig-Holstein*, see footnote 98. See Blanc, N., 'Wirtschaftsakademie Schleswig-Holstein: Towards a Joint Responsibility of Facebook Fan Page Administrators for Infringements to European Data Protection Law?' *EDPL*, Vol. 4, No. 1, 2018, p. 120-126. See most recently concerning controllers, processors and joint controllers, judgment *Nacionalinis visuomenės sveikatos centras*, see footnote 167.

fan page. In turn, the academy, acting as the administrator of the fan page, was acting as a controller because it contributed to determining, jointly with Facebook, the purposes and means of processing the personal data of fan page visitors. Creating the fan page involved the definition of parameters by the academy for the purpose of producing statistics based on visits to the fan page, it permitted Facebook to place cookies on fan page visitors' devices, and the academy benefited from data analytics based on these cookies. As a result, the academy had to be considered as a controller responsible for that processing jointly with Facebook, with 'even greater' responsibility with regard to the personal data of visitors who were not Facebook users ([169]).

The Court emphasised that joint controllership does not require each responsible entity to have access to the personal data concerned ([170]). Most recently the Court has added that national law may determine joint controllers ([171]) and that joint controllership may be implicitly as well as explicitly determined by national law ([172]).

For the Court, the recognition of joint responsibility '*contributes to ensuring more complete protection of the rights of persons*' ([173]) by ensuring that at the end of the day someone is responsible.

Following this landmark ruling, a particular issue remained. In effect the Court had anticipated the second sentence of Article 26(1) GDPR, which requires joint controllers to determine in a transparent manner '*their respective responsibilities for compliance with the obligations under this Regulation …by means of an arrangement between them*.' However, requiring a small controller like the academy to negotiate an arrangement with a BigTech company such as Facebook is somewhat optimistic. This was addressed in the following ruling, *Fashion ID*.

In this case, rather than using a fan page, a company operated its own website to sell its merchandise online, on which it placed a Facebook 'Like' button. This was in fact an embedded social media plug-in, which permitted Facebook to track visitors, whether or not they were Facebook users. Simply visiting the website containing such an application is sufficient to trigger the transfer of the user's data to Facebook and enable it to place tracking cookies on the user's device. The company benefited from the use of Facebook 'Insights,' as in *Wirtschaftsakademie,* and the presence of the "Like" button gave its products enhanced visibility. Once again, there was no information provided to users by Fashion ID or Facebook, nor was consent requested for placing the social media plug-in.

([169]) *Wirtschaftsakademie Schleswig-Holstein*, see footnote 98, paragraphs 34-to 41.

([170]) *Ibid*, paragraph 38. See also *Jehovan todistajat*, see footnote 98, paragraph 69; *Belgian State (*Processing of data by an Official Journal*)*, see footnote 167, paragraph 48.

([171]) See *Nacionalinis visuomenės sveikatos centras*, see footnote 167, paragraphs 40 to 43 and the case-law cited.

([172]) See *Belgian State (*Processing of data by an Official Journal*)*, see footnote 167, paragraphs 49 to 50.

([173]) *Wirtschaftsakademie Schleswig-Holstein,* see footnote 98, paragraph 42.

Advocate General Bobek pointed out that there was a need to enhance the precision of the notion of joint controller, because otherwise the '*effective protection of something tends to dramatically decrease if everyone is made responsible for it*.' Reality must play a role, including '*issues of knowledge and genuine bargaining power and the ability to influence* ([174]) *any of the imputed* activities' ([175]).

The Court found that there was a joint controllership of Facebook and Fashion ID, but clarified that Fashion ID was only a joint controller for the activities where it effectively codetermined the means and purposes of the processing, that is for operations over which it can exert control, i.e. the collection & transmission of the personal data. Fashion ID was responsible for providing information to users and obtaining any necessary consent. However, Fashion ID had no control over the analysis and further processing of the personal data by Facebook, for which Facebook alone is responsible, together with, in consequence, ensuring the rights of access and rectification ([176]).

The academic literature is divided over the broad approach by the Court. Some feel the sharing of responsibilities may create uncertainty and weaken protection ([177]), others are 'not convinced' that the CJEU has in fact allowed Fashion ID to 'cut corners' in respecting its obligations ([178]). Perhaps the real problem in this case law was the ten years taken to enforce the DPA order to Wirtschaftsakademie in November 2011 to deactivate the fan page, which was finally enforced by the national courts in November 2021 ([179]).

4.6. Consent

Consent is defined in Article 4(11) GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes. In a series of cases the Court has taken a firm position on the meaning of specific, informed and unambiguous consent, but has not come to a definitive conclusion on what constitutes freely given consent.

In *Planet49* ([180]), a German online store invited visitors to participate in a lottery to win a laptop, subject to a checkbox which was open, but had to be checked by users both to participate in the lottery and to consent to receiving promotional

([174]) The ability to exert a *decisive* influence over processing has been suggested as a requirement for an entity to be considered as a joint controller, see Wong, B., 'Problems with controller-based responsibility in EU data protection law', *IDPL*, Vol. 11, No. 4, 2021, p. 380.

([175]) *Wirtschaftsakademie Schleswig-Holstein*, see footnote 98, Opinion of Advocate General Bobek of 19 December 2018, *Fashion ID*, ECLI:EU:C:2018:1039, paragraphs 92 and 93.

([176]) The EDPB has issued Guidelines on the concepts of controller and processor in the GDPR, Version 2.1, adopted 7 July 2021, which take account in particular of the recent case law.

([177]) Millard, C., 'At this rate, everyone will be a [joint] controller of personal data!', *IDPL*, Vol. 9, No. 4, 2019, p. 217 at p. 219; Finck, M., 'Cobwebs of control: the two imaginations of the data controller in EU law', *IDPL*, Vol. 11, No. 4, 2021, p. 338.

([178]) Bygrave, L.A., and Tosoni, L., 'Article 4(7) Controller', in Kuner, C., Bygrave, L.A., Docksey, C. (eds.), op. cit. (footnote 91), p. 39.

([179]) Urteil des OVG Schleswig vom 25.11.2021, 4 LB 20/13.

([180]) Judgment of the Court of Justice of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801.

offers, and a second checkbox which had already been checked, indicating consent to the installation of cookies, which users had to uncheck to refuse consent. The German federal consumer association challenged the validity of consent in these two checkboxes and requested an injunction.

The Court found that there was no valid consent in this case. The pre-checked checkbox did not constitute *active* consent ([181]), nor did the checking of the open checkbox constitute *specific* consent to the purpose of advertising bundled with participation in the lottery ([182]).

In addition, the Court ruled that users should be able to determine easily the consequences of any consent. A website must therefore inform the user of the duration of the operation of the cookies that are used and the extent to which third parties are given access to the cookies ([183]). Advocate General Szpunar added that '*if third parties have access [to the cookies], their identity must be disclosed*' ([184]) and emphasised the obligation to fully inform data subjects before seeking their consent online ([185]).

The Court did not discuss the fourth element of consent, whether it has been freely given, since this had not been raised by the referring court ([186]), nor did it pronounce on the *monetisation* of personal data, even though the Advocate General had recommended accepting the 'selling' of access to content using personal data.

This left open the question whether freely given consent is consistent with so-called 'cookie walls,' the practice of conditioning access to a service on users' acceptance of cookies on their devices, in effect on their accepting tracking and profiling.

Following the ruling in *Planet49*, the EDPB updated its advice on consent with regard to 'cookie walls,' advising that:

> *'In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls)' ([187]).*

([181]) See recital 32 GDPR, which adds that *'(s)ilence, pre-ticked boxes or inactivity should not … constitute consent'* and that, where there are multiple purposes, consent should be given for all of them.

([182]) *Planet49*, see footnote 180, paragraphs 50 to 63.

([183]) *Ibid*, paragraphs 74 to 80.

([184]) See also the Opinion of Advocate General Pitruzzella of 9 June 2022, *Österreichische Post (*Information regarding the recipients of personal data*)*, C-154/21, ECLI:EU:C:2022:452, point 32.

([185]) Opinion of Advocate General Szpunar of 21 March 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:246, points 180 and 67.

([186]) *Planet49*, see footnote 180, paragraph 64.

([187]) EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Section on Conditionality, adopted on 4 May 2020, paragraphs 38-41.

However, when the French DPA, the CNIL, sought to follow the EDPB guidance at national level, the Conseil d'Etat found that the CNIL could not legally prohibit the practice of blocking access to a website if cookies are refused ([188]). The CNIL therefore accepted the practice of cookie walls, subject however to fully informed consent to cookies and the existence of a reasonable and satisfactory alternative, such as paid access, if consent is refused ([189]).

In *Orange România* ([190]), the CJEU continued to stress the need for fully informed consent as a requisite for consent to be freely given. A telecoms company had the practice in its stores of taking a copy of the identity documents of customers when concluding SIM contracts, which included a clause that the customers had been informed of, and had consented to, the taking of that copy. However the consent box in the paper contract was checked by the sales agent, not the customer, and it was not clear to customers that the contract could still be concluded even if they refused consent. Finally, customers who refused consent to their identity document being copied were required to sign a specific form declaring that they did not consent.

The Court confirmed that consent had not validly been obtained in the case of silence, pre-ticked boxes or inactivity. It stressed that data subjects must enjoy 'genuine freedom of choice', which meant that contractual terms must not mislead the data subject as to the possibility of concluding the contract if consent is refused. Finally, the additional requirement to declare refusal of consent in handwriting was liable to affect unduly the freedom to choose whether to consent.

Most recently, in *Meta Platforms v BKA*, the CJEU in effect limited the operator to using consent as the legal basis for its processing of Facebook users' data, rather than other legal bases ([191]). In this respect, the Court found that the fact that a controller holds a dominant position on the market concerned does not, as such, preclude freely given consent by the users of its service. However, a dominant position is liable to affect the freedom of choice of its users, who might be unable to refuse or withdraw consent without detriment, and must therefore be taken into consideration in assessing whether users have freely given their consent.

The Court concluded with a finding that has set the stage for further litigation. Facebook users must be free to refuse individually to give their consent to particular data processing operations which are not necessary for the performance of the contract,

> *without being obliged to* ***refrain entirely*** *from using the service offered by the online social network operator, which means that those users*

([188]) Decision of 19 June 2020 of the Conseil d'Etat, No. 434684, ECLI:FR:CECHR:2020:434684.20200619.

([189]) CNIL, Cookie walls : la CNIL publie des premiers critères d'évaluation, 16 May 2022.

([190]) Judgment of the Court of Justice of 11 November 2020, *Orange România SA*, C-61/19, ECLI:EU:C:2020:901.

([191]) *Meta Platforms and others (*General terms of use of a social network*)*, see footnote 57, paragraphs 127 to 139.

> *are to be **offered**, if **necessary** for an **appropriate fee**, an **equivalent alternative** not accompanied by such data processing operations (emphasis supplied) ([192]).*

Following this ruling, Meta has decided to impose a 'subscription for no ads' choice upon users of Facebook and Instagram ([193]), otherwise known as 'pay or ok'. EEA users may either consent to Meta tracking and profiling or pay a monthly sum to use the service free of such processing. Meta claims that this system conforms to the CJEU ruling, but its high calculation of the amount demanded will be closely scrutinised. Moreover, in view of the imbalance of power between Meta and its users, and its dominant market position, the Court will undoubtedly be seised in due course of the question whether the subscription fee is a 'reasonable alternative' under data protection law or whether it is an abuse of a dominant position under competition law, taking data protection law into account. There is no doubt that the *Meta* ruling, followed by the launching by a commercial operator *itself* of a 'pay-with-money-not-data option' heralds a significant change in the data protection ecosystem ([194]).

5. Balancing fundamental rights

5.1. Freedom of religion

The landmark ruling in *Jehovan todistajat* ([195]) illustrates the approach of the CJEU to balancing and reconciling the fundamental rights enshrined in the Charter, together with its accountability approach to definitions and exceptions and the interaction between the Luxembourg and Strasbourg jurisdictions.

In this case, volunteers from the Jehovah's Witnesses community in Finland carried out door-to-door evangelising and kept paper notes of their religious conversations with the persons visited and their attitudes. In 2013, the Data Protection Board prohibited the community and its members from taking such notes without the consent of the discussion partner or in violation of the data protection rules. In response the community claimed that this decision interfered with their freedom of religion, their evangelising fell within the household exception, the keeping of the paper notes did not constitute processing of personal data, and the preaching fell within the household exception because it took place in private households (or on their thresholds).

([192]) *Ibid*, paragraph 150.

([193]) Meta, Facebook and Instagram to Offer Subscription for No Ads in Europe, 20 October 2023.

([194]) See Kuner, C., Cate, F.H., Lynsky, O., Millard C., Ni Loideain, N., and Svantesson, D., 'If the legislature had been serious about data privacy…', *IDPL*, Vol. 9, No. 2, 2019, p. 77.

([195]) See Gellert, R., 'Door-to-Door Preaching by Jehovah's Witnesses Community Falls under Data Protection Law', *EDPL*, Vol. 4, No. 3, 2018, p. 391 – 395.

The CJEU affirmed that freedom of religion is a fundamental right under Article 10 of the Charter, which is *respected* and *not prejudiced* under the Treaty (Article 17 TFEU) and the GDPR (recital 165). However it is not *exempted* from respect for other fundamental rights, so that, whilst the volunteers had the right to evangelise, they had to process personal data lawfully when doing so. Moreover, subjecting the preaching activity to compliance with the data protection rules does not constitute an intolerable or disproportionate interference with the freedom to preach. The taking of notes and their transmission within the religious community is in no way of the same nature as preaching.

The ruling also affirms that the activities excluded from the scope of the legislation in what is now article 2(2) GDPR, must be strictly construed because they delimit the scope of the data protection rules. The Court found that preaching is not a household activity merely because volunteers may enter the homes of the 'visited' persons from time to time.

The Court confirmed that it is not required that each of the controllers must have access to (all of) the personal data concerned. Thus, the religious community could be a joint controller even in cases where the community itself apparently had no access to the collected data in question. It was enough that the preaching activity, in the course of which personal data was apparently being collected, was influenced and organised by the community itself ([196]).

Finally, this is the first and only ruling on manual processing under the data protection rules. The Court found that the notes taken by members formed part of a 'filing system' under Article 2(c) DPD, now Article 2(1) GDPR. Advocate General Mengozzi observed that the paper notes were filed by geographical area, the member himself, the persons visited – their name, address and a summary of the conversation, in particular concerning their religious beliefs and family circumstances. He concluded that *'(s)uch a structure, even if not sophisticated, allows easy access to the data collected'* ([197]), echoing the explanation in recital 15 DPD. The Court agreed that the concept of a 'filing system' covers the collection of such data if those data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use. Both these criteria were set forth in recital 15 DPD, whereas recital 15 GDPR only refers to the need for there to be specific criteria. The Court's ruling suggests that the useful criteria in the DPD will be retained.

