



EUROPEAN DATA PROTECTION SUPERVISOR

Annual Activity Report

2021

Contents

1.	Introduction	4
2.	Operational achievements.....	5
2.1	The EDPS in 2021	5
2.1.1.	Data Protection in a global health crisis	5
2.1.2.	Leading by example in safeguarding EU digital rights	6
2.1.3.	Shaping a safer digital future for the EU	16
2.1.4.	The EDPS as a member of the EDPB	20
2.1.5.	International cooperation in data protection	22
2.2	The EDPB in 2021	23
2.2.1.	EDPB Strategy 2021-2023 and Work Programme 2021-2022.....	24
2.2.2.	Meetings	26
2.2.3.	Guidelines, Opinions, Decisions and other documents	26
2.2.4.	Stakeholder engagement	32
2.2.5.	The EDPB Secretariat contribution to the national SAs' cooperation.....	33
2.2.6.	IT communications tool (Internal Market Information) & the new EDPB website	34
2.2.7.	The EDPB Secretariat activities relating to access to Documents.....	35
2.2.8.	The EDPB Secretariat activities relating to Data Protection Officer activities	35
2.2.9.	Coordinated Supervision Committee	36
3.	Resource management	38
3.1.	The EDPS Ethics Framework Activities	38
3.2	Human resources	39
3.2.1	Management of the Covid-19 crisis and reflection on a back to the office strategy	40
3.2.2	Internal coaching and organisation of wellbeing actions for staff (New Wellbeing coordinator role).....	40
3.2.3	Automation of HR processes	41
3.2.4.	Launch of a new Data protection specialist competition.....	41
3.3	Budget	41
3.3.1.	Allocated budget for 2021.....	41
3.3.2.	Budget execution 2021.....	42
3.3.3	Working methods.....	42
3.3.4	Draft budget 2022 exercise	43
3.3.5.	Discharge 2019 Budget	43
3.3.6	Staff.....	43
3.4	Procurement and contracting.....	43
3.4.1	Professionalization	43
3.4.2	Framework contracts and concluded contracts	44
3.5.	Finance	45
3.6	Missions management	46
4.	Management and internal control.....	47
4.1	Characteristics and nature of activities	47
4.1.1	The mission of the EDPS	47
4.1.2	Core values and guiding principles	49
4.1.3	Data Protection and the EDPS in 2021	49
4.2	Strategy 2020-2024	51
4.2.1	EDPS strategic objectives	51
4.2.2	Action plan.....	51
4.2.3	Measuring performance	51
4.3	Inter-institutional cooperation	52
4.4	Ex post controls	53
4.5	Events during the year that affected reputation	53
4.6	Internal control management system	54
4.7	Internal evaluation of the internal control system and indicators underpinning the statement of assurance	55
4.8	Cost effectiveness and efficiency of Internal Control	55
4.9	Results of independent audit during the year	56

4.9.1 Court of Auditors	56
4.9.2 Internal Audit Service (IAS)	59
4.9.3 ICS monitoring situation	60
4.9.4 Follow-up to the European Parliament's discharge resolution of 2020	60
4.10 Conclusions on the effectiveness of internal control	61
5. Reservations and impact on the statement	61
5.1 Materiality criteria	61
5.1.1. Objectives of materiality criteria	61
5.1.2. Qualitative criteria.....	61
5.1.3. Quantitative criteria.....	62
5.1.4. Criteria of the Internal Audit Service	62
5.2 Reservations	62
5.3 Conclusion.....	62
6. Statement of assurance from the authorising officer by delegation.....	62
7. Annexes.....	64
Annex 1: Summary of annual activity report.....	64
Annex 2: Human resources at the EDPS	65
Annex 3: Budget 2021	67
Annex 4: Detailed list of missions undertaken by the Supervisor (2021)	70
Annex 5: EDPS strategic objectives	71
Annex 6: EDPS strategic objectives and its Action Plan	72

1. Introduction

The Financial Regulation (Article 74.9¹) provides that each **authorising officer by delegation** (AOD) shall send an annual activity report to their institution, together with financial and management information. This report shall present the achievements of their institution in relation to the resources used. It shall also be a management report on performance in the context of their task as AOD. This requirement is the logical consequence of paragraph 2² of this same article, which gives the AOD responsibility for internal controls.

In the annual activity report of the AOD, this latter must include a statement of assurance ("Statement") based on their own judgment and on the information available in which the AOD:

- states that the information contained in the report gives a true and fair view;
- declares that the AOD has reasonable assurance that the resources allocated to the activities described in the report have been used for their intended purposes and in accordance with principles of sound financial management, and that the control procedures put in place give the necessary guarantees as to the legality and regularity of the underlying transactions;
- confirms that the AOD is not aware of any matter not reported which could harm the interests of the institution.

¹ Financial Regulation, Article 74(9): The authorising officer by delegation shall report to his or her Union institution on the performance of his or her duties in the form of an annual activity report containing financial and management information, including the results of controls, declaring that, except as otherwise specified in any reservations related to defined areas of revenue and expenditure, he or she has reasonable assurance that:

- (a) the information contained in the report presents a true and fair view;
- (b) the resources assigned to the activities described in the report have been used for their intended purpose and in accordance with the principle of sound financial management; and
- (c) the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

The annual activity report shall include information on the operations carried out, by reference to the objectives and performance considerations set in the strategic plans, the risks associated with those operations, the use made of the resources provided and the efficiency and effectiveness of internal control systems. The report shall include an overall assessment of the costs and benefits of controls and information on the extent to which the operational expenditure authorised contributes to the achievement of strategic objectives of the Union and generates EU added value. The Commission shall prepare a summary of the annual activity reports for the preceding year.

The annual activity reports for the financial year of the authorising officers and, where applicable, authorising officers by delegation of Union institutions, Union bodies, European offices and agencies shall be published by 1 July of the following financial year on the website of the respective Union institution, Union body, European office or agency in an easily accessible way, subject to duly justified confidentiality and security considerations.

² Financial Regulation, Article 74(2): For the purposes of paragraph 1 of this Article, the authorising officer by delegation shall, in accordance with Article 36 and the minimum standards adopted by each Union institution and having due regard to the risks associated with the management environment and the nature of the actions financed, put in place the organisational structure and the internal control systems suited to the performance of his or her duties. The establishment of such structure and systems shall be supported by a comprehensive risk analysis, which takes into account their cost effectiveness and performance considerations.

2. Operational achievements

2.1 The EDPS in 2021

2021 was the second year of the COVID-19 pandemic, and like many other organisations, the EDPS had to adapt its working methods as an employer as well as its priorities, since the COVID-19 pandemic strengthened the call for the protection of individuals' privacy with the appearance of contact tracing apps and other technologies used for the fight against the coronavirus. While technology can certainly contribute to limiting the spread of the virus, the EDPS' priority is to ensure the protection of individuals' personal data and right to privacy.

The EDPS' [Strategy for 2020-2024](#) overarching aim is to shape a safer digital future, with three core pillars outlining the guiding actions and objectives for the organisation to the end of 2024: **Foresight, Action and Solidarity**. These three pillars, and our strategy as a whole, were the driving force for our work in 2021.

2.1.1. Data Protection in a global health crisis

Following the outbreak of the COVID-19 pandemic, the EDPS immediately established an internal [task force](#) to actively monitor and assess both the EU's and EU Institutions (EUIs) responses to the outbreak. Throughout 2021, the COVID-19 task force has been following developments and preparing for the future of data protection and privacy after the COVID-19 crisis.

From the outset of the COVID-19 pandemic, [the EDPS emphasised](#) the need for a pan-European approach in tackling the pandemic. In addition to providing guidance to EUIs, the EDPS closely cooperated with other Members of the European Data Protection Board (EDPB) to offer practical guidance in relation to the most pressing challenges of the pandemic. Among other important points covered in its guidance, the EDPS stressed that pandemic-related technologies requiring the processing of personal data must be temporary, have a defined and limited purpose, and comply with EU data protection law.

Moreover, throughout 2021, the EDPS has been involved in various activities relating to the assessment of actions, initiatives and proposals by EUIs as controllers, together with the evaluation of proposed technological solutions to fight the COVID-19 pandemic and the issuance of guidance for EUIs in order to assist the EUIs to adequately fight the pandemic, while ensuring compliance with data protection law.

The EDPS has also been consulted both informally and formally by the legislator on numerous COVID-19 related legislative initiatives. Amongst such initiatives, the EDPS has also issued a Joint Opinion together with the EDPB on a Proposal for a Regulation of on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (now EU Digital COVID-19 Certificate)³ (Opinion 4/2021).

³ https://edpb.europa.eu/system/files/2021-04/edpb_edps_joint_opinion_dgc_en.pdf

Lastly, the EDPS has actively engaged in working on the longer- term consequences of the pandemic and measures taken to fight it. To this end, the EDPS organised a [webinar on 'Data for the public good: building a healthier digital future'](#), aimed at exploring the impact of measures taken in response to the COVID-19 pandemic and identifying ways in which data can be used to be better prepared for the next crisis.

Through its work, the EDPS will continue to ensure that the fundamental rights of data protection and privacy are embedded in each solution envisaged to overcome any obstacle due to the COVID-19 pandemic and effectively and efficiently use data for the public good.

2.1.2. Leading by example in safeguarding EU digital rights

In 2021, the EDPS continued its efforts to supervise Union institutions, bodies, offices and agencies' (EUIs) compliance with data protection laws. As outlined in our Strategy 2020-2024, we are determined to support EUIs to continue to lead by example in safeguarding digital rights and responsible data processing. Examples of several initiatives the EDPS has worked on in 2021, and will continue to work on during this mandate, are described below.

1. Strategic actions concerning transfers of personal data outside of EU/EEA after the Schrems II judgment

Following the Court of Justice of the European Union's "Schrems II" judgment in July 2020 (case C-311/18), the EDPS' launched various initiatives. The EDPS continued to put in place the measures set out in the EDPS' [Strategy for EU institutions to comply with the "Schrems II" judgment \(EDPS' Schrems II Strategy\)](#), published on 29 October 2020. The strategy aims to ensure and monitor compliance of EU institutions, bodies, offices and agencies (EUIs) with the judgment concerning transfers of personal data to non-EU/EEA countries, and in particular, the United States. The strategy builds on cooperation and accountability of controllers as well as on the use of corrective powers, including suspensions and bans of transfers to ensure compliance. As part of the strategy, the EDPS is pursuing three types of actions in parallel: investigations; authorisations and advisory work; and guidance to assist the institutions in discharging their duty of accountability. Such an extensive exercise in monitoring EUIs compliance with Regulation (EU) 2018/1725 and the reinforced cooperation with EUIs, national DPAs and international organisations on transfers, require dedicating special resources and expertise in international transfers.

a) EDPS investigations following the Schrems II judgment

As part of our enforcement actions following the publication of the EDPS' Schrems II Strategy in October 2020, the EDPS developed an action plan to streamline compliance and enforcement measures, distinguishing between short-term and medium-term compliance actions.

Our strategy builds on the cooperation and accountability of controllers to assess, in line with the Court's ruling, whether the ***essentially equivalent standard of protection*** is guaranteed when personal data is transferred to (or remotely accessed by) recipients in

non-EU/EEA countries. Two priorities should be addressed in the short-term: ongoing controller to processor contracts and/or processor to sub-processor contracts involving transfers of data to non-EU/EEA countries. As a first step, we ordered in October 2020 that EUIs map their ongoing transfers of personal data to non-EU countries in the context of contractual relationships and report on certain categories of those transfers to the EDPS.

The analysis of the information reported to the EDPS confirmed that a prominent part of data transfers are directed towards the United States and towards recipients that may be subject to problematic US surveillance laws⁴, raising critical compliance issues with Regulation 2018/1725. In particular, the analysis showed that EUIs increasingly rely [on cloud-based software and cloud infrastructure or platform services from large ICT providers](#), of which some are based in the US and are therefore subject to legislation that, according to the [“Schrems II” judgment](#), allows disproportionate surveillance activities by the US authorities.

As part of the strategy, the EDPS launched two investigations on 27 May 2021. These investigations were aimed to ensure that any ongoing and future international transfers by EUIs and on their behalf are carried out in accordance with EU data protection law. One investigation focuses on the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EUIs, while the other investigation focuses on the use of Microsoft Office 365 by the European Commission. The two investigations are continuing in 2022.

The objective of the first investigation is to assess EUIs’ compliance with the “Schrems II” Judgement when using cloud services provided by Amazon Web Services and Microsoft under the so-called “Cloud II contracts” when data is transferred to non-EU countries, in particular to the US. We underline that, although *the* “Cloud II contracts” were signed in early 2020 before the “Schrems II” judgment and that both Amazon and Microsoft have announced new measures with the aim to align themselves with the judgment, these announced measures may not be sufficient to ensure full compliance with EU data protection law.

The aim of the second investigation into the use of Microsoft Office 365 is to verify the European Commission’s compliance with the [Recommendations](#) previously issued by the EDPS in 2020 on the use of Microsoft’s products and services by EUIs. This also includes compliance regarding international transfers. With these investigations, we aim to help EUIs *improve their data protection compliance when negotiating contracts with their service provider*.

We believe that EUIs are well positioned to lead by example when it comes to privacy and data protection. The announced steps are part of a continuous cooperation between the EDPS and the EUIs to ensure a high level of protection of these fundamental data rights.

The EDPS is also cooperating with the data protection supervisory authorities of EU and EEA Member States, by building on the experience set out in the EDPS’ Schrems II

⁴ Section 702 FISA and EO 12333.

Strategy. In particular, in 2021 the EDPS [proposed](#) the use of cloud-based services by public sector bodies as the topic of the first [coordinated enforcement action](#) of the European Data Protection Board. We proposed this topic in light of the need for closer cooperation and action to ensure compliance with EU data protection laws, in particular with regard to the controller-processor relationship and international transfers when public sector bodies use cloud-based services. The EDPS is actively participating in this coordinated action of the EDPB focusing on supervision of compliance with Regulation (EU) 2018/1725 when EUIs use such services. In 2021, we substantively contributed to the common preparatory work for the coordinated action's kick-off in 2022.

b) EDPS authorisations and advisory work

The Schrems II judgment has also complicated the process of issuing authorisations for EUIs that intend to transfer personal data (including by way of remote access) outside of the EEA. The judgment has far-reaching consequences on all legal tools used to transfer personal data from the EEA to any third country and in particular to the United States. In October 2020, **EDPS strongly advised EUIs against starting any new** processing operations or new contracts with any service providers that would involve **transfers of personal data to the US**. Nevertheless, EUIs that have to transfer personal data to the US and other third countries need in most cases to request the authorisation of the EDPS. This process, which involves a careful analysis of each case and the inclusion of tailor-made conditions for each authorisation decision as well as their monitoring also require extensive resources and special expertise. In 2021, the EDPS dealt with a number of authorisation requests from EUIs under Article 48 of Regulation (EU) 2018/1725.

(i). Authorisation of administrative arrangements to transfer personal data

On 12 May 2021, the EDPS issued the first [Decision](#) on the use of an administrative arrangement as a tool providing appropriate safeguards for the transfer of individuals' personal data to non-EU/EEA countries. The arrangement focused on transfers of individuals' personal data between the European Commission and the [Turkish Medicines and Medical Devices Agency](#) (TMMDA) in the context of the Turkish participation in the EU regulatory system for medical devices [EUDAMED](#). We based our assessment on the European Data Protection Board's [Guidelines](#) for transfers of personal data between EEA and non-EEA public authorities and bodies as these guidelines explain the criteria of the minimum data protection safeguards for such transfers. The EDPS recommended in its Decision that the European Commission amends a number of clauses in the submitted administrative arrangement to ensure that individuals' data is appropriately safeguarded, in particular clauses concerning the purpose for which individual's data may be processed, the transparency towards the individuals on the processing and their data protection rights, the security and confidentiality measures, and the oversight of the processing and redress options for individuals. Concerning the possible access to individuals' personal data by national security or law enforcement authorities, the EDPS reiterated that the Commission – as the data exporter – is responsible for seeking and assessing whether the authorities in Turkey – as data importer – provide sufficient data protection safeguards. The EDPS asked the European Commission to report on an annual basis on how the implementation of the Decision issued is going and to inform the EDPS

without delay of any suspended transfers of data or in the event of a revision or termination of the administrative arrangement with the TMMDA.

On 17 June 2021, the EDPS issued a Decision authorising, subject to conditions, the use of an administrative arrangement between the European Medicines Agency and the Department of Health of Canada concerning to exchange personal data in their capacity as regulators and public authorities responsible for supervision and pharmacovigilance of medicinal products.

On 5 July 2021, the EDPS issued another Decision authorising, subject to conditions, the use of the administrative arrangement between the European Joint Undertaking for ITER and the Development of Fusion Energy and the ITER International Fusion Energy Organization in the context of the implementation of the ITER Agreement.

The follow up to the three EDPS authorisation decisions mentioned above is continuing in 2022.

(ii) [Authorisation of contractual clauses to transfer personal data](#)

On 31 August 2021, the EDPS issued a decision following a request from the Court of Justice of the European Union for authorisation of *ad hoc* contractual clauses between the Court, Cisco International Limited UK and Cisco Systems Inc in the context of transfers of personal data in the Court's use of Cisco Webex and related services. The EDPS authorised the use of *ad hoc* contractual clauses between the Court and Cisco until 30 September 2022, given the special circumstances of the COVID-19 pandemic.

In our findings, we identified several compliance issues. Meanwhile, the Court and Cisco had put in place additional measures and made mutual commitments to take even further specific measures, such as limiting data transfers outside the EU and concrete encryption, which we also assessed and considered in our decision.

The EDPS imposed a few strict conditions that the Court and Cisco are required to put in place to ensure compliance with Regulation (EU) 2018/1725 and to ensure the essentially equivalent level of protection for transferred data. Conditions include:

- locating processing within the EEA;
- concluding additional contractual safeguards;
- measures for the effective encryption of data processed in the EEA;
- measures for the effective pseudonymisation or anonymization of the remaining personal data processed outside the EEA, including through any remote access.

The Court must resolve the compliance issues identified within one year from the date of the decision, following which the EDPS will reassess the transfer authorisation and may order the suspension of data flows. The Court should also provide an intermediary report within six months of the decision date that demonstrates that the conditions included in the EDPS' decision are being put in place. The follow up to the EDPS temporary authorisation decision is thus continuing in 2022.

(iii) Data Protection Impact Assessments for data transfers

On 7 July 2021, the EDPS issued an opinion following a prior consultation request from the European Central Bank (ECB) on its data protection impact assessment (DPIA) concerning a new Customer Relationship Management system for the ECB, based on Microsoft Dynamics 365.

Our Opinion addressed whether mitigating measures identified by the ECB in its DPIA were sufficient to appropriately address the high risks identified by the ECB in relation to its use of Microsoft Dynamics 365:

- (i) non-compliance with the rules on international transfers in light of the Schrems II judgment;
- (ii) lack of control over Microsoft sub-processors;
- (iii) certain limitations of the contract with Microsoft negotiated by the European Commission on behalf of all EU institutions, bodies, offices and agencies (EUIs).

We concluded that the measures envisaged by the ECB were insufficient to mitigate the high risks it had identified. The EDPS found that there were no sufficient guarantees and appropriate safeguards that the processing and transfers of personal data to Microsoft and its sub-processors in the ECB's use of Microsoft Dynamics 365 will meet the requirements of Regulation (EU) 2018/1725 and ensure an essentially equivalent level of protection to that guaranteed in the European Economic Area (the EEA).

The EDPS issued a warning and made several recommendations to assist the ECB in ensuring that the processing of personal data by the ECB, Microsoft and any sub-processors is compliant. These recommendations include assessing new contractual data protection safeguards, as well as on the technical and organisational measures to put in place concerning international transfers to Microsoft or its sub-processors, and assessing alternative solutions to Microsoft Dynamics 365.

c) Training EUI staff on personal data transfers to non-EU/EEA countries

Over the course of 2021, the EDPS gave a series of online advanced lectures at the European School of Administration (EUSA) and other venues for staff members of all EUIs and their DPOs concerning transfers of personal data by EUIs or on their behalf.

An online training session was held on transfers of personal data to non-EU/EEA public bodies and organisations and two sessions on the conditions and data protection safeguards for transfers to non-EU/EEA private entities. Transferring personal data to non-EU/EEA countries may present additional risks for individuals, as these countries may not have the same legislation put in place to ensure that personal data is adequately and sufficiently protected. This is why when transferring individuals' personal data to countries outside the EU/EEA, EUIs have to ensure that the level of protection offered by the country of destination offers an essentially equivalent level of protection as in the EU/EEA. During the training sessions, the EDPS experts gave recommendations on how EUIs need to carry out Transfer Impact Assessments and put in place effective

supplementary measures to ensure an essentially equivalent level of data protection as in the EU/EEA for the data that will be transferred to that recipient in that third country. The EDPS experts emphasised that if no essentially equivalent level of protection is guaranteed by a country of destination, then the transfer of individuals' personal data to that country should not occur.

The EDPS regularly organises training sessions and lectures on challenging topics, such as the topic of international data transfers, for EUIs, their data protection officers, and their members of staff. These training sessions, either organised by the EDPS' own initiative, or at the DPO's request, aim to ensure that EUIs stay up to date with data protection regulation and requirements in their day-to-day activities.

2. Creation of a new Sector for the Supervision of the Area of Freedom, Security and Justice

The EDPS recently gained new powers to supervise those European agencies and bodies active in the Area of Freedom, Security and Justice (AFSJ), namely: Europol, Eurojust, EPPO, Frontex, eu-LISA, and the EUAA. This covers three main EU policies: EU border management, police Cooperation and Criminal justice.

The supervision of the AFSJ brings forth two main challenges. First, although the EU has accumulated a patchwork of measures in the areas of police and judicial cooperation and border management, the legal framework remains fragmented, creating unnecessary discrepancies. This puts unwarranted constraints on the EDPS' supervisory and enforcement powers. In light of this, the EDPS has committed in the 2020-2024 Strategy to identify discrepancies in the standards of data protection within EU law in the AFSJ and to enforce the rules consistently. Second, personal data processing activities in this Area have a high impact on individuals' rights and freedom, for example criminal data or data about migrants. This impact will increase in the coming years with the exchange of personal data through the Interoperability framework and the development of a hit/ no hit between the Information Systems of these agencies and bodies. As the AFSJ bodies' and agencies' activities evolve, more resources from the EDPS are necessary to ensure that individuals' personal data is sufficiently protected.

In order to tackle these challenges, the EDPS created a dedicated Sector within the S&E Unit, with seven data protection experts with working knowledge in the area, who will work in tight collaboration with colleagues in the Technology and Privacy Unit. This will allow the EDPS to identify disparities in the way EU data protection law is applied across all AFSJ bodies and agencies, and to facilitate effective and consistent enforcement where necessary.

a) Follow up on the inquiry regarding Europol's big data challenge

In September 2020, the EDPS concluded its inquiry into the processing of large datasets by Europol and decided to admonish Europol, urging the agency to submit an Action Plan and to inform the EDPS about the measures put in place to address these concerns.

Throughout 2021, the EDPS has engaged in a close follow-up of the measures put in place by Europol to implement their Action Plan and to mitigate the risks posed by this processing. What is fundamentally at stake in these discussions is the risk that people, whose link with criminal activity is not established, are inserted into Europol's systems. To prevent such a risk, the legislator inserted strict safeguards in the Europol Regulation. Namely, by including Annex II.B, the legislator created a requirement that data shared with Europol should only concern individuals' who have a link with criminal activity. This is because transmitting personal data from the level of national police to Europol, where data will be shared with other LEAs and cross-checked with information coming from other countries, significantly magnifies the potential impact and risks for the data subject.

As part of these proceedings, we have had regular exchanges with Europol with regard to the implementation of the action plan, to ensure that the measures put in place fully address the above-described risks with as little delay as possible.

The EDPS considered satisfactory a number of measures being put in place (flagging, labelling, and a separate secure environment for storing large datasets), but identified ongoing areas of concern, following up with detailed feedback, requests for clarification and improvement. Chief among these was the need for Europol to set a more restrictive maximum time limit for the storage of large datasets whose compliance with the Europol Regulation is not established.

In July 2021, the EDPS formally requested Europol to implement retention periods. As the reply from Europol was not satisfactory, the EDPS decided, upon a careful analysis of the existing legislation in place, to use its corrective powers and to impose a 6-month retention period to filter and to extract personal data. Datasets older than 6 months that have not undergone the Data Subject Categorisation must be erased. As a result, Europol will no longer be permitted to extensively retain data about people who do not have an established link to a criminal activity.

On 3 January 2022, the EDPS notified Europol of the decision to delete data concerning individuals with no established link to a criminal activity (so-called Data Subject Categorisation), issued on 21 December 2021. In the spirit of understanding practical needs (such as potential existing backlog), the EDPS granted a 12-month period to comply with the Decision for the datasets received before this decision. Europol was asked to report every 3 months on the actions taken to implement the decision.

b) AI: monitoring the use of pre-trained machine learning models by Europol

In 2021, the EDPS issued his first Opinion related to the use of AI by an EUI.

In February 2021, Europol submitted a prior consultation on the development and use of machine learning models for the operational analysis of a big dataset in the context of a specific Joint Investigation Team (i.e. a specific cross-border criminal investigation) and Europol's support to the involved countries.

On 5 March 2021, the EDPS issued an opinion in which he formulated twenty-one recommendations that Europol should follow in order to avoid possible breaches of the Europol Regulation and, in particular, suggested the establishment of an internal governance framework ensuring that in the course of developing machine learning

models Europol assesses. Recommendations revolved around the need to comply with the necessity and proportionality principle, the data minimisation principle and the data retention principle; to tackle any risks presented to the data subjects as a result of any bias or inaccuracy in the algorithms and in the datasets used; as well as regard the security of the new environment (Europol's suite of machine learning tools) that was set up.

In order to follow up on his Opinion and to check the correct implementation of the recommendations by Europol, the EDPS decided to dedicate part of the 2021 annual inspection of Europol on these issues. The inspection covered Europol's machine learning tool development process and the related data protection risk assessment process.

On 28 October 2021, taking into account the relevance of the machine learning models for the performance of Europol's core tasks and the progress achieved in establishing an internal governance framework for artificial intelligence systems, the EDPS decided to allow the development of such tools upon the requirement that Europol implements specific measures. However, the EDPS required Europol to conclude the relevant data protection impact assessments before making use of these models.

Even if Europol cannot mitigate completely some risks posed by specific processing operations, it is still necessary to identify them and to keep monitoring the latest developments so that those risks are better mitigated as soon as state-of-the-art techniques allow for it. The EDPS will continue to monitor the use of AI by Europol, also in the context of the revised Europol Regulation, which however only obliges Europol to inform the EDPS prior to the launch of research and innovation projects (new article 33a).

3. Overview of remote audits

[Audits](#) are an exercise that the EDPS carries out on a regular basis as the data protection authority of EUIs. Amongst this year's audits, one was carried out remotely due to the COVID-19 pandemic, the rest could again (as in previous years) be carried out on-the-spot (Eurojust, Europol and COVID-related retention periods). The remote audit that we carried out aimed at understanding how EUIs have taken into account the recommendations issued by the EDPS when drafting their Internal Rules under Article 25 of the Regulation, which allow EUIs to restrict data subjects' rights under certain circumstances.

4. Advising and guiding EUIs

a) Opinions and guidance

EUIs may consult the EDPS for guidance on their planned processing operations and on their compliance with data protection law. Depending on the complexity of the EUI's request, the EDPS provides advice in different forms, via calls to the DPO hotline, informal advice to staff and formal signed letters, for example. EUIs may also oblige to consult the EDPS on planned processing operations, particularly when they intend to adopt internal rules restricting individuals' right to data protection and with regard to extra-EU transfers of personal data that require prior authorisation. The EDPS can also issue own-initiative opinions. In total, during 2021 the EDPS issued more than 70 opinions.

Throughout 2021, the EDPS has also continued to monitor the COVID-19 situation and its impact on data protection through its dedicated COVID-19 task force. As the data protection authority of EUIs and as an employer itself, we have produced guidelines on [manual contact tracing](#) and on [return to the workplace](#) and other initiatives to support EUIs in their processing activities during this time.

We also launched a survey with EUIs on the new processing operations and on the IT tools that EUIs introduced to ensure business continuity during the COVID-19 pandemic.

The report is based on an earlier survey and comprises three parts: new processing operations implemented by EUIs; IT tools implemented or enhanced by EUIs to enable teleworking; and new processing operations implemented by EUIs in charge of tasks related to public health. The dynamic evolution of the COVID-19 pandemic means that EUIs must continually adapt their processes. The report aims to support them in what appears to be a long-lasting challenge, which will likely continue to have an impact even after the end of the pandemic. The survey results were summarised in a report (published in March 2022) will feed into updating existing EDPS guidelines, or contribute to the development of new guidelines, depending on the evolution of the pandemic and the new practices that will continue once it is over. The survey results will also inform the EDPS' execution of audits and investigations under [Article 58](#) of Regulation (EU) 2018/1725.

b) Training

Delivering training sessions to EUIs and providing them with the necessary tools to protect individuals' personal data in data processing activities are an integral part of how the EDPS monitors EUIs' compliance with data protection laws.

A number of training sessions are routinely carried out every year. In 2021 almost all training sessions were carried out remotely. These training sessions are usually recorded and made available to all staff of EUIs in the inter-institutional learning platform EU Learn. These training sessions deal with areas in which further clarity or assistance to ensure compliance with Regulation 2018/1725 is required. For example, the EDPS organised several training sessions on international data transfers to public and private entities in third countries, on EUIs' use of social media and information and communication technology tools for remote working, on data protection in procurement and outsourcing, and on personal data breaches in the EUIs. In addition, the EDPS also organised on-demand training sessions requested by EUIs and their DPOs, focusing on data protection operations and their implications in relation to the EUI's core activities and area of business. The training sessions by the EDPS include expert presentations on the subject, case studies and practical examples that staff of EUIs may encounter in their daily work.

In 2021, the EDPS launched an **online course on Data Protection** – EUDPR fast-track training course for practical application in your daily tasks, which was made available in EU Learn to all staff of EUIs. The course provides EUIs' staff with an overview of Regulation 2018/1725 by explaining key concepts and their obligations under this Regulation, as well as giving them practical advice on how to ensure that individuals' personal data that they process is protected. The course is divided into 5 comprehensive modules, covering the basics and more complex notions, as well as giving the EUIs' staff the opportunity to assess

themselves with 38 questions on data protection. Detailed feedback and more information for each question is also available to enhance their learning experience.

Other factsheets on this topic, as well as many other pertinent subjects relevant for EUIs, were published on our website in 2021. A practice that we will continue in 2022 as it is an efficient and accessible way to support DPOs of the EUIs.