The case was subsequently heard by the ECtHR, which found that the rights of the applicant community had been correctly balanced against the rights of individuals whose data was being taken. In consequence there had been no

([196]) *Jehovan todistajat*, see footnote 98, paragraphs 68 to 72. Affirmed and applied in judgment of the Court of Justice of 7 March 2024, IAB Europe, C-604/22, EU:C2024:214, paragraphs 57 to 58 and 64 to 69.

([197]) Opinion of Advocate General Mengozzi of 1 February 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:57, point 57.

violation of the community's right to freedom of thought, conscience and religion under Article 9 ECHR ([198]). This was the second case to be heard by the ECtHR following a preliminary ruling by the CJEU. The earlier case, *Satamedia* ([199]), also from Finland, concerned the balancing between the rights to private life and data protection on the one hand and freedom of expression on the other. In the same way the ECtHR found that the national court, implementing the preliminary ruling by the CJEU, had correctly balanced the rights concerned.

5.2. The right to be forgotten and freedom of information

In *Google Spain* ([200]), Mr Costeja complained against the continued publication of a 1998 newspaper auction notice for unpaid debts. He requested its erasure by Google Spain, Google Inc and by the newspaper. As noted above, the CJEU determined that the processing fell within the territorial and material scope of the legislation.

The ruling also imposed the responsibility on search engines to remove links to web pages displayed after a search on person's name, the so-called 'right to be forgotten' ([201]).

Advocate General Jääskinen had advised the Court that there was no general right to be forgotten. He felt that there was no '*positive obligation on the EU and the Member States*' to enforce such a right against internet search engine service providers, which are private subjects. The information in question had been lawfully processed and it was neither incomplete nor inaccurate. He made two more points which remain subjects of discussion. First, he counselled against falsifying history or compromising the right to information, which has become an issue after recent rulings by the ECtHR modifying its protective approach to the press ([202]). Second, he wanted to '*discourage the Court from concluding that these conflicting interests could satisfactorily be balanced in individual cases on a case-by-case basis, with the judgment to be left to the internet search engine service provider*' ([203]).

([198]) ECtHR judgment of 9 May 2023, *Jehovah's Witnesses v. Finland*, no. 31172/19

([199]) ECtHR judgment of 27 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, no. 931/13

([200]) *Google Spain and Google,* see footnote 162.

([201]) Characterised more precisely as the 'right to suppression' of links to search engine results, see Kuner, C., 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines' in: Hess, B., Mariottini, M.,C. (eds.), *Protecting Privacy in Private International and Procedural Law and by Data Protection 19-55* , LSE Legal Studies Working Paper No. 3/2015, p. 7.

([202]) See Docksey, C., Journalism on trial and the right to be forgotten, *Verfassungsblog*, 9 March 2022.

([203]) *Google Spain and Google*, see footnote 162, paragraphs 129 to 133. It remains questionable whether it is appropriate for search engines themselves to carry out the balancing between individual requests and the interests of publishers and the wider public, see the Report of the Advisory Council to Google on the Right to be Forgotten, including comments by experts consulted and dissenting comments by individual members.

However his advice would have left a gap in the protection of data subjects, and in this landmark ruling the CJEU applied the right to be forgotten under the DPD ([204]).

The right to be forgotten requires a balancing between privacy and data protection and other fundamental rights and interests such as those expressed in recital 4 GDPR. The Court therefore turned its attention to Article 7(f) DPD, the so-called 'balancing clause' (now Article 6(1)(f) GDPR) between the rights and interests of the controller and the data subject. There were in fact three interests to weigh in the balance with the fundamental rights to privacy and data protection under Articles 7 and 8 of the Charter: the freedom of the search engine operator to conduct a business under Article 16 of the Charter, and freedom of information and freedom of expression of the internet user, both in Article 11 of the Charter.

First, the Court weighed the economic interest of the search engine operator, based on its freedom to conduct a business. Since the activity of search engines is liable significantly to affect the fundamental rights to privacy and data protection, the Court found that this merely economic interest was not enough to justify interference with those rights.

The Court then considered how to find a 'fair balance' between the legitimate interests of third parties such as internet users potentially interested in having access to information, and the data subject's fundamental rights. In this case, in the absence of such a specific public interest to weigh in the balance, the Court held that the search engine had to delist links to web pages resulting from a search on a person's name if inclusion of those links at that point of time was inadequate, irrelevant, no longer relevant, or excessive. As a result, although the information in question had indeed been lawfully processed and was neither incomplete nor inaccurate, it had to be delisted because it was no longer relevant and quite misleading.

A number of questions arose after the *Google Spain* ruling. First, the nature of the public interest that may override the right to be forgotten. Many of these have now been set forth in Article 17(3) GDPR on the right to erasure, in particular the right of freedom of expression and information.

Second, the Court considered the territorial scope of the obligation to remove links. In *Google v CNIL,* ([205]), the CNIL ordered Google to apply de-referencing across all its domains, both inside and outside the EU. The CJEU followed a pragmatic 'European de-referencing' solution whereby de-referencing should apply across the whole EU, and not solely to the Member State where the search

([204]) It has been argued that the right to be forgotten has deep roots within data protection in Europe and its basic statutory underpinnings are present in the great majority of G20 countries, see Erdos, D., and Gartska, K., 'The 'right to be forgotten' online within G20 statutory data protection frameworks', *IDPL*, Vol. 10, No. 4, 2020, p. 297 and 308.

([205]) *Google (*Territorial scope of de-referencing*)*, see footnote 14. This case arose following the ruling on jurisdiction and the right to be forgotten in *Google Spain*, discussed above.

request is made. In addition, search engines should make use of geo-blocking technology to remove data from the results of searches apparently located outside the EU but in fact located within the jurisdiction. The Court recognised that a global de-referencing approach would meet in full the objective of guaranteeing a high level of protection of personal data throughout the EU, due to the global nature of the internet. Whilst EU law does not presently require or accept global scope in this area ([206]), it would justify the existence of a competence on the part of the EU legislature to lay down such an obligation.

The Court added that EU law neither requires nor prohibits de-referencing outside the EU. In consequence global de-referencing would be permissible under national law ([207]). In view of the risk of fragmentation threatening the unity of EU law the Court referred to its rulings in *Åkerberg Fransson* and *Melloni* ([208]), in which it had laid down the proviso that '*the level of protection provided for by the Charter … and the primacy, unity and effectiveness of European Union law are not thereby compromised*' ([209]).

Third, the Court considered the burden of proof where a request for dereferencing is based on the claim that the information is false. The '*dereferencing of allegedly inaccurate content*' ruling concerned a couple who were involved in various financial services and investment companies. A website published three articles in April and June 2015 criticising the investment model of those companies together with photographs of the complainants suggesting that they were enjoying a life of externally financed luxury. The plaintiffs asked Google to dereference the articles and images from search results because they were incorrect and defamatory. Google refused the request, referring to the professional context of the articles and photos and the right of the public to know, and arguing that it did not know whether the information in the articles was true or not.

The Court focused on two basic principles. On the one hand, the right to be forgotten should not be applied where the personal data concerned are necessary for freedom of information ([210]), *per* Article 17(3). On the other hand, there is no right to freedom of inaccurate or false information. The Court was faced with two contrasting views on how to resolve these issues. The referring court felt that the data subject should bear the burden of obtaining an interim

([206]) See also the Opinion of Advocate General Szpunar of 10 January 2019, *Google (*Territorial scope of de-referencing*)*, ECLI:EU:C:2019:15, points 50-61.

([207]) *Ibid*, point 72. In the event, the Conseil d'Etat held that there was no statutory authorisation under French law for extraterritorial jurisdiction by the CNIL: Conseil d'Etat, section du contentieux, 10ème et 9ème ch. réunies, décision du 27 mars 2020.

([208]) Judgments of the Court of Justice of 26 February 2013, *Åkerberg Fransson*, C-617/10,EU:C:2013:105, paragraph 29, and *Melloni*, C-399/11, EU:C:2013:107, paragraph 60.

([209]) However the CJEU omitted to actually use this phrase in the ruling, which is 'puzzling,' see Kranenborg, H., 'Article 17', in Kuner, C., Bygrave, L.A., Docksey, C. (eds.), op. cit. (footnote 91), p. 95.

([210]) Judgment of the Court of Justice of 8 December 2022, *Google (*dereferencing of allegedly inaccurate content*)*, C-460/20, ECLI:EU:C:2022:962. See also the Opinion of Advocate General Pitruzella of 7 April 2022, *Google (dereferencing of allegedly inaccurate content)*, C-460/20, ECLI:EU:C:2022:271, point 27, and the judgment of the Court of Justice of 9 March 2017, *Manni*, C-398/15, EU:C:2017:197, paragraph 42.

order from a court against the content provider, whereas Advocate General Pitruzella ([211]) suggested a solution of 'procedural data due process' or 'procedural fairness', whereby, the data subject bears the burden of providing prima facie evidence of the false nature of the information at issue. The search engine should then carry out checks to confirm or disprove the evidence provided, and even, if possible, initiate rapidly an adversarial debate with the web publisher. The Court agreed with the lighter approach suggested by the Advocate General, i.e. there is no need to obtain a judicial decision, but felt that a search engine cannot be required to actively investigate the facts or organise an adversarial debate with the website. It therefore imposed an intermediate burden of proof, to establish the 'manifest inaccuracy' of the information, based on evidence that the data subject can reasonably be required to try to find. Faced with such relevant and sufficient evidence, the search operator must accede to the request.

Finally, the CJEU has addressed the situation where a directive has laid down the requirement to publish personal information in the public interest. *Luxembourg Business Registers*, concerned the amended anti money-laundering directive ([212]), which requires Member States to keep a register containing information on the beneficial ownership of companies incorporated within their territory, for the purposes of combating and preventing money laundering and terrorist financing. Access to the register was originally limited to public authorities and entities demonstrating a 'legitimate interest' but the directive was amended to require that any member of the general public should have access to the register, subject to the safeguard that beneficial owners could request access to be restricted in 'exceptional circumstances', defined as '*disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation*'. Notwithstanding this safeguard, some data subjects complained that publishing the information on their beneficial ownership made it dangerous for them to travel to certain countries in view of the danger of kidnapping or violence ([213]).

The Council and the Commission argued that the general public's free access to information on beneficial ownership had a deterrent effect, enabled greater scrutiny, and facilitated the conduct of investigations, including those carried out by the authorities of third countries, and that these objectives could not be achieved by a less intrusive means.

The EDPS intervened to argue, contra, that the EU legislator had not actually demonstrated that public access was more effective than less intrusive scrutiny by public authorities and organisations with a legitimate interest in such access.

([211]) Opinion of Advocate General Pitruzella, *Google (*dereferencing of allegedly inaccurate content*)*, see footnote 210, point 44.

([212]) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU,OJ L 156, 19.6.2018, p. 43.

([213]) *Vyriausioji tarnybinės etikos komisija*, see footnote 143.

The objective of transparency was ill-defined and was insufficient to justify the serious interference with the fundamental right to data protection in the absence of proof of its necessity and proportionality ([214]).

The Court held that opening the register to free public access was a more serious interference than the previous system, and was neither strictly necessary nor proportionate to the objective pursued.

The ruling was severely criticised by NGOs as weakening the anti-corruption legislation by removing the greater transparency enabled by public access to beneficial ownership information. There was also the risk that national differences in the definition of legitimate interest might lead to excessive limitations on access to the information on beneficial ownership. The Court specifically addressed this risk by noting that '*both the press and civil society organisations that are connected with the prevention and combating of money laundering and terrorist financing have a legitimate interest in accessing information on beneficial ownership*' ([215]). As a result the investigative journalists and anti-corruption organisations concerned should still be able to access the beneficial ownership data.

There is no doubt that public access made it easier for NGOs to access the register, particularly in view of national differences but the issue for the Court was that a less intrusive solution did exist which should be applied more effectively. As in *OT*, the Court had no sympathy with easy solutions that failed to respect the rights enshrined in the Charter, and so declared invalid the amendment in the 2018 directive introducing public access ([216]). As the U.S. Supreme Court declared in *Riley v California*: '*Privacy comes at a cost*' ([217]).

6. Conclusion

The CJEU has played a significant role in shaping the development of EU law on data protection. It has filled gaps, tightened definitions, provided significant support for the developing governance of data protection, and endeavoured to keep the law relevant and up to date. DPAs have played a significant role in the case law, as plaintiffs, intervenors and, increasingly, as defendants. The Court has been criticised for going too far in some cases, even by its own Advocates General. But we can be grateful for its commitment to ensure the *effective and complete protection* of the fundamental rights to privacy and data protection.

([214]) EDPS pleading at the hearing of the Court in Joined Cases C-37/20 (Luxembourg Business Registers) and C-601/20 (SOVIM), 19 October 2021.

([215]) *Luxembourg Business Registers*, see footnote 158, paragraph 74.

([216]) See also the ECtHR judgment of 9 March 2023, *L.B. v. Hungary*, no. 36345/16, in which the ECtHR found that a legislative requirement to publish on the internet the names and home addresses of tax debtors had not considered the additional value of such publication nor taken account of the Convention rights of the individuals concerned.

([217]) 573 U.S. 373 (2014)

20

20th Chapter for the 20th Anniversary

Wojciech Wiewiórowski

20th Chapter for the 20th Anniversary

Wojciech Wiewiórowski (*)

In writing what is to be the final chapter of this book, I have the tricky task of sharing ideas and thoughts for the future: for the EDPS and for data protection. The problem with predicting the future is that you are almost always wrong. That, in itself, is not that much of an issue as long as no-one remembers what you once said. It is much worse, however, when your 'wisdom' is written down in the book like this one and everybody can read it many years later!

I would therefore try to turn predictions into wishes – wishes of the EDPS, and data protection at large, could hopefully build on; wishes that could carry us (the EDPS and data protection as such) into the unknown, and motivate us.

1. Embrace change

When data protection laws emerged in the 1970s, they were largely a reaction to the growth of computerisation and, linked to that, large databases that were made possible due to technological developments. Since then, every decade has brought more innovation, and each decade has been 'faster' than the previous one. In this context, data protection has, from its beginnings, been developed in a rapidly changing environment, remaining nevertheless relatively stable in terms of basic principles and concepts.

I know, it is a cliché, but it is obvious that the world is always changing and the process of evolution accelerates. If the world today is changing more than yesterday, it only means that tomorrow it will change even faster. Exponential increase of the speed of change is the only thing that does not change. I wish for us to embrace the change and be able to drive it.

(*) European Data Protection Supervisor (2019-2024)

The next 20 years will only magnify the challenges and struggles of data protection, while our successes of the last 20 years will gradually mean less and less. I, however, see the EDPS as an institution that has managed, due to incredible people that have been working there to continuously advance the world of data protection, to rethink concepts and to bring new perspectives.

The EDPS is already embracing change in many ways: through our strategies, through our focus on foresight and technology monitoring, through our constant engagement with civil society, academia, experts, technologists, and industry. This might, however, not be enough, which brings me to the second wish.