In 2021, the EDPS continued to publish our “**Quick News for DPOs**” editions, a monthly newsletter for data protection officers of the EUIs. The DPO newsletter was created in 2019 as we recognise the importance of staying in touch regularly with data protection officers to foster good communication and collaboration, especially during the COVID-19 pandemic. The newsletter provides DPOs with the latest updates on EDPS Guidelines, Recommendations or Opinions directly relevant to their day-to-day work, their EUI’s core business and current data protection developments that concerns them or their institution. While preserving the anonymity of the EUI in question, we also share information about common questions, complaints or consultations that we may have received from an EUI, as these can help DPOs know what measures to put in place if they encounter the same/similar situation. 10 editions of the DPOs Quick News were published in 2021. Some of the topics covered throughout the year include: basic data protection principles; transfers of personal data to non-EU/EEA countries; protecting individuals’ data in the context of recruitment; how to handle employees’ data in the context of a pandemic. The newsletter is also used to promote upcoming training sessions or events organised by the EDPS for Data Protection Officers and other members of staff of EUIs, which DPOs are always encouraged to join. Each edition also includes a data protection recommendation of the month.

5. EDPS meetings with the network of DPOs

Due to the important role played by DPOs as interlocutors between the EDPS and EUIs, a meeting is held twice a year to discuss current and upcoming data protection challenges. This provides an opportunity to realign data protection priorities for the DPOs of EUIs and to identify areas where extra guidance or support from the EDPS is needed.

Two remote EDPS meetings with the network of DPOs were held in 2021, one on 4 June 2021 and one on 14 December 2021.

The [meeting in June](#) covered different workshops and exchanges on current data protection issues such as personal data protection breach notifications, use of software alternatives to large-scale providers, international transfers and cloud services, and better cooperation between the EDPS and DPOs of EUIs.

The [meeting in December](#) focused on how to protect individuals’ personal data in times of COVID-19, with a brief presentation on the results of the EDPS’ 2020 survey on the EUIs’ data processing operations in connection with COVID-19, and with two workshops, organised with the help of DPOs, on manual contact tracing and on access control, in which we reviewed the EDPS’ guidance on COVID-19 matters and EUI’s current practices.

2.1.3. Shaping a safer digital future for the EU

Throughout 2021, the EDPS has closely examined technological developments and multiple initiatives with a meaningful technology footprint and impact on data protection presented by the EU's legislators as well as the use of technology by the EUIs. The EDPS places importance on analysing the possibilities, risks and challenges that up and coming technologies and other initiatives may have on data protection and individuals' personal data in order to shape a safer digital future for the EU, as explained in our EDPS Strategy 2020-2024. An overview of several examples demonstrating this are provided below.

Monitoring technologies

Artificial intelligence and Facial Recognition

Artificial intelligence (AI) is a reality and has woven its way into everyday life: virtual voice assistants, facial recognition, spam filters and recommender systems to name but a few. Of the whole set of technologies the term AI encompasses, machine-learning is possibly the subset with most significant advancements. Machine-learning techniques generally rely on big datasets to achieve good performances. If machine-learning system results are to be applied in a European context, it is also necessary to train them with datasets that are representative of such context. This is creating and increasing thrust to collect and process data (personal and non-personal) for the AI system development. The increased processing of personal data in turn present challenges for privacy and data protection.

Contribution to the debate on Digital Sovereignty

On 27 January 2021, the EDPS organised a panel at the CPDP entitled "Enhancing Personal Data Protection through Digital Sovereignty". The discussion explored the progress and the public and private sector support for EU sovereign Infrastructures and how digital sovereignty could benefit privacy and the protection of personal data.

IPEN

The EDPS founded the [Internet Privacy Engineering Network \(IPEN\)](#) in 2014 to bring together experts from a range of different areas and to encourage the development of engineering solutions to privacy problems. Through facilitating exchange between regulators, researchers and developers who build privacy into new and existing digital tools, IPEN aims to promote and advance state-of-the-art practices in privacy engineering. In 2021, the EDPS held two IPEN workshops, one on the use of 'synthetic data' as a possible technology to mitigate data protection risks, and another one on the guidance on and practical use of pseudonymisation techniques to mitigate data protection risks when processing personal data.

TechDispatches

The EDPS continued to publish [TechDispatches](#) to explain emerging developments in technology. Each TechDispatch provides factual descriptions of a new technology, preliminarily assesses the possible impact upon privacy and the protection of personal data, as we understand them now, and provides links to further recommended reading. The topics covered were Facial emotion recognition and Card-based payments.

In 2021, the EDPS TechDispatch initiative received the Global Privacy and Data Protection 2021 Award in the category “Education and Public Awareness”, on the occasion of the 43rd Global Privacy Assembly 2021 hosted by the Mexican DPA. The Global Privacy Assembly is an international forum with more than 130 data protection and privacy authorities worldwide. The GPA Global Privacy and Data Protection Awards celebrate the achievements of the GPA community, and award good practices in the field.

TechSonar

In 2021 the EDPS has also started its TechSonar initiative, with the aim to examine which technologies are worth monitoring to be prepared for a more sustainable digital future where the protection of personal data is effectively guaranteed. While our TechDispatch reports continue to provide in-depth analysis on emerging technologies, our TechSonar reports aim to anticipate technology trends.

TechSonar falls within the Foresight pillar of our Strategy and is a process that empowers the EDPS to continuously analyse the technology arena with the aim of selecting tech trends we foresee for the following year. The first publication of our TechSonar reports focuses on topics such as synthetic data, smart vaccination certificates, just walk out technology and biometric continuous authentication.

In the context of the wider strategy on technology monitoring, the EDPS has decided to use foresight tools for the main purpose of “closely examining both the potential risks and opportunities offered by technological advances, understand the possibilities of new technologies and, at the same time, encourage the integration of data protection by design and data protection by default in the innovation process”. TechSonar⁵ is the first project of the EDPS in this field, aiming to identify emerging technologies in the short time window of one year. The decision to select such a small time frame is guided by the need to have an immediate return in the technological preparedness of the officers involved in activities occurring on a daily basis.

Based on the fundamental pillar that guides its work – namely, independence the EDPS decided to develop an inclusive and agile foresight methodology process that leverages on collective intelligence and increases the collaboration between internal departments.

The first TechSonar Report 2021-2022⁶ was published in December 2021, with its own dedicated section in the EDPS website⁷. The second deployment of the project is starting, and will see results in the course of 2022.

Legislative Consultation

The EDPS provides guidance on proposed legislation to the European Commission, as the institution with the right of legislative initiative, and the European Parliament and the Council, as co-legislators. Our guidance may take the form of:

⁵ Hyperlink: https://edps.europa.eu/press-publications/publications/techsonar_en

⁶ Hyperlink: https://edps.europa.eu/system/files/2021-12/techsonar_2021-2022_report_en.pdf

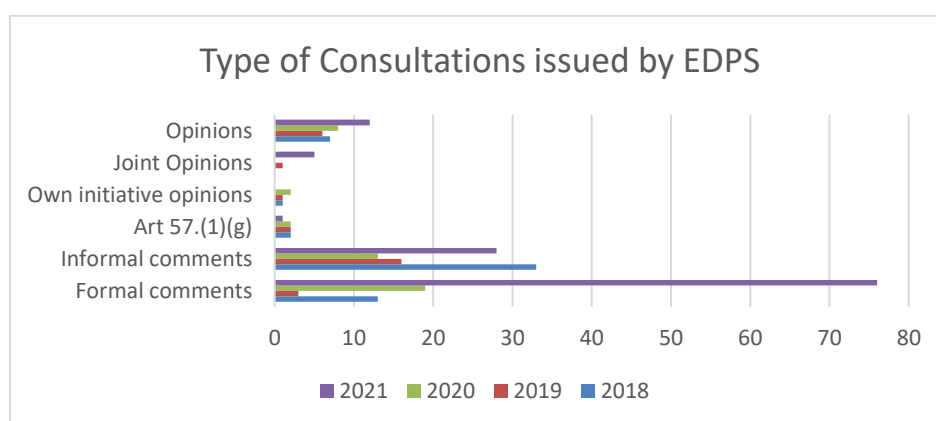
⁷ Hyperlink: https://edps.europa.eu/press-publications/publications/techsonar_en

- **Opinions:** our Opinions are issued in response to mandatory requests by the Commission, which is legally obliged to seek our guidance on any legislative proposal, or draft implementing or delegated acts, as well as recommendations and proposals to the Council in the context of international agreements according to Article 42(1) of Regulation (EU) 2018/1725⁸.
- **Formal Comments:** similar to our Opinions, our Formal Comments are issued in response to a request from the Commission under Article 42(1) and address the data protection implications of legislative proposals. However, they are usually shorter and more technical, or only address certain aspects of a proposal. Our Formal Comments are published on our website.
- **Informal Comments:** the European Commission is encouraged to consult the EDPS informally before adopting a proposal, which has an impact on data protection. This allows us to provide the Commission with input at an early stage of the legislative process, usually at the stage of the inter-service consultation. Informal Comments are, in principle, not published.
- **Joint EDPS-EDPB Opinions:** where a legislative or other relevant proposal is of particular importance for the protection of personal data, the Commission may also consult the EDPB. In such cases, the EDPS and EDPB work together to issue a joint opinion⁹.

Significant increase in the number of legislative consultations

The statistics provided below clearly demonstrate that the number of requests for legislative consultation has significantly increased over time. The increase in the number of requests for legislative consultations is **particularly significant between 2020 and 2021**. In 2021, the number of consultations reached **three times the total volume experienced in 2020**.

The steady increase in legislative consultation activities is shown on the following graph:



⁸ Opinions, as well as their summaries in all official languages of the EU, are available on the EDPS website and published in the [Official Journal](#) of the EU. Opinions highlight our main data protection concerns and recommendations on legislative proposals or other measures. They are issued in response to a request from the Commission and are addressed to the EU co-legislator.

⁹ See also Article 20 of the EDPS Rules of Procedure.

	2018 ¹⁰	2019	2020	2021
Formal comments	13	3	19	76
Informal comments	33	16	13	28
Joint EDPS-EDPB Opinions	0	1	0	5
EDPS Opinions	7	6	8	12
EDPS own-initiative Opinions	1	1	2	0
Art. 57(1)(g)	2	2	2	1
Total	56	29	44	122

In 2021, the EDPS responded to **88 formal legislative consultations** pursuant to Article 42(1), issuing 12 opinions and 76 formal comments. In addition, **5 joint opinions** were adopted with the EDPB pursuant to Article 42(2) EUDPR. As the EDPS authors joint opinions together with the EDPB and its members, such files require additional cooperation and coordination.

The statistics for 2021 also reflect an increased expectation on the Commission's services side that the EDPS should be involved and **provide advice at the informal stage of preparation** of legislative/policy proposals (i.e. even before the informal consultation stage)¹¹. This includes: attending workshops, expert meetings and sometimes inter-service meetings, responding to public consultations or targeted consultations or providing inputs to external studies. In this context, the EDPS issued **28 informal comments** in 2021, in addition to other forms of providing informal assistance.

Timelines vary from a few days in the case of an urgent consultation to eight weeks for an opinion on a legislative proposal or an opinion on a prior consultation (according to Regulation (EU) 2018/1725). These short timelines, and the large number of cases in relation to the small size of the EDPS, necessitate careful planning and monitoring to allow planning and executing other, proactive activities, so far as possible within these constraints.

The steady increase of the legislative consultation activities has led to a significant rise on the translation costs for Policy and Consultation Unit.

Increased number of follow-up requests

Growing awareness of data protection issues also results in requests from European Parliament, its committees (LIBE, IMCO) and/or individual (shadow) rapporteurs for comments or opinions on compromise amendments or possible outcomes of trilogue

¹⁰ Until 12 November 2018, Article 28(2) and 41 of Regulation 45/2001 was still in force. As a result, guidance provided in relation to implementing and delegated acts were provided as informal comments (rather than Opinions), which contributed to the relatively high number of informal comments issued in 2018.

¹¹ See recital 60 EUDPR.

negotiations. A new and increasing phenomenon are invitations from relevant working parties of the Council to present EDPS opinions. The Supervisor and EDPS staff regularly respond to such invitations and requests, which puts an additional pressure on available resources.

While the Unit within the EDPS in charge of legislative consultation has grown slightly since 2018, its increase in staffing is still not commensurate to the overall increase of workload. The substantial increase in consultation requests is also one of the main reasons why there has been a decrease in the number of own-initiative opinions issued by the EDPS.

2.1.4. The EDPS as a member of the EDPB

The [European Data Protection Board](#) (EDPB) is an independent body established under the GDPR that promotes cooperation between national DPAs to ensure the consistent application of data protection rules across the EU. The EDPS is both a member of the EDPB and the provider of an independent Secretariat, which offers administrative and logistic support, performs analytical work and contributes to the EDPB's tasks. A [Memorandum of Understanding](#) determines the terms of cooperation between the EDPS and the EDPB.

Much of the work carried out by the EDPB takes place within expert subgroups, each of which covering a specific range of topics. These include key provisions of the GDPR, international transfers, technology and financial matters, among many others.

The EDPS is formally coordinating the Key Provisions Expert Subgroup. In this context, we consistently play a leading role as a lead rapporteur, co-rapporteur, or a member of the drafting team.

As a member of the EDPB, the EDPS contributed to multiple EDPB initiatives in 2021, including:

- [EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors;](#)
- [EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries;](#)
- [Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive;](#)
- [EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research;](#)
- [Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime \(Budapest Convention\);](#)
- [EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance \(Data Governance Act\);](#)
- [Statement 03/2021 on the ePrivacy Regulation;](#)
- [EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance,](#)

- [verification and acceptance of interoperable certificates on vaccination, testing and recovery;](#)
- [Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation \(EU\) 2016/679 on the adequate protection of personal data in the United Kingdom;](#)
 - [Guidelines 03/2021 on the application of Article 65\(1\)\(a\) GDPR;](#)
 - [Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive \(EU\) 2016/680 on the adequate protection of personal data in the United Kingdom;](#)
 - [Statement 05/2021 on the Data Governance Act in light of the legislative developments;](#)
 - [EDPB Response to Mr. de Serpa Soares, Under-Secretary-General for Legal Affairs and UN Legal Counsel \(May 2021\);](#)
 - [EDPB response to Mr Miguel de Serpa Soares regarding the ongoing dialogue between the EDPB and the United Nations on data protection \(November 2021\);](#)
 - [Final version of the Recommendations 1/2020 on supplementary measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data \(after public consultation\);](#)
 - [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 \(Artificial Intelligence Act\);](#)
 - [Opinion 20/2021 on Tobacco Traceability System;](#)
 - [EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro - to the European Central Bank;](#)
 - [Guidelines 02/2021 on virtual voice assistants \(after public consultation\);](#)
 - [Guidelines 07/2020 on the concepts of controller and processor in the GDPR \(after public consultation\);](#)
 - [Guidelines 10/2020 on restrictions under Article 23 GDPR;](#)
 - [EDPS proposal on 2022 coordinated action of the EDPB in the context of the Coordinated Enforcement Framework;](#)
 - [Statement on the Digital Services Package and Data Strategy;](#)
 - [Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR;](#)
 - [Guidelines 01/2021 on Examples regarding Personal Data Breach Notification;](#)
 - [Opinion 39/2021 on whether Article 58\(2\)\(g\) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject;](#)
 - [Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive \(LED\) under Article 62;](#)
 - [Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation \(EU\) 2016/679 on the adequate protection of personal data in the Republic of Korea;](#)
 - [Urgent Binding Decision 01/2021 on the request under Article 66\(2\) GDPR from the Hamburg \(German\) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited;](#)

- [Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65\(1\)\(a\) GDPR.](#)

2.1.5. International cooperation in data protection

As data flows across borders, there is a need to consider data protection in a global context.