2. Avoid reactiveness

Data protection, as any regulated field, is naturally prone to being always one-step behind, always slightly late. To a certain extent there is nothing wrong with that – the history of regulation is a history of reactiveness. But data protection should not, and I hope that the EDPS never does, remain comfortable in a reactive mode – of waiting for and replying to complaints, of lamenting dangerous developments, of expecting more resources to do the same, only more.

The risks of reactiveness of data protection is somewhat exacerbated by its nature: by being applicable to such a wide spectrum of human activity, it risks being seen as the 'law of everything'. But it cannot fall into such a trap, for it will become a law of nothing, to the detriment of fundamental rights and principles it aims to protect. On the contrary, we need to think strategically about the biggest challenges of our time, for example in light of the scale of the impact on people, or in the light of the responsibility the actions of some major players may have on people's liberties and rights, and address them meaningfully. I wish for us to pick wisely our battles and win them.

We should invest as much time in being proactive as we spend being reactive. We need to proactively imagine the future we want to live in, and pursue this future by crafting actions and rules that contribute meaningfully to more just, and fairer, societies based on freedoms and the protection of rights for everyone, especially the most vulnerable.

3. Bring data protection to people

Data protection can be perceived as difficult and surely it can be somewhat technical. However, being a fundamental right, it speaks to the core and heart of people's lives. And yet, we encounter issues in making our actions go through.

There is perhaps tension between the societal impacts of today's large scale data processing and the philosophy of data protection which is in part individual-centric, empowering the data subject to be in control. If in this tension one might see data protection as making a false promise to citizens, it should only be a source of motivation, for the EDPS, for data protection authorities, for data protection community, to turn these promises into a set of tools at the disposal of large groups of individuals.

The GDPR has already achieved a lot in this regard – being probably one of the most known EU laws among citizens of EU Member States. But, it is still far from fulfilling its potential. And it will not, unless it is being used by many. It is our task to make it happen.

On the 20th anniversary of the EDPS, I wish for us to find ways to make data protection resonate more with individuals. Including by critically rethinking ourselves and letting new people bring new ideas.

4. See beyond data protection laws

One of the lessons from the 20 years of the EDPS is how crucial it is for a data protection authority to possess knowledge of multiple areas that data protection engages with. From competition law to consumer protection. From large scale IT systems, to electronic communication. From media regulation to financial laws.

Data protection is a fundamental right, but it is also is an area of law. An area being part of a broader legal system. As such, it needs to be able to engage with other fields, otherwise we will miss the possibility to actually understand our world. Let me clear about this. If data protection does not engage with all sorts of relevant realities and other fields of law, there will no longer be any data protection.

I wish for us to understand that data protection is broader than a sectorial application of the law, and critically pursue a dimension of integration of policies and different fields of law.

5. Reinforce the European way

There is an especially important notion in the 'EDPS' acronym: European. 20 years of the EDPS have been dedicated to a large extent to advocating an EU-wide data protection framework, and to promote its model globally.

While we should be open and respectful to other cultures' understanding of privacy – which can differ from the European meaning – Europe needs to lead globally. It needs to face and overcome challenges, and pave the way for new ideas. By doing this, it needs to nurture its values, for they are fragile and easy to destroy. I wish for us to see and make data protection as an enabler for a modern and open-minded global presence of Europe, and European Union in particular. It is in our hands.

When I read these wishes of mine, I look back on the 20 years of the EDPS, proud of how much these ideas and hopes were something that the EDPS deeply cared about. And I am optimistic about the future, knowing that the EDPS will continue to shape the world of data protection and beyond.

Looking back: a photographic timeline

2000

18 December 2000

A data protection regulation for EUIs: Regulation (EC) 45/2001

© Photo by Guillaume Périgois on Unsplash

This Regulation aims to legislate how EU institutions, bodies, offices and agencies (EUIs) process individuals' personal data. Importantly, with this Regulation, the European Data Protection Supervisor is created and designated as the independent data protection authority in charge of supervising the way EUIs process personal data. The EDPS is provided with specific tasks and powers to do so.

2004

17 January 2004

Peter Hustinx is appointed as European Data Protection Supervisor and Joaquín Bayo Delgado is appointed as Assistant Supervisor

© European Data Protection Supervisor

"Developing from a very modest start, the EDPS was able to exercise considerable influence by concentrating on three main roles – supervision, consultation, and cooperation – and by emphasising that effective data protection should be seen as a condition for success. In this way, the first ten years provided the basis for how the EDPS is operating today."

Peter Hustinx
EDPS (2004-2014)

"At the beginning of the EDPS in January 2004, there were three main challenges: to set up the new institution, to organise its tasks as data protection supervisory authority of the EU and to define and start its functions as advisory body on data protection matters".

Joaquín Bayo Delgado
Assistant Supervisor (2004-2008)

2005

March 2004

First EDPS-DPO meeting

© European Data Protection Supervisor, Archives 2007

"In the early days of Regulation 45/2001, data protection in EU institutions was still confined to a handful of interested persons. It took several years to build a genuine culture of compliance and to convince that data protection was an asset rather than an obstacle for an organisation. This was made possible thanks to the close cooperation and constant support of the EDPS. And by EDPS I mean of course the full team!"

Philippe Renaudière
EU Commission Data Protection Officer (2006-2018)

13 September 2005

First EDPS workshop on data protection with International Organisations – *in cooperation with the Council of Europe and the Organisation for Economic Cooperation and Development*

© European Data Protection Supervisor

"Data protection is a crucial aspect of protecting the lives and dignity of people affected by armed conflicts. The ICRC is honoured to collaborate with the EDPS in fostering better norms and practices among humanitarian and international organisations through the workshops on Data Protection within International Organisations."

Massimo Marelli
Head of the Data Protection Office at the International Committee of the Red Cross

18 October 2005

First EDPS intervention at the Court of Justice of the EU (*Parliament / Council, Joined Cases C-317/04 and C-318/04*)

© iStock.com/arsenisspyros

Hielke Hijmans
Co-founder of the EDPS Policy and Consultation Unit

"I consider the fact that the Court allowed the EDPS to intervene in the PNR-case to be a first big success of the EDPS, in the early days of becoming a serious player. I am still proud that we managed to convince the Court, without any precedent for such intervention under EU law."

Veronica Maria Perez Asinari
Former Head of Unit, EDPS Supervision and Enforcement

"The PNR case brought law enforcement into the international data protection debate, which until that moment was mainly focused on private sector aspects. While the judgement did not analyse the data protection issues we raised in the pleading, it paved the way for many other leading cases in the field. It was an honour for me to represent the EDPS before the Court of Justice of the European Union."

2006

25 November 2005

EDPS joins the Article 29 Working Party

© European Data Protection Supervisor, Archives 2012

"Since 2004, the newly appointed EDPS, Peter Hustinx, had been a member of the Article 29 Working Group. The challenges were enormous, especially with regard to the integration of the ten states that joined the European Union on 1 May 2004. The EDPS played an important role in this work."

Peter Schaar
Chairman of the Article 29 Working Party (2004-2007)

28 January 2006

EDPS gains public recognition

© European Data Protection Supervisor

With the creation of a new website and logo, the EDPS initiates a variety of outreach activities to bring its work closer to the public. This includes participating in the EU Open Days, a tradition still perpetuated today.

2007

4 April 2007

Prüm Treaty

© Stadt Prüm

The EDPS plays a substantial role in the area of freedom, security and justice. Amongst its work, the EDPS presents an Opinion on the Treaty of Prüm, a piece of legislation, applicable throughout the EU, that aims to step up cross-border cooperation, to combat terrorism and cross-border crime.

12-13 October 2007

EDPS attends the first CPDP conference

© CPDP Computers, Privacy and Data Protection conference

The first Computers, Privacy and Data Protection Conference, or CPDP, is launched. A global platform at the heart of Brussels. An international forum in which the EDPS has actively participated since its creation to this date with the aim to further advance cooperation between legal, regulatory, academic and technological fields in order to enhance privacy and data protection standards.

2008

23 December 2008

Peter Hustinx is reappointed as European Data Protection Supervisor and Giovanni Buttarelli is appointed as Assistant Supervisor

© European Data Protection Supervisor

"Fundamental rights and freedoms, such as the respect for private life and protection of personal data can only become a reality if they are delivered in practice, both in the information systems of Community institutions and bodies, and in the adoption of new rules and policies that have an impact on the protection of personal data. Thank you to the European Parliament and the Council for their confidence in reappointing me for the second term and for appointing Giovanni Buttarelli as the new Assistant Supervisor."

Peter Hustinx
EDPS (2004-2014)

2009

25 November 2009

Update of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive)

© European Union

"The protection of terminal equipment is the guardian of individual privacy in the vast realm of electronic communications. In the EU, we are committed to safeguarding this gateway to the digital landscape, preserving the essence of personal freedom and trust in the connected world."

Stavros Lambrinidis
EU Ambassador to the United Nations; European Parliament Rapporteur on 'Strengthening Security and Fundamental Freedoms on the Internet' (2009)

2011

1 December 2009

Treaty of Lisbon enters into force

© European Union

"After years of dreaming of its own constitution, the EU got the Lisbon Treaty, which nevertheless triggered remarkable change. The EU Charter became legally binding and Article 16 TFEU asserted the existence of a right to data protection, which suddenly was not only once, but twice! at the highest level of EU law."

Prof. Dr. Gloria González Fuster
Research Professor at the Vrije Universiteit Brussel (VUB)

5 April 2011

EDPS organises the Spring Conference

© European Data Protection Supervisor, Archives 2015

The EDPS organises the annual Spring Conference that brings together data protection authorities from Europe to discuss matters of common interest and to exchange information and experiences.
The conference focuses on the legal developments, such as the Lisbon Treaty, EU legal framework, Convention 108, and the Area of Freedom, Security and Justice.

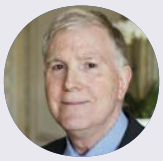
2012

16 November 2011

Appointment of Christopher Docksey as Director

© European Data Protection Supervisor

"In 2010 the Supervisor Peter Hustinx remodelled the Secretariat to have more impact. I was honoured to be appointed as Director to lead the change. It was a challenging, stimulating and exciting time, I was very happy to be a part of it."



Christopher Docksey
EDPS Director (2011-2018)

25 January 2012

Proposal for a General Data Protection Regulation (GDPR)

© European Union

"The Treaty of Lisbon and the Charter of Fundamental Rights made the protection of personal data a legal obligation. At a time of huge digital changes, I proposed modernised EU rules that would protect citizens and reign in the data-industry. The GDPR has become a global standard and serves as the basis for future regulations in the technological environment."

Viviane Reding
Former Vice-President and Commissioner for Justice of the European Commission

2013

1 April 2012

Expanding our institution

© European Data Protection Supervisor

A new sector, Information and Technology Policy (IT Policy Unit), is created in the organisation, to focus on the impact of technologies on data protection. Similarly, other organisational changes are made within the previously created units (S&E, P&C and HRBA), namely head of activities are created. The EDPS now counts more than 52 privacy professionals and other experts working to protect individuals and their personal data.

9 July 2013

First EDPS pleadings in a preliminary reference procedure before the CJEU

© European Data Protection Supervisor

The EDPS makes oral pleadings at the hearing before the Grand Chamber of the Court of Justice of the EU in joined preliminary references C-293/12 and C-594/12 Digital Rights Ireland and Others. Both cases concern the validity of the Data Retention Directive 2006/24/EC. It is the first time that the Court decides, on the basis of Article 24 of its Statute, to invite the EDPS to attend a hearing in a preliminary reference procedure, to provide answers to specific questions.

2014

12 November 2013

EDPS receives the first European Data Protection Award from the Confederation of European Data Protection Organisations

© European Data Protection Supervisor

The Confederation of European Data Protection Organisations' award is a token of recognition by the data protection community. The EDPS at the time, Peter Hustinx, received this award at the international privacy conference held at the University of Castellon, Spain, organised by Professor Artemi Rallo Lombarte, former director of the Spanish Data Protection Authority.

20 January 2014

Celebrating 10 years of the EDPS

© European Data Protection Supervisor

To celebrate its first decade, the EDPS organised a conference gathering stakeholders during which distinguished guests and speakers reflected on the EDPS' contribution to the advancement of data protection in the EU and beyond.

8 April 2014

Court of Justice of the EU invalidates the Data Retention Directive 2006/24/EC (Digital Rights Ireland and Seitlinger and others, *Joined Cases C-293/12 and C-594/12*)

© iStock.com/csreed

"While acknowledging that the fight against terrorism and serious crime justifies limitations on the rights to privacy and to the protection of personal data, this landmark judgment stressed that such limitations must be proportionate. As the Data Retention Directive did not meet that test, but rather created the feeling that 'Big Brother is watching you', it was declared invalid."

Koen Lenaerts

President of the Court of Justice of the European Union

26 September 2014

First workshop of the Internet Privacy Engineering Network (IPEN)

© European Data Protection Supervisor

"In September 2014, the EDPS initiated the Internet Privacy Engineering Network (IPEN) and organized a first Workshop which took place in the Berlin State Parliament. I was privileged to co-host this meeting back-to-back with the meeting of the International Working Group on Data Protection in Telecommunications ("Berlin Group"). Since then IPEN has done ground-breaking work in the field of Privacy by Design in the online world."

Dr. Alexander Dix LL.M.

Berlin Commissioner for Data Protection and Freedom of Information (2005- 2016), Currently Vice-Chair of the European Academy for Freedom of Information and Data Protection

4 December 2014

Giovanni Buttarelli is appointed as European Data Protection Supervisor and Wojciech Wiewiórowski as Assistant Supervisor

© European Data Protection Supervisor

Giovanni Buttarelli
Assistant Supervisor (2008-2014), EDPS (2014-2019)

"I am committed to supporting the EU legislator fully in its work to ensure that the data protection reform is adopted in 2015 and that modern and forward-thinking data protection mechanisms are implemented. In confronting the issues associated with big data, the time has come to make privacy and data protection more effective in the digital environment."

Wojciech Wiewiórowski
Assistant Supervisor (2014-2019), EDPS (2019-2024)

"I am looking forward to building on my experience in effective enforcement and technological know-how in order to make existing and new data protection principles more effective in practice. EU institutions need to ensure a high level of compliance and further implement the principle of accountability that will be developed in the reform."

2015

17 June 2015

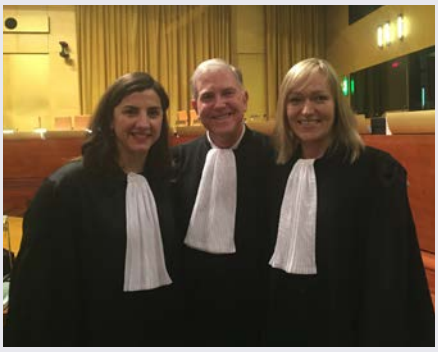
EDPS launches mobile app for data protection reform

© European Data Protection Supervisor

The EDPS launches a free EU Data Protection App to download the texts of the General Data Protection Regulation (GDPR) and the Law Enforcement Directive. The app also includes the history of the reform process of the pieces of legislation to allow its users to compare the new rules with the original rules, and the proposed texts from the European Parliament (EP) and the recommendations from the EDPS.

6 October 2015

Court of Justice of the EU invalidates the Safe Harbour Decision (Schrems, C-362/14)



© European Data Protection Supervisor

"The CJEU sent a strong message on 'mass surveillance' not only when it comes to EU ideas like 'data retention', but also when it comes to protecting our digital infrastructure against third countries. However, in the long run, we would need international agreements among democratic countries to ensure we can have both privacy and the free flow of data."

Max Schrems
Co-founder of nyob

2016

27 April 2016

Adoption of Regulation (EU) 2016/679 (GDPR)

© Photo by Mikhail Pavstyuk on Unsplash

"Data protection is a fundamental right in the EU. The new rules will put the Europeans back in control of their data. Now we have a choice and can decide what happens and who has what sort of data."

Věra Jourová
European Commissioner for Justice, Consumers and Gender Equality (2014-2019)

27 April 2016

Adoption of the Law Enforcement Directive (EU) 2016/680

© European Data Protection Supervisor

"While the Law Enforcement Directive (LED) covers only the processing of personal data for law enforcement purposes by national competent authorities, it signifies a very important legislative tool. Although the LED has still not achieved all its goals, it has nevertheless paved the way towards a more coherent and comprehensive framework on the protection of personal data for law enforcement purposes at national level."

Prof. Dr. Eleni Kosta
Professor of Technology Law and Human Rights, TILT-Tilburg University

2017

16 June 2016

EDPS-Civil Society Summit

© European Data Protection Supervisor

The EDPS strengthens its cooperation with civil society to discuss the state of privacy and data protection rights in the EU. Amongst its initiatives, the EDPS-Civil Society Summit, held each year since 2016, is created. At this particular meeting, discussions focused on the implementation of the GDPR, the directive on data protection rules for the police and criminal justice to name a few examples.

10 January 2017

Proposal for a ePrivacy Regulation

© iStock.com/KeremYucel

"Unfortunately, the ePrivacy Directive - adopted in 2002 and amended 15 years ago - did not withstand the test of time. Its intended replacement, the draft ePrivacy Regulation, is no longer fit for purpose, overtaken by the rapid technological developments. The legislative process has stalled, in part due to concerns related to access to traffic and location data for law enforcement and national security purposes. I hope that the new Commission will find the courage to bring forward new proposals that would overcome the current stalemate. Even with the GDPR in force, the EU still needs specific rules to protect the confidentiality and security of electronic communications."

Anna Buchta
Head of Unit 'Policy and Consultation', EDPS

11 April 2017

Necessity Toolkit: guiding policy making that respects individuals' privacy rights

© European Data Protection Supervisor

Almost all EU policy proposals involve some form of personal data processing. As part of its commitment to facilitating responsible and informed policymaking, the EDPS publishes a necessity toolkit to provide policymakers with a practical checklist, setting out the criteria to consider when policymakers assess the necessity of new legislation that may limit the fundamental right to the protection of personal data.

19 April 2017

EDPS starts supervising Europol

© European Data Protection Supervisor

With the new Europol Regulation, the EDPS supervises Europol, the European Union Agency for Law Enforcement Cooperation, whose remit is to help make Europe safer by assisting law enforcement authorities in EU Member States. The new Regulation also provides for the establishment of the Europol Cooperation Board, for which the EDPS provides the secretariat. The Board facilitates cooperation between the EDPS and EU Member States' data protection authorities on its supervisory activities.

2018

29 May 2017

First meeting of the Digital Clearinghouse

© European Data Protection Supervisor

"Data is a key source of market power in the digital economy. As competition the Bundeskartellamt is regularly dealing with data issues. Given the intersections with privacy issues, we continue to cooperate closely with data protection authorities and value the interdisciplinary exchange i.a. promoted by the Digital Clearinghouse."

Andreas Mundt
President of the Bundeskartellamt

1 April 2018

Appointment of Leonardo Cervera Navas as Director

© European Data Protection Supervisor

"Becoming the second Director in the history of the EDPS was a great honour for me. From that role I saw the EDPS take its place as relevant stakeholder in the data protection arena with a greatly successful international conference under the hosting of Supervisor Buttarelli."

Leonardo Cervera Navas
EDPS Director (2018-2023), EDPS Secretary General (2023-)

18 May 2018

Council of Europe adopts the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108+')

© European Union

"The global protection of the rights to data protection and privacy is crucially reinforced with the adoption of Convention 108+ - the protocol amending the 1981 initial Convention. Convention 108+ offers to all countries of the world a strong means to protect people in an ever increasing interconnected digital environment."

Sophie Kwasny
Head of Data Protection (2011-2021), Council of Europe

25 May 2018

Entry into application of Regulation (EU) 2016/679 (GDPR)

© European Data Protection Supervisor

"It is a historic day for data protection in the European Union. The GDPR brings a big shift towards the principle of accountability and stronger powers of enforcement."

Giovanni Buttarelli
Assistant Supervisor (2008-2014), EDPS (2014-2019)

25 May 2018

Establishment of the European Data Protection Board

© European Data Protection Supervisor

With the entry into force of the GDPR, the European Data Protection Board (EDPB), replacing the Article 29 Working Party (WP29), is created to bring together national data protection authorities of the countries of the European Economic Area, and ensure the consistent application of the GDPR and the Law Enforcement Directive. The EDPS provides the EDPB's secretariat and is a key contributor to the consistent application of the GDPR by cooperating with the EU and EEAs' data protection authorities.

22-26 October 2018

40th edition of the International Conference of Data Protection and Privacy Commissioners: Debating Ethics – Dignity and Respect in Data Driven Life

© European Data Protection Supervisor

"The 40th ICDPCC (now Global Privacy Assembly) underlined the importance of preserving values in the digital era. For the first time, the ICDPCC was conducted in two different venues, by the Bulgarian Commission for Personal Data Protection and the EDPS, completely proving that "No one is big enough, alone!" as well as demonstrating the capacity for innovation."

Ventsislav Karadjov
Chairman of the Bulgarian Commission for Personal Data Protection since 2014, Member of the GPA Executive Committee since 2023, two terms Vice-Chair of the EU Art. 29 Working Party (2014-2018), EDPB Deputy Chair (2018-2023)

11 December 2018

Entry into application of Regulation (EU) 2018/1725 (EUDPR)

© European Data Protection Supervisor

"The 'EUDPR' creates a consistent legal framework for processing of personal data in the EU institutions and agencies. It promotes greater transparency and accountability by obliging all EU institutions to set up a central register of data processing and make it publicly accessible, a step towards greater freedom of information."

Cornelia Ernst
Member of the European Parliament

31 December 2018

EDPS reaches 100 employees

© European Data Protection Supervisor

By the end of 2018, the EDPS counts 100 members of staff working towards protecting individuals' personal data. The EDPS brings together a diverse team of legal and technical experts, as well as other specialists in their field from across the European Union to shape the world of data protection.

2019

23 January 2019

European Commission adopts the EU-Japan mutual adequacy arrangement

© European Data Protection Supervisor, Archives 2022

"Following the adoption of the GDPR, ensuring that the protection travels with the data has been at the centre of the Commission's work on privacy. By creating the world's largest area of free and safe data flows, the landmark mutual adequacy arrangement with Japan has shown the potential and benefits of convergence around high standards of protection. Since then, we have stepped up our engagement with partners around the globe to further develop our network of trusted transfers."

Bruno Gencarelli
Head of Unit for International Affairs and Data flows, DG Justice, European Commission

25 February 2019

EDPS publishes guidelines on proportionality

© Photo by Mikhail Pavstyuk on Unsplash

The EDPS' Guidelines on assessing proportionality aim to provide policymakers with practical tools to help assess the compliance of proposed EU measures that could impact the fundamental rights to privacy and the protection of personal data with the Charter of Fundamental Rights. The Guidelines also complement the EDPS Necessity Toolkit, which help to evaluate the necessity of measures that limit the fundamental right to the protection of personal data.

12 July 2019

First EDPS-EDPB Joint Opinion

© European Data Protection Supervisor, illustration

Where a legislative or other relevant proposal is of particular importance for the protection of personal data, the European Commission may consult the EDPS and the EDPB, in accordance with Article 42(2) of Regulation (EU) 2018/1725. In such cases, the EDPS and EDPB work together to issue a Joint Opinion. The EDPS and EDPB issue their first Joint Opinion on the processing of patients' data and the role of the European Commission within the eHealth Digital Service infrastructure (eHDSI).

20 August 2019

In Memoriam Giovanni Buttarelli

© European Data Protection Supervisor

"Europe lost the visionary. Italy lost one of the best ambassadors of the EU."

Wojciech Wiewiórowski
Assistant Supervisor (2014-2019), EDPS (2019-2024)

"I am saddened to hear of the loss of Giovanni Buttarelli, the European Data Protection Supervisor. He was a champion in defending the privacy of 500 million EU citizens."

David Sassoli
President of the European Parliament (2019-2022)

"Heartbroken by the loss of my friend Giovanni Buttarelli, a visionary who advanced the cause of privacy in Europe and around the world. Our thoughts are with his family and all who loved him. Giovanni was a great man, and we are forever in his debt."

Tim Cook
CEO of Apple

10 September 2019

EDPS pleading before the Court of Justice of the EU

© European Data Protection Supervisor

The EDPS is invited to the hearing of the Court of Justice in Cases C-623/17 (Privacy International) with joined cases C-511/18 and C-512/18 (La Quadrature du Net and Others) and Case C-520/18 (Ordre des barreaux francophone et germanophone and Others), and shared its views on various aspects of privacy of electronic communications and data retention measures.

28 November 2019

Data Protection in Practice: the European Data Protection Case Handling Workshop

© European Data Protection Supervisor

The EDPS hosts the 31st edition of the annual European Data Protection Case Handling Workshop, bringing together 28 EU and non-EU data protection authorities. The unique set-up of the workshop is an opportunity to meet a wide array of practitioners and to share our experiences of investigating complaints, providing guidance to controllers, and enforcing data protection law. It is a platform to exchange with colleagues from other data protection authorities about supervisory and enforcement tasks.

6 December 2019

Wojciech Wiewiórowski is appointed as European Data Protection Supervisor from 2019-2024

© European Data Protection Supervisor

"I am delighted to have been selected as the new EDPS and look forward to continuing my work with the dedicated and talented team of individuals that make up this small but incredibly important institution. My mandate will embody the spirit of collaboration and unity. We will continue to work with authorities and experts across different policy areas to address the digital asymmetries that have become more acute during the Covid-19 public health crisis."

Wojciech Wiewiórowski
Assistant Supervisor (2014-2019),
EDPS (2019-2024)

12 December 2019

Supervising Eurojust: a new cooperation framework

© European Data Protection Supervisor

The EDPS starts supervising Eurojust - an EU agency in charge of combating serious forms of crime - in its processing of operational personal data.

"Ensuring a secure and open Europe requires increased operational effectiveness, but it also requires a commitment to protecting the fundamental rights and freedoms of individuals, including the rights to data protection and privacy. Under the new rules, it will be the job of the EDPS to ensure that Eurojust is able to perform its role as a law enforcement body as efficiently as possible, while demonstrating full respect for EU data protection law."

Wojciech Wiewiórowski
Assistant Supervisor (2014-2019),
EDPS (2019-2024)

2020

6 April 2020

EDPS calls for a pan-European approach to the pandemic

© European Data Protection Supervisor

"Together we are stronger and in a time of unprecedented crisis like the one we are going through; the European Union is the perfect place to pull resources together and to find common solutions. The European Data Protection Supervisor, as a data protection authority and as a EU institution, is fully committed co-operate with other European Institutions to put in place as soon as possible efficient measures to fight this existential threat to Europeans, to our economy and to our way of life. Our "mantra" is that big data means big responsibility. We have to know what we are doing, and to know that we are responsible for the results of our activity."

Wojciech Wiewiórowski
Assistant Supervisor (2014-2019), EDPS (2019-2024)

30 June 2020

Shaping a safer digital future: a new strategy for a new decade.

© European Data Protection Supervisor

Wojciech Wiewiórowski unveils his 2020-2024 Strategy. The overarching objective of the EDPS is to promote a safer digital future for the EU and to promote positive vision of digitisation that values and respects all individuals. To bring the strategy closer to the general public, the EDPS accompanied the launch of his strategy with a press conference, dedicated website and informational videos.

2021

15 October 2020

First meeting of the Global Privacy Assembly (GPA)

© Global Privacy Assembly

"My primary philosophy as Chair of the GPA was inclusiveness. I wanted the GPA to open its gates and become a truly international body. The GPA now represents more than 130 jurisdictions, and the executive has mandated cross-continent representation. It is important to remember that there is no fixed template of data protection law that applies worldwide; and therefore, there is no fixed template of what a data protection regulator looks like."

Elisabeth Denham
Chair of the Global Privacy Assembly 2018-2021 and Information Commissioner for the UK (2016-2021)

1 June 2021

EDPS supervises EPPO as it becomes operational

© European Data Protection Supervisor

The EDPS becomes responsible for supervising the European Public Prosecutor's Office (EPPO) in its operational capacity, the independent European body in charge of investigating and prosecuting criminal offences against the European Union's financial interests.

19 August 2021

GPA Giovanni Buttarelli Award

© European Data Protection Supervisor, illustration

The Giovanni Buttarelli Award was launched in 19 August 2021, by the Chair and Executive Committee of the Global Privacy Assembly, in memory of Giovanni Buttarelli, former European Data Protection Supervisor and Executive Committee member. The award ensures that Giovanni's legacy and advocacy for international cooperation continue.

28 September 2021

Launch of TechSonar and TechDispatch

© European Data Protection Supervisor, illustration

Data protection has a strong connection with technology. As such, the EDPS launches a new initiative, TechSonar, that aims to anticipate emerging technology trends to better understand their future developments, especially their potential implications on data protection and individuals' privacy. In October 2021, the EDPS' TechDispatch initiative received the Global Privacy and Data Protection 2021 Award, for the "Education and Public Awareness" category at the 43rd Global Privacy Assembly 2021. TechDispatch explains, informs and raises awareness of potential data protection issues surrounding new technologies.

2022

03 January 2022

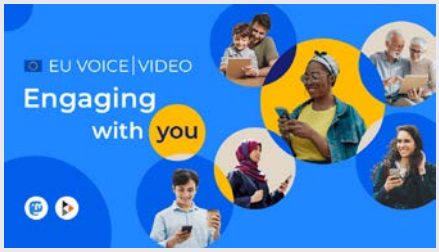
EDPS orders Europol to erase data with no established link to a criminal activity

© European Data Protection Supervisor

The EDPS notifies Europol of an order to delete data concerning individuals with no established link to a criminal activity. Datasets older than 6 months that have not undergone this categorisation must be erased. This means that Europol will no longer be permitted to retain data about people who have not been linked to a crime or a criminal activity for long periods with no set deadline.