In 2021, the EDPS actively participated in a number of international fora with the aim of sharing information and good practices, finding common ground and developing guidance, and working together to improve the understanding of data protection law.

Examples of international conferences that the EDPS has participated in throughout 2021 are presented below.

Global Privacy Assembly

The EDPS is an active member of the [Global Privacy Assembly](#) (GPA) (previously known as the International Conference of Data Protection and Privacy Commissioners, ICDPPC) and former host of the 2018 Conference that gathered more than 1000 delegates discussing digital ethics and the challenges of a data driven society.

The 43rd Global Privacy Assembly (GPA) took place between the 18th and 21st of October. The virtual conference was hosted by National Institute for Transparency, Access to Information and Protection of Personal Data (INAI), Mexico, and brought together more than 90 members and observers to consider key data protection challenges. The conference started with an Open Session (18 and 19 October) and ended with the Closed Session (20 and 21 October).

During the Closed Session, a series of [Resolutions](#) were discussed and agreed at the conference on a very important topics such as:

- Data sharing for the public good;
- Children's digital rights;
- Government access to data; and
- The future of the Global Privacy Assembly.

The GPA also adopted a [strategic plan](#) for the next two years, committing to a continued focus on advancing global privacy, maximising the GPA's influence and building capacity for members.

Council of Europe and OECD

The EDPS also follows the activities of the Consultative Committee of the Convention 108 (T-PD) and represents the Global Privacy Assembly before the T-PD.

The EDPS participates in T-PD as an observer. Our role involves ensuring 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 impact for the EDPS (children's data protection; facial recognition, artificial intelligence, digital solutions to fight Covid-19, digital contact tracing, oversight by intelligence services, digital identity, processing of personal data in the context of political activities and elections, contractual clauses in the context of transborder data flows. etc). With the modernisation of the Convention 108, a very important and strategic follow-up mechanism to the Convention will be created which will also create additional tasks for the T-PD.

The EDPS is also following the activities of the OECD in particular the activities of the Working Party on Data Governance and Privacy (DGP) and Privacy Guidelines Expert Group (PGEG). Some of the activities are of strategic importance for the EDPS, for instance on the question of Government access to personal data held by the private sector.

Cooperation with International organisations

Generating and fostering global partnerships in the field of data protection is a priority for the EDPS. One of the ways in which we do this is by co-organising a yearly workshop dedicated to data protection within international organisations. The workshop is a forum for the exchange of experiences and views on the most pressing issues in data protection faced by international organisations all over the world. The size and the relevance of this event has been growing since the first edition in 2005. This confirms the need for a platform for international organisations to engage, share best practices and discuss unsolved dilemmas, and demonstrates the increasing awareness of the importance of ensuring strong safeguards for personal data.

The 2020 remote workshop of data protection within International Organisations demonstrated a strong demand on the size of international organisations to have an in-depth discussion with EU's representative on international transfers to international organisations and on practical and pragmatic tools to be developed to facilitate such transfers. As a follow-up and in 2021, the EDPS led the activities of a taskforce on international transfers to international organisations with a view to develop concrete solutions to frame transfers to international organisations. This work is still ongoing and the next in-person edition of the workshop with international organisations will take place in May 2022 (no workshop was held in 2021 due to the pandemic situation).

2.2 The EDPB in 2021

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules, such as the General Data Protection Regulation 2016/679 (GDPR), throughout the European Economic Area. The EDPB is composed of representatives of the national EU and EEA EFTA data protection supervisory authorities, and the European Data Protection Supervisor (EDPS).

The Secretariat of the EDPB works under the exclusive instructions of the EDPB Chair and is managed by the head of the EDPB Secretariat. The EDPB Secretariat provides analytical, administrative and logistical support to the EDPB. In practice, the EDPB Secretariat deals with a range of tasks, from drafting EDPB documents, providing IT solutions to ensuring

transparent communications, handling media relations, ensuring respect of the legal framework and planning as well as organising meetings. The EDPB Secretariat is composed of a multifaceted team facilitating the Board's fair and effective decision-making and acts as the gateway for clear and consistent communications.

2.2.1. EDPB Strategy 2021-2023 and Work Programme 2021-2022

In early 2021, the EDPB adopted its two-year [work programme](#) for 2021-2022, according to Art. 29 of the EDPB Rules of Procedure. The work programme follows the priorities set out in the [Strategy for 2021-2023](#) and will put the EDPB's strategic objectives into practice.

This Strategy includes four main pillars with strategic objectives, as well as a set of three key actions per pillar to help achieve these goals.

The pillars and key actions are as follows:

Pillar 1: Advancing harmonisation and facilitating compliance

The EDPB will continue to strive for a maximum degree of consistency in the application of data protection rules and limit fragmentation among Member States. In addition, the EDPB will develop and promote tools that help to implement data protection into practice, taking into account practical experiences of different stakeholders on the ground.

- Further guidance on key notions of EU data protection law to promote consistent application of data protection rules, taking into account stakeholders' practical experience gathered through events and public consultations (e.g., guidelines on data subject rights, on legitimate interest, on children's data...).
- Pursue consistency activities directly addressed to national supervisory authorities to ensure consistency of their decisions in a number of areas (evaluation of Codes of conduct, Certification schemes and criteria, Binding Corporate Rules, creation of Standard contracts, list of risky processing to be subject to an impact assessment,...) in accordance with Article 64(1) and (2) GDPR. The EDPB will also continue acting as a dispute resolution body for any dispute between EEA supervisory authorities (Article 65(1) GDPR binding decisions; urgency procedure Article 66 GDPR decisions/opinions).
- Promote compliance mechanisms for controllers and processors (e.g., guidelines on assessment of certification criteria).
- Advising the EU legislator on any important issue related to the protection of personal data in the EU (e.g., Data Governance Act; ePrivacy; Anti-Money Laundering legislation...), and intensified engagement and cooperation with other regulators and policymakers.
- Develop raising awareness common tools on GDPR for a wider audience (e.g., tools specifically tailored for non-expert professionals, such as SMEs and data subjects).

Pillar 2: Supporting effective enforcement and efficient cooperation between SAs

The EDPB will facilitate a more efficient functioning of the cooperation and consistency mechanisms between all national supervisory authorities that work together to enforce

European data protection law. It will also strive for the development of a genuine EU-wide enforcement culture among supervisory authorities.

- Encouraging and facilitating the use of the full range of cooperation tools enshrined in GDPR and the Law enforcement directive (LED), and continuously evaluating and improving the efficiency and effectiveness of these tools, as well as further promoting a common application of key concepts in the cooperation procedure (e.g., guidelines on Article 60 GDPR (One-Stop-Shop), on Article 65 GDPR (binding decisions), on the calculation of administrative fines, ...).
- Implementation of the Coordinated Enforcement Framework (CEF)¹² to carry out annual coordinated actions on a pre-defined topics to allow SAs to pursue joint actions in a flexible but coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations.
- Implementation of the Support Pool of Experts (SPE). The EDPB will launch the pilot project of SPE to provide material support to EDPB Members in the form of expertise that is useful for investigations and enforcement activities and to enhance cooperation and solidarity between EDPB Members by sharing, reinforcing and complementing strengths and addressing operational needs.

Pillar 3: A fundamental rights approach to new technologies

The EDPB will monitor new and emerging technologies and their potential impact on the fundamental rights and daily lives of individuals, and will help to shape Europe's digital future in line with our common values and rules, continuing to work with other regulators and policymakers to promote regulatory coherence and enhanced protection for individuals.

- Reinforcing the application of fundamental data protection principles and individual rights, and establishing common positions in the context of new technologies (e.g., guidelines on Blockchain, on anonymisation and pseudonymisation, on the use of facial recognition by law enforcement authorities...).
- Strengthening cooperation with external stakeholders (e.g., ENISA advisory group, ISO liaison, Contact point of the Stakeholder Cybersecurity Certification Group...).

Pillar 4: The global dimension

The EDPB is determined to set and promote high EU and global standards for international data transfers to third countries and will reinforce its engagement with the international community to promote EU data protection as a global model and to ensure effective protection of personal data beyond the EU borders.

- Providing guidance on the use of transfer tools ensuring an essentially equivalent level of protection, and increasing awareness on their practical implementation and on issues relating to government access to personal data (e.g., opinions on draft adequacy decisions (e.g., UK, Republic of Korea, ...); PNR agreements (e.g., UK, Canada, ...); guidelines on codes of conduct or certification as tools for transfers, guidelines on Article 48 GDPR (transfers or disclosures not authorised by Union law); ...).
- Engaging with the international community to promote EU data protection as a global model and to ensure effective protection of personal data beyond EU borders and

facilitating the engagement between EDPB members and third countries' SAs with a focus on cooperation in enforcement cases involving controllers/processors located outside the EEA.

- Finally, the EDPB will continue to take any actions to foster the cooperation between EU and EEA EFTA data protection supervisory authorities. In particular, the coordination of the supervision of European large-scale IT systems will fall within the framework of the activities of the EDPB (EPPO during 2021, EES and ETIAS during 2022), in addition to the already existing ones (IMI and Eurojust).

The EDPB Strategy and Work Programme helped guide the EDPB's work in 2021 and will help for the years to come. The tools included in the Work Programme will help create a more consistent understanding of the key concepts and processes in the GDPR and the cooperation and consistency mechanism in particular. This will allow the EDPB to reinforce its leadership in ensuring consistency across the EEA and further drive EEA SAs to work in one direction and to speak in one voice.

2.2.2. Meetings

In 2021, The EDPB held 389 meetings, including 15 plenary meetings, 200 expert subgroup meetings and 174 drafting team meetings, during which EDPB members formally adopted documents or discussed developments or policy questions in relation to issues of significant strategic importance.

The EDPB Secretariat takes part in all of those meetings, provides analytical support and makes all the administrative arrangements.

2.2.3. Guidelines, Opinions, Decisions and other documents

During the plenary meetings, the EDPB adopted Guidelines, Opinions, Decisions and other documents such as statements or informative notes to advise the European Commission, national Supervisory Authorities, and other stakeholders on GDPR matters.

The EDPB Secretariat led the drafting of over 40% of the Guidelines, Opinions, Recommendations and Statements adopted by the EDPB in 2021.

2.2.3.1. Guidelines

In 2021, the EDPB adopted six new Guidelines and two sets of Recommendations aimed at clarifying the range of provisions under the GDPR.

- ✓ [Guidelines 01/2021 on Examples regarding Data Breach Notification](#)
- ✓ [Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive](#)
- ✓ [Guidance on certification criteria assessment \(Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation\)](#)
- ✓ [Guidelines 03/2021 on the application of Article 65\(1\)\(a\) GDPR](#)
- ✓ [Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions](#)

- ✓ [Guidelines 04/2021 on codes of conduct as tools for transfers](#)
- ✓ [Guidelines 02/2021 on Virtual Voice Assistants](#)
- ✓ [Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR](#)

Five Guidelines and one set of Recommendations were approved by the EDPB in their final form in 2021, following public consultations:

- ✓ [Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679](#)
- ✓ [Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications](#)
- ✓ [Guidelines 8/2020 on the targeting of social media users](#)
- ✓ [Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data](#)
- ✓ [Guidelines 07/2020 on the concepts of controller and processor](#)
- ✓ [Guidelines 10/2020 on restrictions under Article 23 GDPR](#)

2.2.3.2. Consistency opinions

Opinions on draft decisions regarding Binding Corporate Rules

SAs may approve Binding Corporate Rules within the meaning of Art. 47 GDPR. BCRs are data protection policies implemented and adhered to within a group of enterprises established in the EEA for transfers of personal data outside the EEA within the same group. In 2021, several SAs submitted their draft decisions regarding the Controller or Processor BCRs of various companies to the EDPB, requesting an Opinion under Art. 64(1)(f) GDPR. The EDPB issued eighteen Opinions on BCRs.

In all instances, the EDPB concluded that the draft BCRs contained all required elements and guaranteed appropriate safeguards to ensure that the level of protection guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. This is without prejudice of the obligation of the data exporter to assess whether, in the specific case, additional measures are necessary in order to ensure an essentially equivalent level of protection as provided in the EU. In any case, on the basis of the EDPB Opinions, the BCRs could be approved without changes by the relevant SAs.

The various Opinions adopted in 2021 are listed below:

- ✓ [Opinion 34/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Otis](#)
- ✓ [Opinion 33/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Carrier](#)
- ✓ [Opinion 31/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of the COLT Group Adopted: 2 August 2021](#)
- ✓ [Opinion 30/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of the COLT Group Adopted: 2 August 2021](#)

- ✓ [Opinion 29/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of Oregon Tool, Inc \(Formerly “Blount”\)](#) Adopted: 2 August 2021
- ✓ [Opinion 28/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Oregon Tool, Inc \(formerly “Blount”\)](#) Adopted: 2 August 2021
- ✓ [Opinion 27/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia \(Germany\) regarding the Processor Binding Corporate Rules of the Internet Initiative Japan Group](#) Adopted: 2 August 2021
- ✓ [Opinion 26/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia \(Germany\) regarding the Controller Binding Corporate Rules of the Internet Initiative Japan Group](#) Adopted: 2 August 2021
- ✓ [Opinion 22/2021 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the CGI Group](#) Adopted: 1 July 2021
- ✓ [Opinion 21/2021 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the CGI Group](#) Adopted: 1 July 2021
- ✓ [Opinion 09/2021 on the draft decision of the Baden- Wurttemberg Supervisory Authority regarding the Controller Binding Corporate Rules of Luxoft Group](#) Adopted: 16 February 2021
- ✓ [Opinion 08/2021 on the draft decision of the Baden- Wurttemberg Supervisory Authority regarding the Processor Binding Corporate Rules of Luxoft Group](#) Adopted: 16 February 2021
- ✓ [Opinion 07/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Kumon Group](#) Adopted: 16 February 2021
- ✓ [Opinion 06/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of Kumon Group](#) Adopted: 16 February 2021
- ✓ [Opinion 04/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of BDO](#) Adopted: 22 January 2021
- ✓ [Opinion 03/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of BDO](#) Adopted: 22 January 2021
- ✓ [Opinion 02/2021 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Elanders Group](#) Adopted: 22 January 2021
- ✓ [Opinion 01/2021 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Saxo Bank Group](#) Adopted: 22 January 2021

Opinions on draft requirements for accreditation of a certification body

Seven SAs submitted their draft decisions on accreditation requirements for certification bodies under Art. 43(1)(b) GDPR to the EDPB, requesting an Opinion under Art. 64(1)(c) GDPR. These requirements allow the accreditation of certification bodies responsible for issuing and renewing certification in accordance with Art. 42 GDPR.

These Opinions aim to establish a consistent and harmonised approach regarding the requirements that SAs and national accreditation bodies apply when accrediting certification bodies under the GDPR. To do so, the EDPB made several recommendations and encouragements to the relevant SAs on the amendments to be made to the draft accreditation requirements.

The SAs then amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the Opinions of the EDPB.