28 April 2022

EDPS launches two social media platforms: EU Voice and EU Video



© European Data Protection Supervisor, illustration

EU Voice and EU Video are part of decentralised, free and open-source social media networks that connect users in a privacy-oriented environment, based on Mastodon and PeerTube software. By launching the pilot phase of EU Voice and EU Video, the EDPS aims to contribute to the European Union's strategy for data and digital sovereignty to foster Europe's independence in the digital world.

7 June 2022

Supervising Frontex

© European Data Protection Supervisor

The EDPS issues two Supervisory Opinions on Frontex's processing operations. The first Supervisory Opinion concerns Frontex's Internal Rules applicable to all of its personal data processing activities. Whilst the second Supervisory Opinion concerns Frontex's personal data processing activities related to the identification of suspects involved in cross-border crimes. In its Supervisory Opinions, the EDPS remarks that Frontex's Internal Rules are not sufficiently clear. The EDPS recalls that special categories of personal data, such as individuals' health data, data revealing racial or ethnic origin, genetic data, can only be processed if this can be legally justified. These special categories of data also need to be protected with specific safeguards to avoid discriminatory practices.

16-17 June 2022

EDPS Conference: The Future of Data Protection: Effective enforcement in a Digital World

© European Data Protection Supervisor

"I believe that the debate on the enforcement model of the GDPR has progressed immensely thanks to our Conference - even before it took place. While there will be many fathers (and mothers!) of the new centralised model in the future, it is on 17 June 2022 when the inevitable has been stated!"

Kazimierz W. Ujazdowski
Member of EDPS Cabinet

16 September 2022

EDPS takes legal action as new Europol Regulation puts rule of law and EDPS independence under threat

© European Union, *Source*: Court of Justice of the European Union

The EDPS requests that the Court of Justice of the European Union (CJEU) annuls two provisions of the newly amended Europol Regulation, which came into force on 28 June 2022. The two provisions have an impact on personal data operations carried out in the past by Europol. In doing so, the provisions seriously undermine legal certainty for individuals' personal data and threaten the independence of the EDPS - the data protection supervisory authority of EU institutions, bodies, offices and agencies.

29 November 2022

Supervision Conference: data protection and criminal justice

© European Data Protection Supervisor

The EDPS co-organises with the European Union Agency for Criminal Justice Cooperation - Eurojust, and the European Public Prosecutor's Office - EPPO, a conference on data protection in the field of criminal justice in the EU.

During the conference, distinguished guest speakers discuss how the amendments to the Eurojust Regulation may impact Eurojust in its processing of personal data, a review of EPPO's first year of operations and explored how the EDPS, as the data protection authority of Eurojust and EPPO, can ensure effective coordination and supervision of Eurojust and EPPO, in light of a complex legal landscape.

2023

14 March 2023

Opening of the EDPS Office in the European Parliament Strasbourg

© European Data Protection Supervisor

"European Parliament LIBE Committee remains fully committed to protecting EU citizen's fundamental rights, notably data protection and confidentiality. The proximity of the EDPS' Strasbourg Office, in the seat of EP Plenary will strengthen the already excellent cooperation between the LIBE Committee and the EDPS."

Juan Fernando López Aguilar
Committee on Civil Liberties, Justice and Home Affairs

23 May 2023

5th anniversary of the GDPR

© European Data Protection Supervisor

To celebrate the 5th anniversary of the GDPR the EDPS organises an event in collaboration with the German Federal Commissioner for Data Protection and Freedom of Information, and the Bavarian Data Protection Commissioner. The event served as an opportunity to analyse its success and challenges ahead and to inform our work as we contribute to the enforcement of the GDPR as a member of the European Data Protection Board.

2024

10 July 2023

Reshaping the EDPS to tackle new challenges of tomorrow

© European Data Protection Supervisor

2023 is marked by organisational changes to ensure the EDPS' efficiency in a fast-changing digital landscape. To reflect the institution's priorities, the EDPS' first Secretary General, Leonardo Cervera Navas, was appointed as trusted strategic advisor and aid. Specialised sectors were also created to tackle ongoing and future data protection challenges, including a sector to monitor the EU's Area of Freedom, Security, and Justice; one to address individuals' complaints; another to ensure that technologies embed privacy principles throughout their development, as well as our very own Legal Service.

17 January 2024

EDPS celebrates its 20th anniversary

© European Data Protection Supervisor; © iStock.com/Aykut Ozlu

The EDPS celebrates two decades of protecting individuals' privacy and data protection rights. Its anniversary is built on 4 pillars, 4 parallel initiatives to promote the importance of data protection. This includes a book and interactive timeline analysing key data protection milestones, 20 insightful talks with leading voices sharing their unique perspectives on data protection and privacy, 20 initiatives and a European Data Protection Summit on 20 June 2024 to continue to innovate as a modern data protection authority.

Memories

Joaquín Bayo Delgado

Assistant Supervisor (2004–2008)

At the beginning of the EDPS in January 2004, there were three main challenges: to set up the new institution, to organise its tasks as data protection supervisory authority of the EU and to define and start its functions as advisory body on data protection matters.

There was an approved budgetary prevision done by the European Commission, but obviously based on theoretical calculations. On the other hand, the three main institutions (EC, Parliament and Council) were very supportive granting the EDPS with the basic infrastructure needed: premises and IT (Parliament), translation services (Council) and administrative help and provisional staff (EP and EC). But, the main challenge in this area was, without doubt, to select and appoint the new staff of the EDPS. We were very lucky because in May 2004 the enlargement of the EU took place, so we were able to gather our team from 25 countries. The process was intensive and difficult, as we had to choose the very best. We did. By 2009, at the end of the first EDPS term, more than 60 people were in the team and it was most satisfactory to work with such a team.

In the area of supervision, there were several priorities. The institutions and agencies of the EU have been, of course, processing personal data for a long time. Some of those processing systems would have had to be prior checked before starting, but there was no EDPS to do so. The solution was to check them *ex post*, to make sure they complied with data protection rules. That was a huge task, for which we had the priceless help of the DPOs already existing (EC, EP, Council…). The second aspect to take care of was to promote the appointment of a DPO where there was none. The third matter was to organise and explain the scope of complaints to be examined by the EDPS; there, it was very important the Memorandum of Understanding signed with the European Ombudsman.

In our advisory tasks, we had to make sure that the EC asked the EDPS's opinion on any proposal of legislation, which involved personal data processing. Receiving such proposals for pinion became more and more frequent. And, it also became frequent to appear before the European Parliament (LIBE Committee) and Council to explain the EDPS Opinion on issues relating to data protection. The EDPS was also very active in the so-called Article 29 Working Party, which was an excellent forum to share perspectives with colleagues of national data protection authorities. The same was the case within European and World Conferences on data protection.

Intimately related to supervision and consultation, the EDPS developed, little by little, other tasks: development of its own internal rules of procedure, interventions before the European Court of Justice, data protection inspections, etc. The rest is data protection history.

Clara Guerra

Portuguese Data Protection Authority and Coordinator of the Coordinated Supervision Committee – CSC

Congratulations to the EDPS!

It is always a joy to celebrate anniversaries, but they become even more especial when it is a data protection authority's party. Ideal moments to reflect on what was achieved and on what is yet to be accomplished, and most importantly, where it stands right now.

Looking back to the last 20 years, it is just fair to say that the history of the EDPS is a story of success. The EDPS is today a high profile DPA, recognised by the increasing quality of its work, in both consultation and enforcement level, and certainly, a voice to be heard when it comes to guaranteeing the fundamental rights to data protection and to privacy.

I have been working in the Portuguese DPA since 1997, so I had the opportunity to follow the discussions in the European Parliament and in the Council about Regulation (EC) 45/2001 to be, as well as the setting up of the EDPS.

In 2004, I witnessed its birth, and then its first steps, its ambition, its development and, more recently, its majority. Too many memories come to my mind when I think of all the challenges data protection authorities have faced together in these two decades.

Besides the common membership of Article 29 Working Party, several times the work of national DPAs crossed paths with the EDPS, in particular in relation to the EU large-scale information systems and in the law enforcement area. The shift from a model of joint supervision to a model of coordinated supervision, between the national and the central level, headed inevitably to a closer relationship with the EDPS and a reinforced cooperation between the EDPS and the national DPAs.

It has been indeed a considerable journey all these years, with the usual ups and downs, but mostly a learning process for an improved cooperation and an effective enforcement.

At this moment, in the Coordinated Supervision Committee – CSC, within the framework of the European Data Protection Board, I would say that cooperation between national DPAs and the EDPS reached a higher threshold of maturity. As Coordinator of the CSC, my experience has been very gratifying in that regard, since there are enhanced interactions, fruitful exchanges and significant support from the very well prepared EDPS's team, which place our supervisory role in the right track and enrich our collective work.

During these 20 years, the EU has changed considerably in many aspects, so has the data protection legal framework and the data protection community. However, we are now living in difficult times for human rights, which is why our task is ever more crucial for the health of democracy. We need resilient supervisors and meaningful enforcement, what we can only achieve by working altogether in practice the rights of the individuals to privacy and to data protection.

Congratulations to the EDPS, and personally to Wojciech, for being a data protection authority that has arrived and stayed at the frontline of this mission!

Isabelle Falque-Pierrotin

Présidente Commission Nationale de l'Informatique et des Libertés (CNIL) (21 septembre 2011 – 2 février 2019), Chair Article 29 Data Protection Working Party (27 February 2014 – 25 February 2018)

Le RGPD a représenté un moment décisif de l'identité européenne. Honnêtement, au début, personne ne pariait vraiment sur les chances d'aboutir. Il a fallu les révélations de Edward Snowden en 2013 pour que s'accélèrent les négociations, notamment grâce à la mobilisation des Allemands. Tout l'enjeu ensuite a été de construire une gouvernance du texte qui fonctionne. Je croyais à la nécessité de construire celle-ci de façon distribuée et non centralisée, reconnaissant la responsabilité première des régulateurs nationaux et ne transférant à Bruxelles que les cas vraiment transnationaux. L'EDPB a été conçu en ce sens, comme une structure légère, dont le fonctionnement était assuré par l'EDPS, et qui devait constituer une sorte de médiateur agile des échanges entre régulateurs nationaux. Le temps passé a montré deux choses : d'une part que le RGPD aurait dû être accompagné de pratiques d'harmonisation régulatoire sur les flous du texte plus rapides que celles intervenues ; d'autre part, que ce schéma nécessitait que l'EDPB monte en puissance vite et que les régulateurs nationaux hésitent moins à le saisir. Aujourd'hui, l'EDPB s'est bien installé et même encore imparfait, ce modèle de régulation distribuée concilie la demande des États de garder la main sur leur régulation tout en apportant une solution concrète aux sujets d'intérêt commun.

The GDPR represented a decisive moment for European identity. To be honest, at the beginning, no one was really betting on the chances of its success. It wasn't until Edward Snowden's revelations in 2013 that negotiations accelerated, thanks in particular to the involvement of the Germans. The next challenge was to build a governance structure for the text that worked. I believed in the need to build this in a distributed way rather than a centralised one, recognising the capacity of national regulators to act at first place and only transferring to Brussels cases that are really transnational. The EDPB was designed with this in mind, as a light structure, for which the EDPS would provide logistical support for its functioning, to act as a sort of mediator for exchanges between national regulators. The passage of time has shown two things: firstly, that the GDPR should have been accompanied by a quicker regulatory harmonisation of the text's ambiguities than has been the case to date; and secondly, that this system required the EDPB to grow rapidly and for national regulators to be less reluctant to refer matters to it. Today, the EDPB is well established and, even though it is still imperfect, this model of distributed regulation reconciles the demands of States to retain control over their regulation whilst providing concrete solutions to issues of common interest.

Willem Debeuckelaere

President of the Belgian Data Protection Authority (2005–2019) and Deputy Chair of the Article 29 Working Party / EDPB (2016–2019)

Dear Supervisor, Dear Wojciech,

I must congratulate you.

Not just for keeping the EDPS alive and alert, and not just because your institution is celebrating two decades of championing the protection of privacy and personal data. I mainly must congratulate you for what you said during the fascinating conference on the "Future of Data Protection: Effective Enforcement in the Digital World", which took place in Brussels on 16 and 17 June 2022.

Upon closing the conference, you gave an edifying speech. I confess that I was surprised by the content of that speech, especially given the prevailing narrative among European regulators and their relationship with the GDPR at the time.

You decided to tell it like it is and to move away from those who uncritically accepted that "everything is great". You called out the need for a cooperation mechanism that works – I can only compare the current one to a rusty set of hinges that moves with difficulty and grinds its teeth at the slightest sand that gets into the machinery. The state of play you described left me inspired.

We will need a thorough revision of the current enforcement mechanism in order to move to a more effective and swift enforcement of the GDPR. Your speech captured many of the criticisms that have been developing for years, and which the Vienna Statement on enforcement cooperation of 28 April 2022 only started to address. For me, your speech represented a first diplomatic attempt to move again towards a more European instead of a predominantly national approach. I find the latter approach to be inefficient and costly, both in terms of time and in terms of resources spent. Especially when most of the cases which are European in nature are left to be handled by one national authority, which is responsible for supervising the bulk of the largest international players without having the necessary resources to do so in an effective manner.

The national approach, also defended by the EDPS at one point in time, was a disappointment to me. Especially since we, as Belgian data protection authority had very good experiences with the support and approach provided by the EDPS until then. To name just one example: SWIFT. The Belgian Data Protection Authority was only taken seriously by the company SWIFT once it had the full

support of the EDPS and the Group 29 (and the Council of Ministers...). And that we were able to bring that case to a good and sound conclusion is partly due to the intellectual and strategic assistance provided to us by your institution. Discreet but decisively valuable.

I forget, then, the sometimes comical discussions about the name and about whether or not the position of Chair of the EDPB could be a full-fledged and full-time position... Sometimes it seemed that it was not efficiency but honour and glory that coloured the positions.

What I also greatly appreciated about the EDPS is its push for greater collaboration with consumer protection and competition authorities in light of the growing concentrations of market power. The idea of the Digital Clearing House launched by the EDPS in 2016 was groundbreaking and a major eye-opener. For the outside world, however, nothing tangible has happened in that area so far. May this be an invitation to pick up that thread again.

All the best to the EDPS, and to you personally, Wojciech, too, in the many years and challenges to come.

Sincere greetings,

Willem Debeuckelaere

Anu Talus

Chair of the European Data Protection Board (2023-2028)

The sum of the whole is bigger than the sum of each part. This aphorism perfectly encapsulates the way EDPS approaches its support to the European Data Protection Board, both as member of the EDPB and as the institution that provides the EDPB Secretariat.