The various Opinions adopted in 2021 are listed below:

- ✓ [Opinion 12/2021 on the draft decision of the competent supervisory authority of Portugal regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted: 20 July 2021](#)
- ✓ [Opinion 13/2021 on the draft decision of the competent supervisory authority of Romania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted: 23 March 2021](#)
- ✓ [Opinion 19/2021 on the draft decision of the competent supervisory authority of Hungary regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted: 1 June 2021](#)
- ✓ [Opinion 25/2021 on the draft decision of the competent supervisory authority of Lithuania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted: 20 July 2021](#)
- ✓ [Opinion 35/2021 on the draft decision of the competent supervisory authority of Belgium regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted 30 November 2021](#)
- ✓ [Opinion 36/2021 on the draft decision of the competent supervisory authority of Norway regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted 30 November 2021](#)
- ✓ [Opinion 38/2021 on the draft decision of the competent supervisory authority of Latvia regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted 20 November 2021](#)

Opinions on SAs' approval of accreditation requirements for code of conduct monitoring body

The EDPB issued five Opinions on draft accreditation requirements for code of conduct monitoring bodies, as requested by the submitting SAs in accordance with Art. 64(1)(c) GDPR.

The aim of such EDPB Opinions is to ensure consistency and the correct application of the requirements among EEA SAs. To do so, the EDPB made several recommendations and encouragements to the various SAs on the amendments to be made to the draft accreditation requirements. On this basis, the SAs amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the Opinions of the EDPB.

The Opinions adopted in 2021 are listed below:

- ✓ [Opinion 37/2021 on the draft decision of the competent supervisory authority of Malta regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR Opinion 24/2021 on the draft decision of the competent supervisory authority of Slovakia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 20 July 2021](#)

- ✓ [Opinion 23/2021 on the draft decision of the competent supervisory authority of Czech Republic regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 20 July 2021](#)
- ✓ [Opinion 24/2021 on the draft decision of the competent supervisory authority of Slovakia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR](#)
- ✓ [Opinion 11/2021 on the draft decision of the competent supervisory authority of Norway regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 March 2021](#)
- ✓ [Opinion 10/2021 on the draft decision of the competent supervisory authority of Hungary regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 March 2021](#)

Opinion on SAs' draft Standard Contractual Clauses

The contract or other legal act to govern the relationship between the controller and the processor in accordance with Art. 28(3) GDPR may be based, in whole or in part, on Standard Contractual Clauses (SCCs).

An SA may adopt SCCs in accordance with the consistency mechanism. As such, the EDPB reviews draft SCCs submitted by SAs to contribute to the consistent application of the GDPR throughout the EEA. In March 2021, the Lithuanian SA (LT SA) submitted its draft SCCs to the EDPB, requesting an Opinion under Art. 64(1)(d) GDPR. The EDPB held that the draft SCCs needed some further adjustments and proposed several recommendations and encouragements on how to amend them.

Opinions on SA approval of codes of conduct

Two SAs submitted their draft decisions on the approval of two codes of conduct that related to processing activities in several Member States. The codes of conduct were reviewed in accordance with the procedures set up by the EDPB in Guidelines 04/2021 on codes of conduct and in the EDPB Document on the procedure for the development of informal "Codes of Conduct sessions". Those codes of conduct do not aim to be used as a tool for international transfer of data (Art. 46 (2) (e) GDPR).

The EDPB considered that the draft codes complied with the GDPR as they fulfilled the requirements imposed by Art. 40 and Art. 41 GDPR. The EDPB also recalled that, in accordance with Art. 40(5) GDPR, the competent SA would have to submit the code of conduct to the EDPB in case of amendment or extension.

- ✓ [Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure FService Providers \(CISPE\) Adopted: 19 May 2021](#)
- ✓ [Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe Adopted: 19 May 2021](#)

Opinion on SAs' authorisation of administrative arrangements

The EDPB adopted an opinion relating to draft Administrative Arrangement for the transfers of personal data between the Haut Conseil du Commissariat aux Comptes and the Public Company Accounting Oversight Board to the French SA, which thereafter requested an [opinion from the EDPB pursuant to Art. 64\(2\) GDPR](#).

Opinion related to Article 58(2)(g)

In December 2021, the EDPB adopted [Opinion 39/2021 on whether Article 58\(2\)\(g\) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject](#).

2.2.3.3. Binding Decisions

In relation to the draft decision regarding WhatsApp Ireland (WhatsApp IE) of the Irish SA and the subsequent CSA objections, the EDPB adopted a binding decision under Art. 65(1)(a) GDPR: [Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Art. 65\(1\)\(a\) GDPR](#). The decision concludes that the Irish SA should amend its draft decision regarding infringements of transparency, the period to bring processing operations into compliance and the calculation of the fine.

Following a request from the Hamburg SA, which had taken provisional measures, in accordance with Art. 66(1) GDPR, against Facebook Ireland Ltd (Facebook IE) banning their processing of WhatsApp IE user data in Germany for their own purposes, the EDPB adopted an urgent binding decision under Art. 66(2) GDPR: [Urgent Binding Decision 01/2021 on the request under Art. 66\(2\) GDPR from the Hamburg \(German\) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited](#)

2.2.3.4. Other documents, including legal advice

The following documents were adopted in 2021:

- ✓ [Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation \(EU\) 2016/679 on the adequate protection of personal data in the United Kingdom](#)
- ✓ Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom
- ✓ Opinion 20/2021 on Tobacco Traceability System
- ✓ Opinion 32/2021 regarding the European Commission draft implementing decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea
- ✓ [EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors](#)
- ✓ [EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries](#)

- ✓ [EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance \(Data Governance Act\)](#)
- ✓ [EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID 19 pandemic \(Digital Green Certificate\)](#)
- ✓ [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 \(Artificial Intelligence Act\)](#)
- ✓ Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)
- ✓ Statement 03/2021 on ePrivacy Regulation
- ✓ [Statement 04/2021 on international agreements including transfers](#)
- ✓ Statement 05/2021 on the Data Governance Act in light of the legislative developments
- ✓ Statement on digital services package
- ✓ EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime
- ✓ [Statement 05/2021 on the Data Governance Act in light of the legislative developments](#)
- ✓ [EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research 02/02/2021](#)
- ✓ [Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive \(LED\) under Article 62 – 14/12/2021](#)

Other Guidance and Information Notes:

- [Pre-GDPR BCRs overview list](#)
- [Statement on the end of the Brexit transition period - update 13/01/2021](#)
- [Information note on data transfers under the GDPR to the United Kingdom after the transition period - update 13/01/2021](#)
- IMI Report (CSC)
- a list of competent supervisory authorities on IMI. (CSC)
- List of Status of Members - EU Agencies and Bodies (CSC)

2.2.4. Stakeholder engagement

The EDPB organises stakeholder events to gather input and views on specific issues in the interest of developing future guidance. In 2021, the EDPB organised one such event on processing personal data for scientific research purposes on 30 April. The event took place online and secured approximately 60 participants that represented a combination of academia, NGOs, commercial organisations and SAs. They shared their experience concerning the use of personal data for scientific research purposes and emphasised areas that needed further clarifying or explaining. Alongside this provided input, the EDPB gathered further valuable insights on the topic from a questionnaire sent prior to the event to both parties who attended and could not attend the event. The EDPB will use all the provided stakeholder input in the context of drafting future guidance on data processing for scientific research purposes.

Following the preliminary adoption of Guidelines, the EDPB Secretariat organises public consultations to give stakeholders and citizens the opportunity for additional input. This input is then taken into account by the EDPB members in charge of drafting.

In 2021, the EDPB Secretariat launched the following consultations:

- In January, the EDPB opened a public consultations on Guidelines 01/2021 on Examples regarding Data Breach Notification.
- In March, the EDPB opened a public consultation on Guidelines 02/2021 on Virtual Voice Assistants.
- In April, the EDPB opened two public consultations on Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) and, Guidelines 03/2021 on the application of Article 65(1)(a) GDPR.
- In July, the EDPB opened a public consultation on Guidelines 04/2021 on codes of conduct as tools for transfers.
- In November, the EDPB opened a public consultation on Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

For the fourth year in a row, the EDPB Secretariat conducted a survey as part of the annual review of the Board's activities under Article 71.2 GDPR. Questions focused on the content and adoption process of the EDPB's Guidelines, with a view to understanding to what extent stakeholders find them helpful and practical to interpret GDPR's provisions.

2.2.5. The EDPB Secretariat contribution to the national SAs' cooperation

As part of its 2021-2023 Strategy, the EDPB established a [Support Pool of Experts](#) (SPE) in 2020. The terms of reference of the SPE specify that its objectives are to provide material support to the EDPB Members in the form of expertise that is useful for investigations and enforcement activities, and to enhance cooperation and solidarity between the EDPB Members by sharing, reinforcing and complementing strengths and addressing operational needs. In October 2021, a new Head of Activity for Enforcement Support and Coordination was appointed to coordinate the work of the SPE, and in December 2021, EDPB members agreed on SPE priorities for 2022.

Further in line with the 2021-2023 Strategy, the EDPB set up a [Coordinated Enforcement Framework](#) (CEF). The CEF provides a structure for recurring annual coordinated action by the SAs. The CEF aims to facilitate joint actions in a flexible and coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations. The purpose behind the recurring annual coordinated actions is to promote compliance, empower data subjects to exercise their rights and raise awareness. EDPB members agreed to launch the first coordinated action, in 2022, on the use of Cloud based services by the public sector. The EDPB Secretariat is contributing to this work.

The EDPB Secretariat is also in charge of the management of a [register on the EDPB website gathering the final decision taken concerning cross-border cases in the context of](#)

[the OSS mechanism](#). The register offers an exceptional opportunity to read final decisions taken by, and involving, different SAs in a cross-border context. These decisions often contain useful guidance on how to comply with the GDPR in practice. The register contains both final decisions and its summaries prepared by the EDPB Secretariat and duly approved by LSAs.

In the context of cooperation between SAs in the assessment of BCR applications, the EDPB Secretariat organised four BCR sessions in 2021. The sessions streamlined discussions between the SAs and the EDPB Secretariat regarding specific aspects of individual BCRs with the aim to facilitate the assessment of the BCRs and work out a consensus on the standards and expectations for BCRs, before the formal procedure is triggered under Art. 64 GDPR. The BCR sessions thus represent a prior informal cooperation phase that aims to address remaining issues that have arisen regarding a specific BCR based on shared comments by the SAs and the EDPB Secretariat.

Additionally, several informal sessions were organised regarding certification criteria. These sessions fostered discussion between the SAs and the EDPB Secretariat on specific certification criteria that may be submitted to the EDPB under Art. 64(1)(c) GDPR.

2.2.6. IT communications tool (Internal Market Information) & the new EDPB website

On the technical support to SAs' cooperation, throughout 2021, the EDPB Secretariat continued to provide support to the SAs with IT solutions that facilitate their communication. In this respect, the EDPB Secretariat leads the IT Users Expert Subgroup that focuses on assessing the need for development and making changes to the IMI system. Furthermore, it continued to work on best practices to further refine the procedures in use and to share its expertise on the use of the IMI System for the cooperation and consistency mechanism. The EDPB Secretariat is also providing an IMI helpdesk to daily support the staff of the SAs making use of the IMI system.

The EDPB Secretariat also migrated the EDPB Wiki platform used for internal sharing of information to a new instance dedicated to the EDPB and with an enhanced user experience.

In 2021, the EDPB Secretariat enhanced the EDPB website, 'edpb.europa.eu', which underwent a new web design.

In the context of functionality, the website now supports dynamic listing of documents and filters, which improves user experience by eliminating numerous general search queries. The communication functionality was improved by providing a new contact form on the website. The content management system of the website, which manages the creation and modification of digital content, was upgraded to Drupal 8. The EDPB Secretariat is also putting great efforts in implementing a new advanced search functionality that will make the website more user-friendly.

2.2.7. The EDPB Secretariat activities relating to access to Documents

Transparency is a core principle of the EDPB. As an EU body, the EDPB is subject to Art. 15 of the [Treaty of the Functioning of the European Union](#), [Regulation 1049/2001 on public access to documents](#). Art. 76(2) GDPR and Art. 32 of the EDPB's Rules of Procedure reinforce this requirement. The principle of transparency provides any EU citizen, and any natural or legal person residing or having its registered office in a Member State, the right of access to EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities. In exceptional cases, the EDPB may refuse to disclose all or part of a document. The reasons for refusal and other procedural rules are outlined in [Regulation 1049/2001 on public access to documents](#).

In 2021, the EDPB received 39 public access requests for documents held by the EDPB. Confirmatory applications were received in two cases. The EDPB Secretariat is in charge of preparing the answers to those requests, subject to the validation of the EDPB Chair (for confirmatory applications) and Deputy chairs (for initial applications), in accordance with Article 32.2 of the EDPB [Rules of Procedures](#).

A complaint was made to the European Ombudsman regarding an EDPB confirmatory decision for a request for access to documents, which was submitted in 2020. The request concerned access to some of the preparatory documents for the EDPB guidelines 2/2019 on the processing of personal data in the context of the provision of online services to data subjects. Following a re-assessment of the documents, the EDPB decided to grant partial access to these documents as the fact that differing views expressed in the documents were already publicly known. The complainant was satisfied with the EDPB's reply and the Ombudsman decided to close the case.

2.2.8. The EDPB Secretariat activities relating to Data Protection Officer activities

The EDPB processes personal data following [Regulation 2018/1725 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](#) (Regulation 2018/1725). In accordance with Art. 43 of Regulation 2018/1725, the EDPB has designated its own DPO team, which is part of the EDPB Secretariat, to handle the processing of personal data. The DPO's position and tasks are defined in Arts. 44 and 45 of Regulation 2018/1725, and are further detailed in the [EDPB DPO Implementing Rules](#).

In 2021, the EDPB, with the assistance of its DPO team, continued to strengthen the compliance with Regulation 2018/1725 by enhancing its transparency practices through different means, such as:

- The development, publication and update of several privacy notices;
- The continued development of several records, as well as a centralised register for records, which will be made available on the EDPB website;
- The update of its DPO website page with additional information; and
- The improvement of its contact form on the EDPB website.

Furthermore, the DPO team launched several internal legal assessments on various issues concerning the EDPB's processing of personal data and identified suitable legal,

organisational and, where applicable, technical solutions. The assessments were also conducted as part of the DPO's advisory role for the EDPB.

In 2021, the DPO team assisted with the handling of 6 data subject requests under Art. 17 to Art. 24 Regulation 2018/1725, which indicates a decrease in relation to 2020.

Regarding data breaches, the DPO team assisted with the handling of 12 data breaches under Arts. 34 and 35 Regulation 2018/1725, which represents an increase in relation to 2020. The assessment of the majority of these data breaches indicated that they were unlikely to result in a risk to the rights and freedoms of natural persons. At the time of the drafting of this report, only one data breach had required a notification to the EDPS.

The DPO team also assisted with several replies to individual requests for information involving the processing of their personal data, including cases where individuals mistakenly assumed that the EDPB processed their personal data.

In addition, the DPO team delivered several internal training sessions and created awareness-raising material, aimed at EDPB Secretariat staff. These activities were tailored to the needs and expertise of the participants to ensure that all staff members, in particular newcomers, were adequately informed of their duties regarding personal data processing, but also of their rights as data subjects.

Finally, the EDPB DPO team continued to liaise closely with other EU institutions, bodies and agencies and their DPOs, particularly in matters involving or related to the processing of personal data, but also to ensure the exchange of good practices, common experiences and tailored approaches to specific data protection challenges. To this end, the DPO team participated in the EU institutions' network of DPOs and the EDPB network of DPOs, comprising the DPOs of national SAs, the EDPS and the EDPB.

2.2.9. Coordinated Supervision Committee

In accordance with Art. 62 of [Regulation 2018/1725](#), the European Data Protection Supervisor (EDPS) and the national Supervisory Authorities (SAs) shall cooperate actively to ensure effective supervision of large-scale IT systems and of EU bodies, offices and agencies. For this purpose, the EDPS and SAs shall meet at least twice per year within the framework of the EDPB. Additionally, several legal acts on large-scale IT systems and EU agencies refer to this model of coordinated supervision.