Since day 1 as Chair of the EDPB, I have been the lucky recipient of this support, not just at an institutional level, but also at the level of the individuals that lead this respected institution. My very first meeting as newly elected Chair was with the EDPS and ever since, I am always able to count on the support of European Data Protection Supervisor Wojciech Wiewiorowski and Secretary-General Leonardo Cervera Navas for organisational and strategic matters, not in the least the budget of the EDPB and its Secretariat.

This efficient and professional cooperation is reflected at all levels of both our organisations. The men and women that make up the EDPS have no qualms sharing their expertise with EDPB colleagues, and always stand ready to contribute to the work of the EDPB.

Though EDPB and EDPS are separate legal bodies with distinct missions, we are both guided by the conviction that combining knowledge, skills and experiences and pooling resources leads to important synergies. EDPB and EDPS are united in pursuing the same objective of advocating for the fundamental rights to data protection and privacy, as the cornerstone of individual freedom and democracy.

John Edwards

UK Information Commissioner (2022–2027),
Former Privacy Commissioner, New Zealand (2014–2021)

Over the last 20 years, I've seen the EDPS transform from a concept into a data protection authority with influence far beyond its mandate. It remains steadfast in its advocacy for and promotion of fundamental rights to privacy and data protection in an evolving digital and technological landscape.

Under the inaugural leadership of Peter Hustinx, the EDPS became an international force as he brought gravitas, international expertise and diplomatic skill to the role. Whether it's convening the DPO community within EU institutions, putting forward Opinions to improve cross border cooperation, making judicial interventions or organising the Spring Conference for data protection authorities to exchange ideas, he and his small team were present and committed. The UK's regulatory community benefitted from Mr Hustinx' global experience when he joined the ICO as a Non-Executive Director from 2019-2023, helping better connect the organisation with European partners and stakeholders.

The need to collaborate and bring regulatory clarity to individuals and businesses on thorny issues like global data flows and legitimate government access, artificial intelligence and biometric surveillance has never been more important –and the EDPS has convening power. Few will forget the EDPS hosting the "Olympic Games of data protection", the then International Conference of Data Protection and Privacy Commissioners in 2018 under the mandate of the late Mr. Giovanni Buttarelli. He brought courage and deep thinking on issues like ethics. He spoke powerfully about the human values that underpin data protection, the need to speak to those outside of privacy and for DPAs to better understand technology and articulate a more ethical framework. Otherwise, we will struggle to fulfil our mission to safeguard human rights in a digital age.

Under the current leadership of Wojciech Wiewiórowski, the relationship between the ICO and EDPS has gone from strength to strength. Despite global political shifts, pragmatism and collaboration runs deep. Whether that's participating in the annual European Data Protection Case Handling Workshop in 2019 to ensuring greater consistency of approach among DPAs at the G7 and Global Privacy Assembly on generative AI systems, the EDPS has played an enabling role. Our recent signing of a Memorandum of Understanding cements a long-standing commitment to uphold data protection and privacy rights and champion solidarity in the face of a changing digital landscape. After all, they are one, we are many.

Here's to 20 more years. Happy anniversary EDPS.

Ngā manaakitanga

Paul De Hert

Vrije Universiteit Brussels & Tilburg University;
Founder of CPDP

CPDP, EDPS and downwards accountability taken seriously.

In 2014, with my colleague Vagelis Papakonstantinou, I was to take stock of the amazing development of the newly founded EDPS in its first decade under its first European Data Protection Supervisor (Peter Hustinx, 2004-2014). I reflected on the institution and its tremendous capacity to fulfill its legally enumerated roles, while adding an important role of initiating and developing data protection ideas and policies ([1]). The introduction of a new data protection principle on accountability in the GDPR is to no less degree indebted to the receptive mindset of the EDPS, picking up messages and signals from the field, giving them an original twist so they became 'his' and subsequently advocating effectively to get these ideas on the policy agenda, which they often do ([2]). The onus in that first period was of getting the right data protection message out whether that message was addressed to ngo's, to academic audiences, to industry or to policy makers.

As a co-founder of the now renowned Computers, Privacy and Data Protection (CPDP) Conference, I vividly remember how Hustinx attentively followed the first edition organized on October 12-12, 2007 ('Reinventing Data Protection') looking at a decade of the first EU data protection directive. The conference organized by Tilburg University, Université de Namur and the Vrije Universiteit Brussel received mainly international academics, but the presence and interventions of Hustinx were most remarkable. As said, it was all about getting it right and passing on the message of the first-generation data protection founders, scholars and practitioners (Hustinx being one of the founders) to a new data protection generation.

On September 10th, 2019, speaking at a memorial ('Tribute to the life of Giovanni Buttarelli') I was able to reflect a second time about the role of the EDPS, this

([1]) De Hert, P. & Papakonstantinou, V., 'The EDPS as a Unique Stakeholder in the European Data Protection Landscape, Fulfilling the Explicit and Non-explicit Expectations', in Hijmans, H., Kranenborg, H. (eds.), *Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*, Intersentia, Cambridge, 2014, p. 237-252.

([2]) Hence, no accountability, understood as compliance in exchange for less regulatory constraints (as proposed by some international economical players), but accountability understood as a human rights duty to go beyond mere compliance and seek for continued alertness when processing data.

time at the occasion of the tragic passing away of the second EDPS. The message of data protection was no longer menaced by dangerous interpretations that, if accepted, would have thwarted its effectiveness (by limiting the scope of definitional concepts such as 'personal data' or 'provider', by not applying data protection law to posting data on the internet, etc). The second EDPS therefore concentrated on bringing this message to the right placeholders: all the DG's other than DG Justice (home of EU data protection) rolling out the digital agenda. Novel ideas saw the light, such as having ethics complementing hard law and envisaging a 'Digital Clearing House' of enforcers to bring together, for the first time, agencies from competition, consumer and data protection law.

The status of the EDPS as a leader of ideas on data protection was undisputable. His annual presence in the prestigious Caspar Bowden-panel and the attentively attended CPDP-concluding remarks (all on YouTube) were (are) naturally taken for granted.

It is too early to write the history of the third EDPS, although the climate of panic of the Pandemics did not mean peaceful data protection times and vigilance was needed daily. By now it is clear that there is a system behind the continuity of the interaction between the EDPS and conferences like CPDP, -on of the rare non-profit in the landscape supervised by (but not dominated by) academics. The system is one of combining the traditional tasks of a data protection authority, with the not so common task of directing and redirecting the flow of data protection policy development by taking part in public reasoning with great intellectual authority. This strategy has real-world purchase. Accountability, Colin Scott observes, is (also) about promoting fairness and rationality in administrative decision making.Traditionally we think about accountability as rendered to a higher authority ('upwards accountability'), ignoring accountability to broadly parallel institutions ('horizontal accountability') or to lower-level institutions and groups (such as consumers) ('downwards accountability'). While the Digital Clearing House relates to the horizontal variant, CPDP interventions and other public actions of the EDPS serve downwards accountability. The EDPS can be credited for having understood the importance of full, holistic accountability and this since its inception. A genuine leader is not a searcher for consensus but a molder of consensus (Martin Luther King, Jr.).

Ursula Pachl

Deputy Director General of BEUC, the European Consumer Organisation

A lighthouse for upholding people's rights

Over the past two decades, the EDPS has been at the forefront of all debates related to data protection and privacy. It has been highly active in European and international fora, raising the profile of the institution and helping to establish the EU as the leading voice in terms of data protection. The EDPS has indeed led by example, as a prominent voice in Europe and beyond, a global ambassador for the GDPR and a defender of privacy and data protection as fundamental rights.

Importantly, from its beginnings, the EDPS has pushed the boundaries of data protection, following a cross-disciplinary vision that identifies the place and role of data protection in different areas of law and across the data economy (competition, data protection, consumer protection, artificial intelligence, on-line platform regulation). Today, this approach is more necessary than ever to protect individuals' rights and our democratic societies in the digital world effectively.

An outstanding moment for me in the recent history of the EDPS was its conference titled "Future of Data Protection: Effective Enforcement in the Digital World", organised in June 2022. This conference was a milestone, it was decisive both for improving the enforcement of the GDPR, but also for the EU's understanding of enforcement in digital policies in general. Initiating this debate was exactly the right thing to do:

After four years of GDPR application, it was time to openly identify the enforcement weaknesses of the GDPR and to finally address the elephant in the room: how can we ensure effective enforcement in a world that is increasingly digitalised? How can we make sure the EU is a credible regulator when new technologies, new market structures and new business practices arise and change at the speed of light? New laws emerge with various enforcement architectures, but the Digital Markets Act, Digital Services Act, Artificial Intelligence Act, the Digital Governance Act and the Data Act are all based on one pre-condition: that the GDPR is respected and enforced properly.

The stakes were and are still very high. The discussion about effective enforcement is a discussion about the democratic governance model. It is our democratic model that is at stake, it is about the EU's values and our fundamental rights, the credibility of institutions and their regulations not only in the EU but also globally.

It was the EDPS – who else? – that alerted us to the urgency and importance of these developments. It created the space to hold a discussion with all relevant stakeholders, underlining that this is a challenge that can only be addressed if all players work together and contribute according to their respective roles.

This is just one example where the EDPS has been a lighthouse that provides guidance and foresight in these turbulent and sometimes dark times. It does so for regulators, authorities and very importantly also for civil society. The conference was another proof of the invaluable role and contribution of the EDPS, now under the great leadership of Wojciech Wiewiórowski.

Now, more than ever, we need institutions that strongly defend democratic values and have the determination based on a vision to do so.

Thank you very much, dear EDPS, and happy birthday!

Joe Mcnamee

International Privacy Champion 2019

From a personal perspective, I have had a very positive engagement with all of the holders of the office of EDPS, in the 20 years since the role was first filled. While there were, of course, occasional divergences of opinion, the passion of Peter, Giovanni and Wojciech for the protection of our fundamental right to data protection, as well as the freedoms that rely on it, has always been beyond question. Peter's and Giovanni's genius in shaping the role of the EDPS into what it is today, is a huge legacy and an invaluable contribution to the quality of the EU's traditional leadership in data protection. Wojciech has built on this legacy. The first time I saw Wojciech was when he delivered a passionate, heart-felt speech in the European Parliament during the preparatory stages of the GDPR. In over a quarter of a century of being involved in policy discussions in Brussels, I can say with certainty that I never heard another speech that was so compelling, nor one with such personal conviction.

Part of this building of the role was effective engagement with all stakeholders, including with civil society. This meant not just communicating the astonishingly high quality work and analysis of the EDPS to civil society, but also through meaningful mutual learning. Part of the massive success of the European Digital Rights' "Privacy Camp" is attributable, in my opinion, to the strong engagement of the EDPS and the team to provide its unique expertise and perspective. The fact that this strong support can be relied upon year after year consistently enhances the quality and facilitates the planning of the event. In the other direction, civil society often is given the opportunity to speak – and listen – at EDPS events, not least of which are the always-impressive conferences organised by the young prodigies that have the good fortune to become EDPS trainees.

In short, the EDPS has always been a reliable interlocutor for civil society, engaged and committed, but also independent and critical.

Marc Rotenberg

Founder Center for AI and Digital Policy

The laws of data protection are not simply words on a page. Their animating spirit is the individuals and institutions that give life to them. Our privacy champions initiate actions, engage the public, identify emerging challenges, and create effective responses. They defend our freedoms. The creation of Supervisory Authorities was at the foundation of the Data Protection Directive and it remains central to the realisation of the GDPR today.

And so, it is appropriate to celebrate the 20th anniversary of the European Data Protection Supervisor. The EDPS has long been the vanguard of data protection for the EU. Under the leadership of Peter Hustinx, Giovani Buttarelli, and Wojciech Wiewiórowski, the EDPS has emerged as a powerful global force as the world confronts new challenges in the digital age.

Most recently, the EDPS came forward as the Parliament was considering the Artificial Intelligence Act to make clear the need for clear prohibitions on the deployment of certain AI systems that violate fundamental rights. Establishing the red line for impermissible AI systems is perhaps the most difficult challenge of AI policy. Many AI policymakers are inclined to move forward with AI systems as long as they are described as "ethical" or "responsible." They attempt to fix rather than curtail AI systems designed for mass surveillance, social coercion, and manipulation.

The AI Act reflected the hard work of the EDPS, civil society, and members of Parliament. It includes seven distinct prohibitions, from biometric categorization to AI used to exploit the vulnerabilities of people. While work remains to be done regarding the use of AI for immigration and policing, the EDPS has made clear, as did Michelle Bachelet the former UN High Commissioner for human rights, that AI systems should not be designed, developed, or deployed that are incompatible with international norms for human rights.

The EDPS has reached out to civil society for direction and advice, seeking the cooperation and support of those tasked with the representation of the public's growing concern about the risks and harms of unregulated technologies. Together the EDPS and civil society have established an effective alliance that has stood up to forces far more powerful. It was not obvious that the EDPS would take on this responsibility, but it has done so with both courage and acumen.

The EDPS has worked in collaboration with many other EU institutions, most notably the European Data Protection Board. Together the EDPS and the EPDB have helped coordinate enforcement actions among the various DPAs. Although there is still more work ahead to ensure that individual DPAs do not become bottlenecks for effective enforcement, the collaboration of the EDPS and the EDPB, as well as the participation of the Parliament and the Commission, is a positive sign that progress can be made.

In the landmark book, *Protecting Privacy in Surveillance Societies*, David Flaherty observed that data protection officials play a critical role in safeguarding data protection. Flaherty was a keen observer of privacy officials, able to recognise those who were effective as leaders of their institutions and champions for the public. He liked those who would "stand on their soapboxes," say directly what must be said, and take action where they could.

He would celebrate the accomplishments of Peter Hustinx, Giovani Buttarelli, and Wojciech Wiewiórowski, as would the architects of the original Data Protection Directive. The EDPS has ensured the vibrancy of data protection law over the past 20 years. And, we will look to the EDPS to animate these laws in the years ahead.

Birgit Sippel

Member of the European Parliament for the Socialists and Democrats

The European Data Protection Supervisor's 20-Year Journey: Safeguarding Privacy in collaboration with the European Parliament

Over the past 15 years, in various roles – as a member of the LIBE Committee, Rapporteur or Coordinator – I have worked on and followed closely many diverse laws aimed at protecting fundamental rights, specifically privacy and data protection. Throughout this journey, collaborating with the European Data Protection Supervisor has always been a crucial element in evaluating numerous aspects, concerning both individual laws and fundamental questions.

Based on all these experiences, I only can conclude that the EDPS stands as a guardian, safeguarding the fundamental rights of privacy and data protection within the European Union. Celebrating its 20th anniversary, the EDPS has not only fortified its position as an indispensable institution but has also forged a profound collaboration with the EU Parliament, synergising efforts to ensure the integrity of personal data and privacy rights for everyone in the EU.

Established in 2004, the EDPS emerged in response to the growing importance of safeguarding privacy in an ever more data-centric world. Over the last two decades, it has evolved from a regulatory body to a fierce watchdog that navigates the complex landscape of emerging new technologies, legislative changes and increasing desires to access vast amounts of personal data.