To ensure the consistency of supervision efforts on both levels, all SAs involved, including the EDPS, used to cooperate through Supervision Coordination Groups (SCGs). Each of these groups was dedicated to a specific EU database. Since December 2018, Regulation 2018/1725 has provided for a single model of coordinated supervision for large-scale EU IT systems and agencies within the framework of the EDPB. This replaces the current system of individual SCGs. The new model does not apply to all EU information systems and agencies at once, but progressively, according to when the revised version of the establishing act of each EU information system and agency becomes applicable.

In December 2019, the Coordinated Supervision Committee (CSC) was formally established within the EDPB. It brings together the SAs of each EU Member State and the EDPS, as well as SAs of non-EU Members of the Schengen Area when foreseen under EU law. The CSC's tasks include, among others, supporting SAs in carrying out audits and inspections; working on the interpretation or application of the relevant EU legal act; studying problems within the exercise of independent supervision or within the exercise of data subject rights; drawing up harmonised proposals for solutions; and promoting awareness of data protection rights.

Participation in the CSC meetings can occur under various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act. As [announced](#) in December 2020, during its third plenary meeting, the CSC elected Clara Guerra from the Portuguese SA to succeed Giuseppe Busia as its new Coordinator for a term of two years. Sebastian Hüttmeler from the German Federal SA currently holds the position of Deputy Coordinator.

Pursuant to Art. 62 of Regulation 2018/1725, the following EU large-scale IT systems, bodies, offices and agencies currently fall under the CSC's scope:

Internal Market:

- Internal Market Information System (IMI), which allows the exchange of information between public authorities involved in the practical implementation of EU law.

Police and Judicial Cooperation:

- Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States.
- European Public Prosecutor Office (EPPO), the prosecution agency responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget.

In the future, all coordinated supervision of large EU information systems, bodies, offices and agencies will gradually be moved to the CSC, including:

- Schengen Information System (SIS), ensuring border control cooperation (normally no later than June 2022);
- Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Schengen States (expected before the end of 2022);
- European Travel Information and Authorisation System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen Zone (expected in May 2023);
- Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States (expected by the end of 2023);
- Eurodac, which compares fingerprints of asylum applicants to see if they have previously applied for asylum or entered the EU irregularly via another Member State (expected in 2022);

- Customs Information System (CIS), which is an automated information system that assists EU State administrative authorities in preventing, investigating and prosecuting operations that are in breach of customs or agricultural legislation.

Police and Judicial Cooperation:

- European Criminal Records Information System on third country nationals (ECRIS-TCN), which allows EU Member State authorities to identify which other Member States hold criminal records on third country nationals or stateless persons being checked (expected for 2022);
- Europol, the EU's law enforcement agency (expected in 2022).

Schengen Information System (SIS) (see above, as this system also fall under Police and Judicial cooperation)

3. Resource management

3.1. The EDPS Ethics Framework Activities

The EDPS policy with regard to professional ethics aims to safeguard the general framework of rights and obligations enshrined in the Staff Regulations and to promote excellence in the European civil service. To guide questions related to professional ethics and staff conduct, the EDPS adopted its own Ethics Framework. The main objectives are:

- to ensure that all staff meet the highest standards of professional behavior and integrity;
- to prevent staff from finding themselves in situations that could lead to a conflict of interests, or affect their impartiality and objectives in their conduct or decision making;
- to prevent any situation that could potentially damage the credibility and reputation of the institution;
- to raise awareness of the obligations imposed by the Staff Regulations in the area of professional ethics;

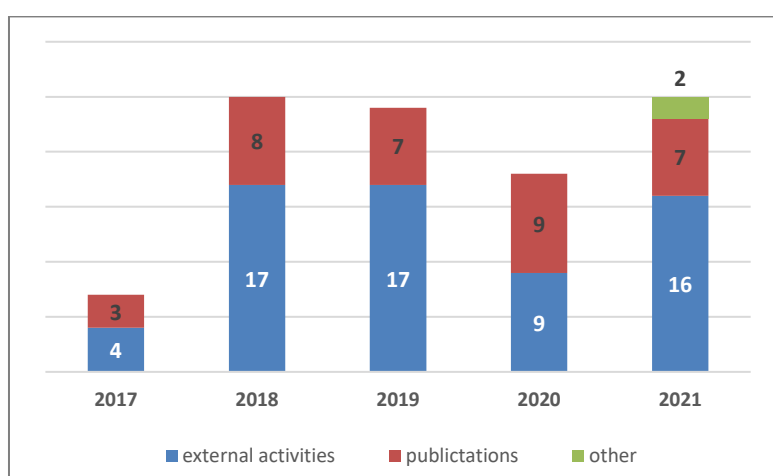
The EDPS Ethics Framework is composed of a specific Code of conduct for the Supervisor as well as a separate Code of conduct applicable to all staff of the EDPS and the EDPB. These Codes of conduct are complemented by a set of Decisions on whistleblowing, anti-harassment, disciplinary proceedings and administrative investigations. The appointment of an Ethics officer to the EDPS ensures the compliance with the provisions included in the Framework.

The EDPS Ethics Framework was last updated end of 2019 and to raise awareness for the changes, all staff followed a mandatory information session beginning 2020. In addition, during their induction training all EDPS and EDPB newcomers attend a mandatory presentation on the Ethics Framework as well as a separate session dedicated to the new Anti-harassment Decision adopted in 2020.

In 2021, four virtual induction trainings have been organised for 25 newcomers. Furthermore, a dedicated intranet space provides an additional source of information with guidelines and relevant documents on ethics and staff conduct at the EDPS.

Beginning of 2021, in line with the specific Code of conduct for the Supervisor, the Supervisor completed and published his annual declaration of interest. During 2021, the newly appointed EDPS Ethics officer advised staff on ethical matters and received 25 formal requests related to the Code of Conduct for staff, mainly linked to the authorisation of external activities (in particular lectures and presentations) and publications. Following the assessment of the Ethics officer, the Supervisor and EDPS Director granted authorisations for 21 requests, while for 3 requests an authorisation was not deemed necessary and 1 request was withdrawn.

Evolution of ethics requests submitted under the EDPS Code of Conduct for all staff



During 2021, no cases of ethical misconduct or whistleblowing were reported and the EDPS was not involved in any European Ombudsman case or investigation by OLAF. This can be indeed seen as a very positive indicator for an ethically healthy organisation. It also confirms the positive acknowledgment by the budgetary authorities of the efforts made by the EDPS in the domain of professional ethics during the budgetary discharge exercises 2019 and 2020.

To maintain a high level of staff awareness, in 2022 it is foreseen to launch an awareness survey on the EDPS Ethics Framework and subsequently organise a series of 'Ethics refresher trainings'. Additional actions will also include the adoption of an EDPS specific 'patronage policy' and to explore with the Commission the possibility to join their Ethics module in Sysper with a view to introduce an e-workflow for Ethics requests at the EDPS. Together with EDPS senior management, the Ethics officer will continue to monitor the implementation of the EDPS Ethics Framework and assess any need for further revision, in particular in the light of the organisational changes and new ways of working induced by the ongoing pandemic.

3.2 Human resources

First of all, various data regarding the evolution of the workforce at the EDPS can be found in Annex 2, in particular as regards nationalities, gender, grades and categories of staff.

In addition, the EDPS HR sector has been working on different projects during 2021, notably:

- Management of the Covid-19 crisis and reflection on a back to the office strategy;
- Internal coaching and organisation of wellbeing actions for staff (New Wellbeing coordinator role)
- Automation of HR processes (appraisal exercise, management of the probation period)
- Launch of a new Data protection specialist competition
- Follow up of the 360 exercise for managers
- Relaunch of the EDPB secondment program

3.2.1 Management of the Covid-19 crisis and reflection on a back to the office strategy

The HRBA unit continued to adapt to the evolution of the COVID-19 pandemic and to the remote working, by implementing a return to the office policy divided in phases and by giving recurrent updates and information to staff as well as adapting the EDPS premises to safety and health measures required, in coordination with the EP and the medical service of the European Commission.

3.2.2 Internal coaching and organisation of wellbeing actions for staff (New Wellbeing coordinator role)

Due to the COVID-19 pandemic and its consequences on staff, the focus of the wellbeing activities went on helping our colleagues coping with the new way of working and supporting them as much as possible by proposing initiatives to increase morale and well-being.

On-line workshops were organised for all the EDPS/EDPB teams on finding balance and building resilience, co-facilitated by the EDPS internal coach and an external coach, raising awareness on stress patterns and burnout and how to alleviate stress and improve resilience. Participants also shared what they put in place to manage their stress.

A pilot co-development project was set up for heads of activities and deputy heads of unit at the EDPS/EDPB enabling colleagues to support each other and develop their professional practice.

Also, inspired by an initiative in the European Commission, the EDPS organised random virtual coffees for staff who could join on a voluntary basis. These coffees were continued up until it was possible to come to the office on a more regular basis.

In addition, the EDPS developed in November 2020 a new role aiming at supporting the wellbeing of EDPS/EDPB colleagues. The main purpose is to ensure that wellbeing activities and initiatives are organised for staff members.

In this context, HRBA launched in 2021 wellbeing actions in the form of motivational emails (TEDx talks) and meditation/healthy living tips send to colleagues.

The plan to inaugurate the new EDPS wellbeing room and launch leisure activities is postponed until mid-2022 for safety reasons linked to the pandemic. The wellbeing room can be used for meditation, yoga/pilates courses as well as for small seminars on wellbeing related topics. As to the leisure activities, a call for expression of interest was sent to all staff in September 2021. The call asked staff members which types of activities they would like to participate in. In addition, the call also targeted the search of volunteers to organise the activities.

Another action towards the wellbeing of EDPS-EDPB colleagues was to encourage them to create an ergonomic and healthy work environment when teleworking by reimbursing part of the ergonomic equipment.

3.2.3 Automation of HR processes

First paperless appraisal exercise

At the beginning of 2021, the EDPS successfully launched the appraisal exercise with the reference period 01/01/2020-31/12/2020 digitally. This allowed the EDPS to convert the procedure to paperless form and integrate it within our HR information system Sysper. Moreover, the EDPS was able to follow the different parts of the procedure and deadlines easily and increased the efficiency of the exercise. Before the exercise started, both staff members and managers were given information sessions regarding the steps, practical information, and new segments of the procedure.

Management of the probation period in Sysper

Throughout 2021, the EDPS started the preparatory works on the implementation of the new way of managing the probation periods in Sysper. The deployment of this module will allow the EDPS to transform the probation period reports from paper to digital environment. The module has been tested under different circumstances and the implementation is foreseen for 2022.

3.2.4. Launch of a new Data protection specialist competition

After preparatory works started in the end of 2019 and with the support of the European Personnel Selection Office (EPSO), a new administrator (AD) specialist competition was launched in September 2021. The aim of this competition is to have a reserve list of 76 data protection experts, from which we will be able to recruit as from the autumn 2022.

3.3 Budget

3.3.1. Allocated budget for 2021

In 2021, the EDPS was allocated a budget of EUR19.463.193. This represents a decrease of 0.07% compared to the 2020 budget (see Annex 3). The difference is mainly due by the reduction of the budget for EDPS and EDPB official staff salaries (which represents about 44% of the overall budget).

Other elements impacting the 2021 budget were the consolidation of the European Data Protection Board secretariat (created the 25th May 2018) for which the EDPS was

entrusted to provide an independent secretariat and the EDPS strategy 2020-2024 linked to the new mandate.

3.3.2. Budget execution 2021

As regards budget implementation, the overall rate in commitment appropriations amounted to 86% compared to 73% of the previous year. This rate is higher than the previous year but lower than the forecasted amount due to the impact of COVID-19 related restrictions on the Institution's activities.

Implementation of commitments in Title 1 shows an execution of 93% even if the global pandemic had restricted mission's activities and external trainings in presence.

For Title 2 the execution rate is at 82%. The budget lines associated to communication expenses, participation and organisation of events and the experts' expenses indicate an implementation rate below 70% due to the cancellation of all physical events in 2021. Furthermore for the same reasons explained above the pandemic slowed down the implementation of certain service and supply contracts.

As to Title 3, dedicated to the EDPB secretariat, the implementation rate was 79%. The effect was connected to the budget allocated to the meetings organised by EDPB with the national Data Protections Authorities. An initial amount of EUR 836,000 forecasted for 2021 and the final outturn of only 7% due to the COVID-19 pandemic. There were in consequence few travel expenses reimbursements and also other meeting related expenses (catering, interpretation, etc.) that were negatively affected.

3.3.3 Working methods

2021 marked the implementation of a new budget management tool, Bluebell. Bluebell is a tool developed and used by the ERCEA in order to:

- establish and revise forecast for the budget based on data uploaded and updated by operational units;
- give a finer view of all budget lines by detailing them into actions (activities) and linking these actions with posting criteria in ABAC so that the forecast can be compared in real time with the actual execution.

The implementation of this system is expected to increase the efficiency as the operational units will enter directly the appropriation requests in the system. The Finance team will in consequence not encode the information anymore but play a support and coordination role. In addition, the monitoring of budget execution will require less manual intervention and will in consequence be more reliable.

The roll-out of Bluebell will generate efficiency gains during the budget preparation and it will improve the monitoring and the follow-up of the budget implementation. It will also streamline the communication flows and establish a workflow of approval for any budget expenditures. Finally, it will be beneficial for audit trail purposes as files and supporting documents will be available anytime in the system.

As Bluebell would dramatically change our way of working, 2021 was a year where dedicated training was organised particularly in the last quarter of 2021. As of 2022 all units in EDPS are using Bluebell while entering the 2023 appropriations in the system.

3.3.4 Draft budget 2022 exercise

The 2022 budget exercise was conducted successfully to meet the priorities planned in EDPS and to comply with the instructions received by the European Commissioner. In practical terms it has required an in-depth analysis of the requested needs in order to stay within or below the ceiling of the forecasted appropriations established in the Multi-annual Financial Framework (MFF).

Apart from the above, which required substantial efforts from all units throughout the Institution, the exercise was also affected by the start of COVID-19 outbreak. It was, certainly at that point, difficult to foresee how long and to which extent the pandemic would affect the activities of the Institution and in consequence the appropriations needed to conduct them.

Notwithstanding these challenges, the EDPS successfully completed the exercise. The budget and MFF were subsequently approved by the budget authority without major modifications.

3.3.5. Discharge 2019 Budget

As every year, the Court of Auditors carried out an audit with respect to the reliability of the annual accounts and the annual activity report of the year N-2. The Court confirmed the absence of material error and the effectiveness of the control systems.

The Budgetary Authority subsequently granted the EDPS discharge in respect of the implementation of the 2019 budget and only issued some minor observations in its recommendation which the Institution will address.

3.3.6 Staff

In 2021 the tendency to grow in terms of staff numbers continued. Nine new positions (FTE) were granted by the Budgetary Authority in 2021 to cover the responsibilities stemming from Regulation 2018/1725, new supervisory tasks and new tasks for the EDPB, which resulted in a decrease of 55% since previous year, reaching a total of 123 staff members at the end of December.

3.4 Procurement and contracting

3.4.1 Professionalization

High standards of professionalism, ethical conduct, social and environmental standards are core values of EDPS's procurement management.

In 2021 EDPS played an important role when proceeding to the ex-ante control of procurement files. Particular focus has been made on the correct application of the Financial Regulation (FR) rules related to the exclusion criteria (Articles 136 to 141) by

ensuring ethical and non-discriminatory principles applicable to all interested economic operators. These fundamental values have been applied both in the management of Calls for tenders and in procedures related to the implementation of Framework contracts.