From my experience, the relationship between the EDPS and the EU Parliament is characterised by mutual trust and has significantly contributed to the EU Parliament's work, enabling informed decisions and legislative precision by shaping the trajectory of data protection policies. The EDPS's independent opinions serve as a lighthouse, illuminating the ethical and legal dimensions of data processing, influencing parliamentary discussions and outcomes. Through its investigations, reports, and consultations, the EDPS has been a reliable and close partner, providing invaluable insights and guidance to legislators. Its guidance has enriched debates, prompting nuanced considerations of privacy and data protection in various policy domains, from tech regulation to law enforcement practices.

Moreover, the EDPS's proactive stance on emerging technologies, such as artificial intelligence and biometrics, has steered the EU Parliament toward a future-focused and rights-based approach, ensuring that legislative measures anticipate potential risks to privacy and data protection. Collaborative efforts have resulted in frameworks that strike a delicate balance between innovation and safeguarding fundamental rights.

As the digital landscape continues to evolve, the EDPS and the EU Parliament face new challenges requiring continued collaboration. Enhancing cross-border data transfers, regulating emerging technologies, and reinforcing individual control over personal data are pivotal areas demanding joint efforts. The EDPS's role as an advisor, watchdog, and advocate remains indispensable in navigating these areas.

Over the period of two decades, the EDPS has exemplified an unwavering dedication to safeguarding fundamental within and – for example with GDPR – beyond the EU. This is even more important as data protection is vital for protecting privacy and other fundamental rights, such as freedom of expression – especially in an ever more digitalised world. The partnership with the EU Parliament serves as a powerful illustration of the alliance between institutions devoted to preserving fundamental rights and core values of the European Union. Rapid technological advancements will not disrupt the solid collaboration between the EDPS and the EU Parliament and with an ongoing strong position of the EDPS and passionate engagement of parliamentarians; we will be successful in protecting our citizens in all challenges to come.

Sophie in 't Veld

Member of the European Parliament for Renew Europe

Happy birthday EDPS! In 2004, the European Data Protection Supervisor was a newbie, like myself as I was first elected in that same year. A lot has changed since then. In my parliamentary work, I focused on privacy and data protection, which was considered a niche topic at the time. "Citizens don't care about privacy. If you have done nothing wrong, you've got nothing to hide. Why do you bother?" was the question I invariably got. Today, in the age of social media, loss of privacy still does not seem to be at the top of most people's minds , but no one underestimates the immense power of data anymore. The Artificial Intelligence Act, strict rules on political advertising and micro-targeting, a ban on the use of TikTok by public officials all testify to the public awareness.

Twenty years of visionary leadership of Peter Hustinx, Giovanni Buttarelli and Wojciech Wiewiórowski have made the EDPS a leading global voice on data protection. They fully understood that data protection is not about protecting data, but about protecting people and protecting our democracy.

Of course, their voice is not welcomed by everyone. If the use of data brings wealth and power, the wealthy and powerful do not like any restrictions on access to, and use of personal data. We note a worrying trend of EDPS opinions being ignored or only partially implemented, as they were considered an obstacle to the political wishes of the Commission and Council. In several cases, the latter were wrist-slapped by the European Court of Justice, like in the case of PNR transfers to Canada, the 2006 Data Retention Directive or the saga with Safe Harbour and Privacy Shield (probably soon to become a trilogy, as their successor has also been challenged). The heated debates around the Child Sexual Abuse Material legislation, the stalled e-Privacy Regulation, the European Health Data Space or the spyware scandal sadly indicate that commercial or political interests frequently take precedence over citizens' rights. But, where Commission, Council and some forces in the European Parliament are sometimes wobbly on privacy and data protection, the EDPS has always unwaveringly been on the side of citizens.

Privacy and data protection are core elements of the democratic rule of law and a vital protection wall for citizens' rights when anti-democratic parties come to power. It must therefore be one of the key tasks of the 2024 European Parliament to fully and forcefully support the EDPS in its mission, to strengthen its means and powers, and to ensure vigorous enforcement of EU privacy and data protection laws.

Many happy returns dear EDPS!

Dr. Patrick Breyer

Member of the European Parliament for the Greens/EFA

The European Data Protection Supervisor has played a vital role since I have become a Member of the European Parliament in 2019. In times of an ever-growing political appetite for surveillance, the EDPS has repeatedly showcased strength, independence and diplomacy in carrying out its mission. Nor did it shy away from investigating and fining EU institutions where necessary.

Nearly every Commission proposal now incorporates data protection-relevant elements, as many aspects of our lives in the information age are datafied. The EDPS' guidance has hence become relevant for an ever-increasing range of areas subject to EU legislation. However, while it is always read, the EDPS' guidance on digital policy seems rarely followed by the legislator. For the latter, the pursuit of digital innovation often eclipses, or come at the expense of, privacy and data protection considerations, and the red lines the EDPS carefully points out have more than once been lightly crossed (thinking of biometric mass surveillance).

While the EDPS has often been the champion of fundamental rights it was designed to be, it has also sometimes shown how wary it is of being (unjustly) considered overly radical. Concerning legislation mandating the indiscriminate collection of every citizen's call and location records (data retention), the EDPS in court has not been on the side of civil society and downplayed the chilling effect of these policies. And, a proposal to use MEP's fingerprints for registering their attendance in Parliament was green-lighted in principle, although employees have been spared biometrics in view of less intrusive alternatives.

The EDPS hence treads carefully, and it was not lightly that it decided to challenge the legalisation of Europol's illegal bulk- data processing practices in Court, or that it decided to bring together multi-disciplinary international critics in a seminar in the European Parliament on the so-called „chat control" proposal (for a "child sexual abuse Regulation", or CSAR), a bold step only a few days before the vote on the text. I highly value the EDPS' decision not to limit itself to issuing written opinions in these cases.

Based on my experience with the EDPS and his staff throughout this legislature, I am confident that MEPs after me will continue to benefit from the advice offered by a robust and independent institution, which will endure as a beacon of light in a world of digital policy.

Axel Voss

Member of the European Parliament for the European People's Party

Safeguarding Privacy: The Role of EDPS in Upholding Data Protection Rights and its Impact on the European Parliament

In an era dominated by digital advancements and interconnected systems, the protection of personal data has become a paramount concern. The European Data Protection Supervisor stands at the forefront of this mission, actively engaging in activities to safeguard the fundamental right to data protection for individuals within the European Union. The EDPS plays a pivotal role in influencing policies and practices that resonate with the core values of privacy and data security, consequently impacting the work of the European Parliament.

The EDPS operates as an independent supervisory authority, ensuring that EU institutions and bodies comply with data protection regulations, especially in one of its primary functions to monitor and enforce adherence to the General Data Protection Regulation. Through a combination of guidance, recommendations, and audits, the EDPS scrutinises the data processing activities of EU institutions, fostering a culture of accountability and transparency.

By actively engaging with the European Parliament, the EDPS contributes to the legislative process to align them with evolving data protection standards. The EDPS provides valuable insights and recommendations, shaping the legal landscape to better protect the privacy of EU citizens. In doing so, the EDPS contributes to the creation of laws that reflect the dynamic nature of technology and its impact on personal data.

The EDPS also plays a vital role in raising awareness about data protection issues amongst Members of the European Parliament and the public, including on emerging threats, best practices, and the importance of a robust data protection framework. Another important point is the task to strike a balance between privacy and broader societal interests, such as security. In such a delicate discussion, the EDPS has been a key actor. This proactive approach fosters a more informed and vigilant decision-making process, better equipped to navigate the complexities of data-driven issues.

Moreover, the EDPS acts as a watchdog, investigating complaints and incidents related to data protection breaches within EU institutions. By holding these entities accountable for their actions, the EDPS not only ensures justice for affected individuals but also sets a precedent that reinforces the significance of upholding data protection rights.

As MEPs work towards crafting policies that balance technological innovation with individual privacy, they rely on the guidance and expertise provided by the EDPS. This cooperation is essential to create a regulatory environment that not only facilitates progress but also safeguards the fundamental right to data protection for all EU citizens. Therefore, I would like to thank the EDPS for its work, the dedication and cooperation and wish the EDPS a very happy anniversary.

Giovanni Buttarelli

Assistant Supervisor (2008-2014), EDPS (2014-2019)

Choose Humanity: Putting Dignity Back into Digital

Ladies and gentlemen, let me welcome you to the public session of the 40th edition of the International Conference of Data Protection and Privacy Commissioners.

I would like to talk to you about what to expect today and tomorrow, and about why your presence here to discuss Digital Ethics is so crucial.

This is not a privacy or data protection conference. Rather, it is a conference about the human values that underpin privacy and data protection.

Make no mistake: Privacy is a universal value.

Some people might try to tell you it is dead.

I suggest you ask those people if they have ever used a 'do not disturb' sign in a hotel, if they have curtains or shutters at home, or indeed, if they ever wear clothes.

Privacy is in fact an evolutionary trait - and it is not even unique to homo sapiens.

Individuals need their own space, physical and mental, and room to think and create and develop their own personalities.

Society is expected to respect this need for privacy. The basic need for privacy does not evolve. What does evolve, however, is how respect for privacy is shown.

A quarter of a century ago, there was a generational shift in the consensus around how to respect privacy. That generational shift was marked by the emergence of rules governing the protection of personal data.

Back then, a certain green and innocent Italian judge published a critique of the new Italian data protection law. It was entitled 'Databases and the supervision of confidentiality.'

Data protection came in response to the growing computational power and availability of information systems.

The ability to collect and use large amounts of information, and the profitability of collecting and using these data, have consequences for individual freedom and privacy.

So, data protection laws established rights for people concerned by the data. They established requirements for those profiting from the use of the data.

And they established mechanisms for supervision and enforcement, to ensure that these rights and obligations were a practical reality on the ground.

I would like to suggest to you, today, that we are now living through a new generational shift in the respect for privacy.

This shift is towards establishing a sustainable ethics for a digitised society. It is driven by the globalisation of the economy, and the socio-technological forces, which Maria Farrell has just so eloquently described.

It is driven by the digitisation of almost everything in our economy and services sector, our social relations, politics and government.

Above all, it is driven by the prospect of human decision-making, responsibility and accountability being delegated to machines.

Digitisation respects no geographical boundaries. Digitisation is not sensitive to human boundaries between what we want to be public, private or something in between.

It injects itself into our most intimate spaces – relationships, communications and attention.

The so-called "privacy paradox" is not that people have conflicting desires to hide and to expose. The paradox is that we have not yet learned how to navigate the new possibilities and vulnerabilities opened up by rapid digitisation.

What do I mean by ethics? Ethics is the sense we all have, often subconscious, of right and wrong in different circumstances.

Philosophers on this stage will shortly explain how ethical consensuses have emerged in the past.

In today's digital sphere, however, there is no such ethical consensus. We do not have a consensus in Europe, and we certainly do not have one at a global level.

But we urgently need one.

Because digital technologies and data flows are already intensely global.

This is a "50-50" moment for humanity in the digital age - a tipping point - where half of the world's population is connected to the internet.

In the words of cyberpunk novelist William Gibson, "The future is already here, it's just not very evenly distributed."

To cultivate a sustainable digital ethics, we need to look, objectively, at how those technologies have affected people in good ways and bad; we need a critical understanding of the ethics informing decisions by companies, governments and regulators whenever they develop and deploy new technologies.

Technology is still, for now, predominantly designed and deployed by humans, for purposes defined by humans. But we are fast approaching a period where design, deployment and control of new technologies and technological processes are delegated to machines.

Let me point to five case studies to illustrate what I mean.

First, killer drones: Automated machines, which, without human agency, can take the life of a human being. At the UN last month, delegates were unable to reach agreement even to start discussions on how to control them.

Second, algorithmic decision-making in criminal sentencing. This submits individuals to life-changing decisions based on opaque criteria with little or no due process. In fact, when asked to disclose the factors leading to decisions, software vendors have claimed those considerations are subject to proprietary IP protection.

Third, the role of social media whose unaccountable algorithmic decision-making has been weaponised by bad actors in ethnic conflict zones, with at times appalling human consequences, notably in Myanmar.

Fourth, consider the block chain. It is still unclear whether the hype surrounding it is justified. But if its current rate of growth continues, block chain technologies will generate as much carbon emissions worldwide as the whole of the United States.

And fifth, the question of rights for robots. This Parliament at the beginning of this year passed a resolution, which – very thoughtfully – anticipated advances in robotics and the eventual need for framework of rights.

But before we start to think about humanised robots of tomorrow, are we considering the "robotised humans" of today? - The rights of people working in warehouses and having their every movement tracked and recorded; human beings who are guided by machines from shelf to shelf according to a logic, which makes sense only to the machine.

And our leisure time is spent on what machines determine we should see. Auto play and recommendations – automated, algorithmic decisions – are responsible for 70% of online video viewing.

All around the world, the most vulnerable individuals are the objects of manipulation through technological applications.

These and countless more practices, even if lawful, have profound effects for people, societies and the environment.

They call into question basic notions of human dignity. Those responsible for these phenomena may be well intentioned. But their ethics are deeply questionable.

These examples illustrate how we are witnessing a state of cognitive dissonance on a global scale.

We need to ask whether our moral compass been suspended in the drive for scale and innovation.

At this tipping point for our digital society, it is time to develop a clear and sustainable moral code.

That is why I wanted this year's public session of the conference to be different.

Yes, 2018 is the year of the GDPR, the year of the modernisation of Convention 108, the year that Brazil became the biggest country in the world (by population) to have a national general data protection law.

But this is not a conference about privacy or emerging technologies. There are plenty of excellent events elsewhere, dedicated to these themes.

This conference is different in several ways: It is the first time that it has been hosted by an independent body within a supranational entity like the EU. Second, all of our discussions will be together, in this room, with no breakouts or parallel sessions. Third, we have a single theme. Each session has been designed to inform and inspire ideas on how to realise the latest generational shift towards ethics. Lastly, there are no sponsors.

Everything you see here is funded from registration fees and from our own small allocation of the EU budget. As host of the conference, the EDPS has adopted this approach not as a criticism of other conferences, but because we wanted to offer something new.

The International Conference has consisted of a conversation among a tight-knit regulatory community, followed by a networking opportunity with industry, academia and civil society representatives from outside.

I would like us to be more ambitious, to facilitate more engagement with important issues.

So this year, for the first time, the central theme of the closed session, ethics and AI, is directly connected to the theme of the public session.

The decisions taken yesterday mean that this conference will grow and consolidate in ways that will reinforce cooperation on a global scale.

But with this edition, our aim, as a community of regulators, is to send ourselves a signal. It is a signal that we must interact much more with people from outside our comfort zone, from outside the (still) small world of data protection experts.

Enforcement is essential, and we must never lower our guard as data protection authorities.