The EDPS constantly search for economic operators that are capable of ensuring qualified standards and proficiency in the implementation of the awarded contracts.

The EDPS ensured equal treatment, transparency and non-discrimination by applying these principles in each of the competition and guaranteeing possibilities for small and medium enterprises to have access to the market and therefore contributing to the accomplishment of social objectives such as employment and economic stability.

In addition the EDPS has applied environmental standards in particular when drafting the qualitative award criteria and demonstrating sensitiveness on green procurement.

The EDPS paid particular attention to the safeguard of data protection rules as well as EU standards on intellectual property rights. This has required ad-hoc drafting by adapting Tender documents provisions, ensuring the fulfilment of Data protection requirements related to Framework contracts implementation and inserting Data Protection Sheets as Annexes to Specific contracts.

The growing budget and the increasing number of procurement procedures requires the implementation of appropriate monitoring tools. HRBA has continued to assess the possibility to implement the Public Procurement Management Tool (PPMT) which is now used by the departments of the European Commission. As its implementation requires the implementation of ARES this project will need to be followed-up in 2022.

3.4.2 Framework contracts and concluded contracts

As in the previous years, in 2021 EDPS continued to implement the approach to reach to an higher degree of administrative efficiency participating in large inter-institutional Framework Contracts. The most important inter-institutional framework contracts we are relying on are related to IT consultancy, interim services, office supplies and office furniture.

In 2021, we have expressed our interest in participating in the following three inter-institutional procedures:

Reference	Subject	LC A	Interes t	Year
Call for tenders 10844	Subscriptions in the communication field	OP	Yes	2021
FWC N°06B30/2021/MC	Acquisition of office furniture and accessories	EP	Yes	2021
EPSO/EUSA/2022/OP/E	Training rooms in Brussels	EC	Yes	2021

In addition to the participation in these inter-institutional procedures, the EDPS conducted one procedure itself leading to framework contract that was cancelled for the reason of not sufficient number of admissible tenders.

Of the 87 procedures carried out, most of them were very low value procedures and procedures implementing existing framework contracts.

Among the procedures indicated above, two were conducted in order to sign direct service contracts.

Five negotiated procedures without publication to be reported in line with art. 74, 10 FR were concluded in 2021.

3.5. Finance

From 2020, the EDPS uses a new financial workflow Speedwell. It can be seen as an extension of ABAC, allowing the electronic circulation of invoices between all actors involved in a payment process and guides them through the verification. The system has an ECAS access which guarantees the identity of the person giving a visa, including the 'certified correct' visa of the invoice and 'passed for payment'. The implementation of this electronic workflow guaranteed the business continuity while remotely working due to the COVID-19 pandemic.

Statistics related to ex-ante controls

In 2021, the number of financial transactions continued to decrease substantially. This is a consequence of the pandemic and the related travel restrictions. The cancellations of non-essential work related travel resulted in the quasi absence of mission and expert reimbursements (which normally constitute a substantial part of the payment request processed by the EDPS).

Payment requests

	2019	2020	2021
Experts reimbursement	1542	319	21
Missions	298	85	53
Other	532	363	298
Grand Total	2372	767	372

In parallel, with the growth of the EDPS and the new budget structure (the budget structure changed as of 2021 mostly in order to better reflect the actual needs of the Secretariat of EDPB), the number of commitments increased a lot between 2020 and 2021 (+26.72%) from 131 to 167. The growth is mainly visible in the provisional commitments (+57%). Another explanation is the introduction of Bluebell, which required a more precise image of the Institution needs.

As required by art. 74.5 of the Financial Regulation, all operations are subject to ex-ante controls. These controls comprise the initiation and ex-ante verification of an operation and concern both the operational and financial aspects. They are operated by staff with the required skills appointed by the Authorising Officer by Delegation.

The EDPS uses checklists listing the basic controls to be operated by the operational and financial agents involved in the processing of the operations. Since the beginning of 2020, the EDPS uses a new electronic processing system (Speedwell) which is connected

with the accounting system (ABAC) and facilitates substantially the aforementioned basic controls applied on payments and commitments.

Missions, expert payments and salaries are processed by the Paymaster Office of the European Commission (PMO) in application of the Service Level Agreement concluded between the respective Institutions. These payments are subject to an additional layer of ex-ante controls which are operated by the PMO staff in addition to the controls applied at the EDPS.

	Total	Refused	
Payment orders	426	23	5,40%
Commitments	311	34	10,93%
Total	737	57	8,17%

(*) A payment order can contain several payment requests

3.6 Missions management

Missions' management at the EDPS is conducted in accordance with the applicable rules of the Commission's Guide to Missions. The EDPS has adopted a speaking engagement policy, which clarifies the rules in those cases where the mission expenses should be paid by the organiser and is selective as regards attendance to external events.

For 2021, mission statistics only relate to the months June to December. All missions from begin January till June were not allowed due to the Covid 19 confinement. From June, only essential missions were allowed.

2021	Supervisor	Staff
N° missions	6	57
Average cost	€446	€505

The chart above provides information about the number of missions and the average cost. All missions of the Supervisor are conducted with full transparency as provided in their Code of conduct. Missions by staff are encoded in MIPs and a mission report is uploaded as a supporting document in the statement of expenses.

As requested by the European Parliament in the previous discharge report, the two following tables give more detailed information in terms of transparency.

N° DAYS + COSTS PER TEAM 2021			
UNIT/SECTOR	N° MISSIONS	TOTAL COSTS €	AT CHARGE ORGANISERS
DIRECTOR	10	4.230,46	2
CABINET	2	1.030,87	
SUPERVISION & ENFORCEMENT	16	8.469,31	
POLICY & CONSULTATION	14	7.927,63	
HRBA	1	216,39	
ITP	11	5.065,95	2
EDPB	3	1849,06	
TOTAL EDPS/EDPB	57	28.789,67	

SUPERVISOR 2021 (detailed list in Annex 4)		
NAME	N° MISSIONS	TOTAL COST
WIEWIOROWSKI Wojciech Rafal	6	2.675,36

The EDPB Chair performed 2 missions in 2021.

EDPB CHAIR 2021		
NAME	N° MISSIONS	TOTAL COST
JELINEK Andrea	2	1.186,40

In order to comply with the recommendation of previous discharge reports which calls for an overview in the Supervisor's annual activity report of the sections on procurement and missions' management, a comparative table of the last four years is included below. However, for 2020, mission statistics only relate to the months from January to March. All missions from mid-March 2020 till June 2021 have been cancelled due to the Covid 19 confinement.

	2018		2019		2020		2021	
	Members	Staff	Members	Staff	Member	Staff	Member	Staff
Number of missions	39	204	29	301	4	39	6	57
Average cost in €	885	701	885	701	537	578	446	505
Total cost in €	34.517	143.107	17.800	207.497	2.147	22.547	2.675	28.789

4. Management and internal control

4.1 Characteristics and nature of activities

4.1.1 The mission of the EDPS

Data protection is a fundamental right, protected by European law and enshrined in Article 8 of the Charter of Fundamental Rights of the European Union.

In order to protect and guarantee the rights to data protection and privacy, the processing of personal data is subject to control by an independent authority. The European Data

Protection Supervisor (EDPS) is the European Union's independent data protection authority, tasked with ensuring that the institutions and bodies of the EU (EUI) embrace a strong data protection culture.

In accordance with Regulation (EU) 2018/1725 (1) the EU as a policy making, legislating and judicial entity looks to the EDPS as an independent supervisor and impartial advisor on policies and proposed laws which might affect the rights to privacy and data protection. The EDPS performs these functions by establishing itself as a centre of excellence in the law, and in technology, insofar as it affects, or is affected by the processing of personal data.

The EDPS carries out its functions in close cooperation with fellow data protection authorities (DPAs) as part of the European Data Protection Board (EDPB), and aim to be as transparent as possible in its work serving the EU public interest. Under the General Data Protection Regulation (GDPR), the EDPS is also responsible for providing the secretariat to the EDPB.

Furthermore, the EDPS is also in charge of supervising the processing of personal data relating to activities at the EU's law enforcement agency, Europol and the EU's agency for judicial cooperation, Eurojust. The relevant legislation in this case is Regulation (EU) 2016/794, which applies to Europol and Regulation (EU) 2018/1725 and Regulation (EU) 2018/1727, which applies to Eurojust. A similar, specific data protection regime is in place for the European Public Prosecutor's Office (EPPO).

The EDPS:

- monitors and ensures the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals.
- advises EU institutions and bodies on all matters relating to the processing of personal information. We are consulted by the EU legislator on proposals for legislation and new policy development that may affect privacy.
- monitors new technology that may affect the protection of personal information.
- intervenes before the EU Court of Justice to provide expert advice on interpreting data protection law.
- cooperates with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal information, in particular both as a provided of the Secretariat and member of the European Data Protection Board.

In addition, the EDPS:

- Aims to develop a culture of accountability whereby the institutions recognise their own responsibility to ensure the protection of personal data when developing new EU policies and legislation;
- Provides support to the EU institutions to be accountable: to help the legislators carry out their own assessment of proposed measures implying the processing of personal data, the EDPS has developed a toolkit on the concept of necessity;
- Aims to provide pragmatic advice by analysing the complexity of a proposal and take advantage of the experience gained in its supervision cases with the EU institutions; the EPDS looks for constructive and workable solutions;

- As an advisor on all data protection matters at EU level, in addition to providing advice on a consultation by the Commission (or other institution), the EDPS also issues advice on its own initiative, when there is a matter of particular significance;
- The EDPS is not for or against any measure involving the processing of personal data and bases its assessment and advice on the evidence justifying its need.

4.1.2 Core values and guiding principles

4.1.2.1 The core values

The EDPS approach to its tasks and the way in which it works with its stakeholders are guided by the following values and principles:

- **Impartiality** – working within the legislative and policy framework given to the EDPS, being independent and objective, finding the right balance between the interests at stake.
- **Integrity** – upholding the highest standards of behaviour and to always do what is right.
- **Transparency** – explaining what we are doing and why, in clear language that is accessible to all.
- **Pragmatism** – understanding its stakeholders' needs and seeking solutions that work in a practical way.

4.1.2.2 General principles

1. The EDPS serves the public interest to ensure that EU institutions comply with data protection policy and practice. He contributes to wider policy as far as it affects European data protection.
2. Using his expertise, authority and formal powers to build awareness of data protection as a fundamental right and as a vital part of good public policy and administration for EU institutions.
3. He focuses his attention and efforts on areas of policy or administration that present the highest risk of non-compliance or impact on privacy. He acts selectively and proportionately.

4.1.3 Data Protection and the EDPS in 2021

The characteristics and nature of activities at the EDPS dealing with data protection are dealt in point 2 of the present report. This section deals only with communication and internal IT.

4.1.3.1 Communicating data protection

Communicating data protection

Effective communication is key to ensure that information on EDPS activities reaches the relevant audience at the right time. The health crisis which started in 2020 has accelerated the pace of digital transformation and increased even more public interest and engagement with data protection. With this in mind, the EDPS communication activities in 2021 aimed to further build on successes of previous years and reinforce our status as

a respected, international leader in the data protection field. This included efforts in such areas as online media, events, publications and external relations with press and stakeholders.

In 2021, the main EDPS communication exercises were directly linked with implementation of the EDPS Strategy 2020-2024¹³. We continued to raise awareness about EDPS activities as part of its role as supervisor, policy adviser and partner to fellow Data Protection Authorities.

The EDPS has also started preparatory work for the EDPS conference planned for June 2022. This included development of a new, dedicated conference website¹⁴, drafting a detailed communication plan, procurement activities as well as first promotional activities informing public about the forthcoming event.

The EDPS has a well-established presence on three social media channels: Twitter, LinkedIn and YouTube. These channels, available directly from the [EDPS website](#)¹⁵, allow EDPS to communicate easily and quickly with its various audience groups.

In 2021 the EDPS continued its efforts to implement an effective social media strategy which helped to expand its influence and outreach online. Additionally, in 2021, together with colleagues from the T&P unit, the EDPS I&C team, launched preparatory work to ensure EDPS presence on two alternative and data protection friendly social media: Mastodon (open source social media 'Twitter style') and PeerTube (open source social media 'YouTube style'). The EDPS presence on these two new channels will be concretised in the first semester 2022, in an attempt to lead by example for an EU digital sovereignty.

4.1.3.2 EDPS IT infrastructure

The EDPS' current major IT infrastructure is supplied by the European Parliament (e.g. network, hardware, office software, mail servers, and mobile devices). The EDPS uses also software provided by other EUIs, whereas its content management system is outsourced to a private company.

In order to steer the digital transformation propelled by the COVID-19 pandemic, the EDPS is currently reflecting on its choices on its IT infrastructure and the agility and independence of the EDPS with respect to IT. The objective would be to achieve more EDPS autonomy and control in relation to IT infrastructure with possibly creating a specific organisational team in the EDPS specifically tasked with deploying, supporting and developing the IT infrastructure (as in the EDPB).

In 2020 we planned for an EDPS digital transformation study. In 2021, we concluded the first phase of the project, called "IT gap analysis", which assessed the EDPS IT business requirements, inventoried IT assets and started looking at first possible solutions to fill gaps to support EDPS tasks. In 2022 we will carry out the second phase of the project with

¹³ https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf

¹⁴ <https://www.edpsconference2022.eu/en>

¹⁵ <https://edps.europa.eu/en>

a feasibility study on a future EDSP IT infrastructure and relevant IT management organisation.

4.2 Strategy 2020-2024

4.2.1 EDPS strategic objectives

The EDPS issued in June 2020 its 2020-2024 Strategy 'Shaping a Safer Digital Future: a new Strategy for a new decade'. In a connected world, where data flows across borders, solidarity within Europe, and internationally, will help to strengthen the right to data protection and make data work for people across the EU and beyond. The Strategy focuses on three pillars: foresight, action and solidarity to address digital challenges for a safer, fairer and more sustainable future. Its 3 strategic pillars and related actions are detailed in Annex 5.

4.2.2 Action plan

The related action plan is detailed in Annex 6. This action plan is implemented and monitored through the yearly annual management plan (AMP).

4.2.3 Measuring performance

The EDPS uses a number of key performance indicators (KPIs) to help it monitor its performance in the context of the main objectives set in the EDPS Strategy. This ensures that it is able to adjust its activities, if required, to increase the impact of its work and the efficiency of its use of resources¹⁶.

The KPI scoreboard below contains a brief description of each KPI and the results on 31 December 2021. These results are measured against initial targets, or against the results of the previous year set as benchmark.

In 2021, we met or surpassed - in some cases significantly - the targets set in eight out of nine KPIs, with one (KPI8 - Occupancy rate of the establishment plan) just falling short of the set target. These results clearly illustrate the positive outcome we have had in implementing our strategic objectives throughout the year, notwithstanding the challenging circumstances in which the EDPS still had to operate in the context of the Covid-19 Pandemic.

KEY PERFORMANCE INDICATORS		Results 31.12.2021	Target 2021
KPI 1 Internal indicator	Number of initiatives, incl. publications, on technology monitoring and on promoting technologies to enhance privacy and data protection organised or co-organised by EDPS	16 initiatives	10 initiatives

¹⁶ The KPIs were partly revised at the end of 2020, to ensure that the performance metrics adapt to developments in EDPS activities.