But at the same time, we must continue to be fully aware of the potential strategies for the evolution of new technologies. Just as we did yesterday adopting a historic document on Artificial Intelligence.

And just like in the Vatican, there are currently two living popes, tomorrow you will hear more about our deliberations from two impressive Chairs of the International Conference.

Because the more often we think out of the box, the better we will perform as data protection regulators.

One such out of the box experiment is the 'Creative Café' tomorrow morning, bringing together 30 of the most highly qualified experts from different fields from around the world ,to think collectively about the next stage of discussions digital ethics.

This conference's focus on ethics does not come "out of the blue". It is fruit of several years of reflection.

Our Opinion 'Towards a New Digital Ethics' in 2015 highlighted the potential impact on human dignity of new technologies like drones, smart cities and 3D bio printing.

'Technology', we asserted, 'should not dictate values and rights, but neither should their relationship be reduced to a false dichotomy.'

Following that opinion, we set up an independent expert advisory group on ethics.

We hosted two workshops first with data protection experts and then with the wider scientific community.

This year we launched a public consultation on digital ethics.

In parallel, in 2015, we tabled before the Executive Committee of the International Conference our proposal for a public session dedicated to ethics.

And the following year we prepared a discussion paper on AI at the 2016 edition in Marrakech, which was the trigger for the report and resolution adopted yesterday.

It is fair to say that the early reactions to this idea of a global debate on ethics were mixed.

Regulators were sceptical because it did not seem to be a priority in a period of sweeping legislative change. Other regulators were worried that ethics might become a 'Trojan Horse', which would debilitate laws like the GDPR from the inside.

Some companies were worried about ethical 'gold plating', adding further compliance burdens to existing legal obligations. Other companies by contrast saw opportunities to equate ethics with flexibility and vagueness – a chance to dilute their responsibilities towards individuals and society.

Some saw an opportunity to weaken controls on the invasive powers of intelligence and law enforcement agencies.

None of these interpretations reflect what I had in mind.

So why are we hosting this debate on ethics? My youngest daughter told me that I ran the risk of becoming a moral preacher, a sort of reincarnation of the uncle of Spiderman. And perhaps, she was not the only one to think so a few years ago.

It is a bit like the president of the European Central Bank, who last week said, according to reports, "My job is to be worried and to worry everybody else."

80% of respondents in our public consultation said that ethics was going to become more and more central to discussions about digital technology, markets and regulation.

Now, I am aware that some very distinguished privacy experts argue against entering into the uncertain domain of ethics and philosophy.

For them, it is enough to have rules on lawfulness, proper use of consent and appropriate use of legitimate interest, with the general principle of accountability as envisaged in the GDPR.

But I am not so sure.

The fact is that the European legislator did not think about ethics when it drafted the GDPR. In fact, the regulation only refers three times to ethical considerations in specific professions, like research.

This is not a criticism of the GDPR. It is a reality check on the limitations of any law, even a comprehensive one.

Laws establish the minimum standard. Best practices are assumed to go beyond the minimum standard.

So for me, compliance with the law is not enough. What then is the relationship of ethics and the law?

From my perspective, ethics come before, during and after the law. It informs how laws are drafted, interpreted and revised. It fills the gaps where the law appears to be silent.

Ethics is the basis for challenging laws. Remember that slavery was legal. Child labour and censorship are still legal in many jurisdictions.

We tackle these injustices on the basis of ethics.

What has all this got to do with data protection authorities? According to the results of our consultation, 86% of respondents believe authorities should play a role in the governance of digital ethics.

Privacy professionals on the ground in business and public bodies are rightly commended for developing a range of compliance tools, and these can be adapted as ethical norms emerge.

But self-regulation alone is not the solution. For us as data protection authorities, I believe that ethics is among our most pressing strategic challenges.

We have to be able to understand technology, and to articulate a coherent ethical framework. Otherwise, how can we perform our mission to safeguard human rights in the digital age?

How will this debate unfold, during our conference and beyond? What do I expect from the debate today and tomorrow?

We are seeking a broad and inclusive debate, not just about the role of industry but that of the state and scientific research.

We have filled this great debating chamber, which serves as the house of representatives of the largest transnational democratic electorate in the world.

The MEPs are meeting in plenary now in Strasbourg and they are due to adopt a resolution on the power of platforms and to call for a complete audit of their market power.

Next year across the European Union, there will be elections to this house, as well as general or presidential elections in 13 Member States of the EU.

Never before has democracy itself been so clearly dependent on the lawful and fair processing of personal data.

For the evangelists of the Fourth Industrial Revolution of big data and AI, dignity and respect are the biggest concerns. That was clear from this year's World Economic Forum in Davos.

Expect this conference to echo the responses to our consultation and mention, for instance solidarity, a fair digital dividend, polarisation and negative impacts on social stability, the concentration of power, the structural inability of people to benefit from their own data, uneven access to new technologies, and algorithms creating societies in which everyone is automatically scored and classified.

We will discuss why we need to go beyond the law.

Another thing is clear. The GDPR is about the rights of the individual. But the more personal data processing affects the collective interest, the less we can look to the GDPR for answers.

Perhaps ethics will fill that void.

I do not want to prejudice the discussion with my own ideas on what a digital ethics should look like. But allow me simply to reiterate my point of departure, which is that not everything that is legally compliant and technically feasible is morally sustainable.

Privacy has too easily been reduced to a marketing slogan. But ethics cannot be reduced to a slogan. To say 'We are an ethical organisation' without a thorough understanding is hollow.

Ethics is deep-seated. Ethics is often subconscious, but it informs the decisions that we take as humans. What we need to do is understand the ethics behind certain practices and, if necessary, challenge them.

To conclude, I would encourage you to participate actively in this debate and help to deepen it after the conference.

All revolutions have victims. So in the Fourth Industrial Revolution, who are the winners and losers?

How can we develop a positive relationship with new technologies, which puts people and dignity at the centre?

This is about defining the values of the future. And we have to do it before it is too late.

So thank you for being here.

Thank you for listening to me and to the wonderful speakers to follow. And thank you to President Tajani, to the interpreters and to all staff in the Parliament who have allowed us to meet here.

I hereby declare open the 40th edition of the Olympic Games of Data Protection.

Building a new independent institution for data protection

17 January 2004 – 23 December 2008

The EDPS starts its work under the leadership of Peter Hustinx as the first European Data Protection Supervisor and Joaquín Bayo Delgado as the Assistant Supervisor.

© Urząd Ochrony Danych Osobowych

Peter Hustinx, European Data Protection Supervisor (2004-2014) attends the International Data Protection and Privacy Commissioners' Conference (todays' Global Privacy Assembly) in Wrocław, Poland, 12 September 2004

© European Data Protection Supervisor

EDPS participates in the European Parliament's Committee on Civil Liberties, Justice and Home Affairs in Brussels, Belgium, 12 July 2005

© European Data Protection Supervisor

Peter Hustinx, European Data Protection Supervisor (2004-2014) meets European Ombudsman Paraskevas Nikiforos Diamandouros (2003-2013) in Brussels, Belgium, 2006

EDPS participates in Data Protection Day in Brussels, Belgium, 2007

Peter Hustinx, European Data Protection Supervisor (2004-2014) and EDPS members of staff, 2008

© European Union

Peter Hustinx, European Data Protection Supervisor (2004-2014) at the European Parliament's Committee on Civil Liberties, Justice and Home Affairs with industry and consumers representatives in Brussels, Belgium, 2008

© European Data Protection Supervisor

Peter Hustinx, European Data Protection Supervisor (2004-2014) and Joaquin Bayo Delgado, Assistant Supervisor (2004-2008) and EDPS staff visiting the Civil Service Tribunal in Luxembourg, 2008

© European Data Protection Supervisor

Peter Hustinx, European Data Protection Supervisor (2004-2014) interviewed by Arte in Brussels, Belgium, 2008

Joaquín Bayo Delgado, Assistant Supervisor (2004-2008) leaves the EDPS in Brussels, Belgium, 2009

Towards excellence in data protection

23 December 2008 – 4 December 2014

Building on the first mandate's success, Peter Hustinx is reappointed as the European Data Protection Supervisor, with a new Assistant Supervisor, Giovanni Buttarelli.

Peter Hustinx, European Data Protection Supervisor (2004-2014) speaking at Privacy Forum in Brussels, Belgium, 28 March 2012

Peter Hustinx, European Data Protection Supervisor (2004-2014) signs Memorandum of Understanding with Brian Gray, European Commission's Internal Audit Service in Brussels, Belgium, 29 May 2012

© European Data Protection Supervisor

From left to right: Paul De Hert, Full Professor at the Vrije Universiteit Brussel, Peter Hustinx, European Data Protection Supervisor (2004-2014), Willem Debeuckelaere, President of the Data Protection Authority of Belgium (2007-2019) and Giovanni Buttarelli, European Data Protection Supervisor (2014-2019), participate in a Privacy Exhibition in Denmark, 13 January 2013

EDPS Staff in Brussels, Beligum, 2013

© European Data Protection Supervisor

Giovanni Buttarelli, Assistant Supervisor (2008-2014) and European Data Protection Supervisor Peter Hustinx (2004-2014) in Brussels, Belgium, 2013

© European Data Protection Supervisor

Herke Kranenborg, Head of Litigation and Legislative Policy at the EDPS and Peter Hustinx, European Data Protection Supervisor (2004 - 2014) attend the hearing on fundamental rights at the European Parliament in Brussels, Belgium, 10 November 2011

Peter Hustinx, European Data Protection Supervisor (2004-2014) and Giovanni Buttarelli, Assistant Supervisor (2008-2014) present their 2013-2014 Strategy "*Towards excellence in data protection*" in Brussels, Belgium 22 January 2013

From left to right: Giovanni Buttarelli, Assistant Supervisor (2008-2014), Peter Hustinx, European Data Protection Supervisor (2004-2014) and Christopher Docksey, EDPS Director (2010-2017) in Brussels, Belgium, 2014

Peter Hustinx, European Data Protection Supervisor (2004-2014) and Giovanni Buttarelli, Assistant Supervisor (2014-2018) in Brussels, Belgium, 2014

Peter Hustinx, European Data Protection Supervisor (2004-2014) celebrates his mandate, December 2014

Leading by example

4 December 2014 - 20 August 2019

Giovanni Buttarelli is appointed as the new European Data Protection Supervisor with Wojciech Wiewiórowski as Assistant Supervisor.

© European Data Protection Supervisor

Wojciech Wiewiórowski, Assistant Supervisor (2014-2019) Peter Hustinx, European Data Protection Supervisor (2004 - 2014), and Giovanni Buttarelli, European Data Protection Supervisor (2014-2019) in Brussels, Belgium, 14 December 2014

Frans Timmermans, First Vice-President of EU Commission in charge of Better Regulation, Inter-Institutional Relations, Rule of Law, Charter of Fundamental Rights (2014-2019) and Giovanni Buttarelli, European Data Protection Supervisor (2014 - 2019), meet at the presentation of the EDPS strategy *"Leading by example: EDPS 2015-2019"* in Brussels, Belgium, 02 March 2015

© European Data Protection Supervisor

EDPS participates in the Spring Conference of Data Protection Authorities in Manchester, United Kingdom, 18 May 2015

© European Data Protection Supervisor

Giovanni Buttarelli, European Data Protection Supervisor (2014 - 2019) speaks at a discussion on "*Delegation Procedure: lack of transparency or European democracy at risk?*" at the Economic and Social Committee in Brussels, Belgium, 26 May 2015

© European Data Protection Supervisor

© European Data Protection Supervisor

Giovanni Buttarelli, European Data Protection Supervisor (2014 - 2019) and Wojciech Wiewiórowski, Assistant Supervisor (2014 - 2019), work together in Brussels, Belgium, 2016

Giovanni Buttarelli, European Data Protection Supervisor (2014-2019) interviewed by The Economists in Brussels, Belgium, 24 February 2016

© European Data Protection Supervisor

Giovanni Buttarelli, European Data Protection Supervisor (2014 - 2019) oversees the implementation of Europol's new legal framework in The Hague, Netherlands, 19 May 2016

Giovanni Buttarelli, European Data Protection Supervisor (2014 - 2019) and Tim Cook, Apple CEO, at the International Conference of Data Protection and Privacy Commissioners (ICDPPC) organised by the EDPS in Brussels, Belgium, 22-26 October 2018

EDPS hosts International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Brussels from 22-26 October 2018

© European Data Protection Supervisor

Giovanni Buttarelli, European Data Protection Supervisor (2014-2019) passes away, 20 August 2019

© European Data Protection Supervisor

Shaping a safer digital future

6 December 2019 - 5 December 2024

Wojciech Wiewiórowski, EDPS Assistant Supervisor (2014-2019),
and former Commissioner of the Data Protection Authority of Poland,
is appointed as the new European Data Protection Supervisor.

Wojciech Wiewiórowski, European Data Protection Supervisor (2019-2024) meets with David Sassoli, President of the European Parliament (2019 - 2022) in Brussels, Belgium 19 February 2020

The EDPS, together with the EDPB representing the EU in the G7 Roundtable of data protection and privacy authorities gathering also data protection and privacy authorities of Canada, France, Germany, Italy, Japan, the United Kingdom and the United States of America in Bonn, Germany, 6 September 2022

Wojciech Wiewiórowski, European Data Protection Supervisor (2019-2024) meets Roberta Metsola, President of the European Parliament (2022-2024) in Brussels, Belgium, 26 October 2022

© European Union

© European Union

Wojciech Wiewiórowski, European Data Protection Supervisor (2019-2024) meets with Síofra O'Leary, President of the European Court of Human Rights (2022-2025) in Strasbourg, France, 14 March 2023

European Data Protection Supervisor Wojciech Wiewiórowski (2019-2024) at the Conference of International Association of Privacy Professionals in Washington DC, USA, 25 April 2023

© European Data Protection Supervisor

EDPS and EDPB meet with the public during the EU Open Day at the European Commission in Brussels, Belgium, 06 May 2023

EDPS, Thomas Zerdick, Head of Unit 'Supervision and Enforcement' at the EDPS, and Bénédicte Raevens, Legal officer at the EDPS, meet with the network of data protection officers of the EU institutions, bodies, offices and agencies in Alicante, Spain, 12 May 2023

EDPS organises a Seminar on the Child Sexual Abuse Material Proposal: "*The Point of No Return?*" at the European Parliament in Brussels, Belgium, 23 October 2023

© IOW

EDPS co-organises International Organisations Workshop with Interpol in Lyon, France, 25 October 2023

Wojciech Wiewiórowski, European Data Protection Supervisor (2019-2024) and John Edwards, UK Information Commissioner, sign Memorandum of Understanding in Brussels, Belgium, 8 November 2023

© European Data Protection Supervisor

Publications Office
of the European Union

Print ISBN 978-92-9242-823-5 doi:10.2804/209010 QT-05-23-438-EN-C
PDF ISBN 978-92-9242-824-2 doi:10.2804/652641 QT-05-23-438-EN-N