KPI 2 Internal & External Indicator	Number of activities focused on cross-disciplinary policy solutions (internal & external)	8 activities	8 activities
KPI 3 Internal Indicator	Number of cases dealt with in the context of international cooperation (GPA, CoE, OECD, GPEN, Spring Conference, international organisations) for which EDPS has provided a substantial written contribution	17 cases	5 cases
KPI 4 External Indicator	Number of files for which the EDPS acted as a lead rapporteur, rapporteur, or a member of the drafting team in the context of the EDPB	23 cases	5 cases
KPI 5 External Indicator	Number of Article 42 opinions and joint EDPS-EDPB opinions issued in response to EC legislative consultation requests	17	Previous year as benchmark
KPI 6 External Indicator	Number of audits/visits carried out physically or remotely	4 audits + 1 visit 43 EUIs impacted	3 different audits/visits 30 EUIs impacted.
KPI 7 External Indicator	Number of followers on the EDPS social media accounts ¹⁷	T 25826 L: 49575 YT:2438	Results of previous year + 10%
KPI 8 Internal Indicator	Occupancy rate of establishment plan	88%	90%
KPI 9 Internal Indicator	Budget implementation	86,12%	80%

4.3 Inter-institutional cooperation

In 2021, inter-institutional cooperation continued in the areas in which the EDPS is assisted by other EU institutions and bodies.

¹⁷ Twitter, LinkedIn, YouTube.

The Commission's assistance is extremely valuable to us in particular with regard to financial, accounting and budgetary matters. DG Budget provides technical assistance to the EDPS in financial and accounting matters and the Central Financial Service assists our small organisation providing information upon request. The Commission's Accounting Officer acts simultaneously as Accounting Officer to the EDPS. The same applies to the Commission's Internal Audit Service.

Inter-institutional cooperation presents many advantages from the perspective of good financial management and budget consolidation. This cooperation is vital for the EDPS, not only because of the small size of our organisation, but also because it increases efficiency and allows for economies of scale; in addition, most of the expenditure remains within the EU administrations, therefore resulting in appreciable savings for the EU budget.

4.4 Ex post controls

According to art. 74.6 of the Financial Regulation, the Authorising Officer can organise, in addition to the mandatory ex-ante controls, also ex-post controls on sample basis depending on risks related to the transactions. As the Institution grew over the years with a substantially increasing budget and number of financial transactions, the EDPS Director, being the Institution's Authorising Officer by Delegation, appointed a verifier who issued ex-post verification reports since 2011. Results and major findings were systematically taken into consideration to re-enforce the existing internal controls.

Due to an internal re-organisation at the end of 2019, whereby the previous ex-post verifier was re-assigned to a position within the Finance Team, the ex-post could not be carried out. In order to avoid the risk of self-review, the ex-post verifier should not be involved in the financial circuits but on the other hand, have a thorough understanding of the financial legal and regulatory framework. For a small Institution as the EDPS, it was therefore not possible to find a replacement fulfilling both of the aforementioned requirements even after an Institution wide call for expression of interest was launched.

It is only at the end of 2021 that we managed to recruit a new colleague with the appropriate knowledge who will be appointed as ex-post verification agent. Moreover, new guidelines, based on the ones being currently adopted in DG BUDG, will be drafted to describe the applicable methodology. An internal decision will be prepared to implement the guidelines in view to perform the ex-post controls of 2021 financial transactions.

4.5 Events during the year that affected reputation

There were no events during 2021 that might have had a negative impact on the institution's reputation. The business continuity plan in place was effective and the period of compulsory closing of our premises did not lead to any issues of significance. The teleworking scheme was smooth and did not lead to any incidents.

4.6 Internal control management system

Internal control covers the totality of the policies and procedures put in place by the institution to ensure the economic, efficient and effective achievement of its objectives. In order to assess and improve the effectiveness of the internal control system, in 2013 the EDPS adopted 15 out of the 16 Internal Control Standards (ICS), laid down in the European Commission decision of 2007¹⁸ ¹⁹. The ICS decision was revised on 12/11/2019 in order to update the legal framework applicable to the EDPS. Furthermore, in the context of the Court of auditors' audit in relation with the Statement of Assurance 2019, the Court of Auditors in its decision of 6 of May 2020 requested the EDPS to update its ICS decision in order to formalise the applicability of ICS 16.

Indeed, since its decision of 22 January 2013 on ICS, the EDPS decided that the ICS 16 as laid down in the European Commission decision of 2007, related to the Internal Audit Capability, was not applicable to it. The EDPS especially considered that the IAS being the internal auditor of the EDPS and taking care of the annual audit work plan which is the main task of the Internal Audit Capability, there were no need of applying ICS 16. The Court wanted the EDPS ICS decision to be clearer on this specific issue. Therefore a revised ICS decision was adopted on 06 October 2020 indicating that the EDPS relies on the internal audit capability provided by the European Commission. It is based on a Service Level Agreement. The IAS is setting up for the EDPS the annual audit work plan and as such, the EPDS applies the relevant provisions of the Financial Regulation as regard the implementation of an Internal Audit function.

In order to provide adequate visibility to all EDPS about the manuals and internal procedures, in 2020 we established the so-called "book of rules"). In this space of the EDPS intranet, the documents are categorized by units, sectors and by themes. The Governance and Internal Compliance Sector oversees and updates the book or rules as necessary.

The EDPS also establishes an Annual Management Plan on a yearly basis. That plan shall translate the long term strategy of the EDPS into general and specific objectives. The plan sets out the activities to be undertaken by specific objectives. The Annual Management Plan also includes the key performance indicators, defined in the Strategy 2020-2024, which are regularly measured to monitor progress achieved during the implementation phase.

Since the adoption of the decision on risk management in July 2012 –modern tools that help to identify the risks and possible plans of action- the EDPS has included risk management as an essential element of its global strategy. Risk management goes beyond assessing the risks; it also involves putting controls and measures in place that then need to be monitored. This assessment of risks and controls and measures in place is detailed in a risk register which is adopted, with close involvement of all managers of the organisation, at the end of every year. The 2021 risk register was formally adopted at the Management Meeting of 17 March 2021 whereas the 2022 risk register was presented at

¹⁸ Communication SEC(2007)1341.

¹⁹ Only ICS number 16 related to Internal Audit Capability is not applicable to the EDPS.

the Management Meeting of 30 March 2022. In view of the sensitivity of some of the issues mentioned in the register, the risk register is only disclosed upon request.

These controls put in place by the EDPS, along with the procedural channels, are intended to correct any financial or procedural error that might arise. They are an integral part of the management of the EDPS, as are any corrections to which they give rise. The AOD is thus aware of any corrections. Neither the nature nor the frequency of the identified risks has been significantly relevant.

4.7 Internal evaluation of the internal control system and indicators underpinning the statement of assurance

The monitoring of the implementation of the ICS is the responsibility of the Internal Control Coordinator (ICC), who reports directly to the Director. The ICC also meets the EDPS units/sectors to ensure effective implementation.

Since July 2014 a report on the implementation of the ICS was established twice a year to assess their effectiveness. The report is presented to the Management Board. Following a suggestion from the Court of Auditors, the ICS monitoring report is now issued once per year.

Furthermore, the ex-post facto verification and the accounting correspondent functions monitor, on a sample basis, the legality and regularity of the financial transactions as well as the quality of accountancy once a year. At the end of 2021 the EDPS recruited a new colleague with the appropriate background to be appointed as ex-post verification agent (see point 4.4. above).

This enables the institution to demonstrate that the overall internal control system is effective, not only that sufficient controls are in place but also that these controls take account of the risks involved and are effective.

At this stage, the AOD estimates that the level of management and control put in place is appropriate and improving. Such improvements are not likely to have a 'material' impact within the meaning of paragraph 0. No reservations are necessary with regard to the improvements underway.

At the time of writing this annual activity report, no significant errors have occurred, and no reservations are necessary as regards preventive controls.

No recommendations that are currently being implemented are therefore likely to have a material impact²⁰.

4.8 Cost effectiveness and efficiency of Internal Control

Being a very small Institution, the EDPS has neither the means nor the resources to carry out a classic cost-benefit analysis. Therefore, we have taken as a base the model applied by EPSO, since this office, as the EDPS, only manages administrative appropriations under Heading V of the EU budget. This model consists of a single global indicator which is

²⁰ The materiality criteria used for this judgment are given in Chapter 0 of this report.

calculated by dividing the approximate total cost of control by all expenditure made during the year (budget implementation in terms of payments).

The total number of FTE's involved in the four main control activities (internal control, procurement and finance) is estimated at around 5 FTE's.

The estimated average cost (all categories of cost included) of the control activities for 2021 would be around 550.406 Euros.

The total budget implementation in terms of payments for 2021 is expected to be of 15.548.213 EUR. It means that the cost of the internal control activities represents only 3.54% of the EDPS expenditure.

4.9 Results of independent audit during the year

There are two independent audits applicable to the EDPS: the European Court of Auditors and the institution's Internal Auditor.

4.9.1 Court of Auditors

4.9.1.1 Statement of Assurance (SoA) 2021 on Administrative Expenditure

In the context of the SoA 2021 approach as regards legality and regularity, the Court of Auditors selects one transaction for the main sample. If the transaction(s) hit is a payment resulting from a contract signed in the period 2011 - 2021, the Court of Auditors will audit the related procurement procedure and treat any error according to their methodology (i.e. a significant error results in the whole payment being considered as affected by a 100% error). For the Statement of Assurance 2021, the Court of Auditor selected one payment request from the EDPS, namely EDP. 7660.

As a specific topic, under SoA 2021, the Court will examine a sample of procurement and recruitment procedures made by the EEAS. The EDPS is not included in the scope of this task.

As regards audit work on supervisory and control systems and the Examination of the 2021 Annual Activity Report (AAR), in SoA 2021, the Court of Auditors applies a rotational approach in terms of the assessment of supervisory and control systems (except for the Commission), by which they examine in-depth the systems of two/three institutions and bodies each year.

The EDPS was selected for the in-depth assessment of systems for SoA 2019. Therefore, in SoA 2021, the work was limited and included only:

-  Internal procedure manuals;
-  Ex-ante and ex-post verifications of commitments and payments;
-  Registers of exceptions;
-  Summary reports and indicators on (ex-ante and ex-post) controls;
-  Recent relevant internal audit reports;

- ✚ Self-assessments on compliance with, and effectiveness of, internal control standards;
- ✚ Risk assessments;
- ✚ AARs.

The Court of Auditors' approach as regards the audit of the accounts and other work on supervisory and control systems and on the annual activity report remains the same as in previous years. On rotational basis (except for the Commission), they will examine in-depth the accounts of one/two institution(s) and bodies each year. The Court of Auditors may select the EDPS for this in-depth review for SoA 2021.

At the date of issuing this AAR, the Court of Auditors is issuing its statements of preliminary findings for two audit modules: (1) Substantive testing of a random sample of transactions; and (2) follow up of previous years' observations. The final report will only be made public at a later stage, most probably in July. The EDPS will be informed in case of any remarks.

4.9.1.2 Statement of Assurance 2020 - Conclusions

The Statement of Assurance of the European Court of Auditors concerning the financial year 2020 (SoA 2020) did not contain any observation on the reliability of the 2020 provisional accounts.

The audit examined the 2020 regularity of transactions and the supervisory and controls systems of the EDPS. This examination did not give rise to any observations.

4.9.1.3 Statement of Assurance 2019 - Clearing Letter 10195

Regarding the issues reported by the Court of Auditors in the clearing letter of 7 April 2020 concerning the SoA 2019, the EDPS has been informed that:

- On the formalisation of the applicable Internal Control Standard (ICS) N°16 in the EDPS decision on ICS requested by the Court. The ICC issued a new ICS decision on 5 October 2020 indicating that the EDPS relies on the internal audit capability provided by the European Commission. It is based on a Service Level Agreement. The observation is **closed** for the Court of Auditors.
- On the requirement of Article 123 of the Financial Regulation to set up an internal audit progress committee, the EDPS explained to the Court of Auditors that the Internal Control Coordinator (ICC) ensures a comprehensive monitoring of the implementation of the recommendations made by the internal auditor with an excellent record that has never led to any complaints or difficulties with our internal auditor. The Court of Auditor has decided to change this remark into recommendation and has therefore, **closed** the observation.
- On the weaknesses in the Policy on identification of sensitive functions, the EDPS conducted a review and adopted "Guidelines on identification and management of sensitive functions" at the Management meeting of 13 January 2021 focusing on differentiation between sensitive functions and sensitive posts; complete further the list

of sensitive functions; assessment of mitigating measures; and setting up a monitoring system to keep the assessment as an alive process. Moreover, the EDPS adopted a “Decision on the Inventory of Sensitive Functions” that complements the said Guidelines, and establishes the list of sensitive functions at the EDPS and adopts the record of the risks inherent to the said sensitive functions and the mitigating controls. The observation is **closed** for the Court of Auditors.

- On the absence of timely monitoring of ABAC rights, the HRBA unit appointed a new colleague for this function and the periodical review of the active accesses was carried out in line with the relevant guidelines of DG BUDG. The observation is **closed** for the Court of Auditors.

- On the weaknesses in the formalisation of the financial workflows and designation of financial actors, the revised EDPS Financial Guide has been formally adopted at the Management Meeting of 17 March 2021. The new guide includes the necessary updates and integrate all finance related working instructions. Financial circuits and responsibilities of the different financial actors are only few of the topics covered. For transactions, where the validation is prepared by another entity (e.g. PMO), there is a more elaborate description of the differentiated responsibilities between entities. In addition, the necessary annexes, such as ex-ante checklists, charters of the financial actors, are attached to the guide. The updated checklists have been integrated in our new electronic workflow system (Speedwell). The EDPS is **waiting for the confirmation that the observation is closed** by the Court of Auditors.

- On the weaknesses in the ex-post verification process and inadequate disclosure of results in the annual declaration of assurance. At the beginning of 2022 a new colleague with the appropriate knowledge has been identified to be appointed as ex-post verification agent. Moreover, the EDPS is about to start the process of drafting new guidelines that will be based on the ones being currently adopted in DG (also available on BudgWeb). An internal decision will be prepared to implement the guidelines describing the applicable methodology in view to perform the ex-post controls of 2021 financial transactions. The EDPS is **waiting for the confirmation that the observation is closed** by the Court of Auditors.

- On the weaknesses in the register of exceptions, the Director of the EDPS adopted on 17/12/2019 a decision which covers comprehensively and substantially the types of deviation that are subject of the new procedure as well as the formalities to be accomplished. This relates more in particular to the use of a form covering the background of the deviation, impact and remediating actions. It furthermore specifies which staff should be involved with their respective responsibilities and provides a circulation sheet to be used for the routing. Following the Court of Auditors’ recommendation, the decision has been completed with the information on the provision or rule from which there has been a deviation. The exception register and the forms as well as the supporting documents related to the individual cases are registered and stored digitally in the Case Management System. The implementation of this updated procedure ensures proper documentation and facilitates reporting on the exceptions and non-compliance events. Ex-ante checklist are adapted to the recommendation whereby the standard question on exception justification is replaced by the obligation of financial actors to justify a negative

answer on questions. The EDPS is **waiting for the confirmation that the observation is closed** by the Court of Auditors.

4.9.2 Internal Audit Service (IAS)

The Commission's Internal Auditor is the internal auditor of the EDPS. To make sure that EDPS resources are effectively managed, the internal auditor conduct regular checks on EDPS internal control systems and on its financial transactions.

In 2019-2020 the IAS conducted an audit of the EDPS activities when supervising Europol. The objective of the audit was to assess the adequacy and effectiveness of the internal control system for the supervisory activities related to Europol, activities related to the Secretariat of the Europol Cooperation Board, and the IT security controls specifically related to the above-mentioned activities. The fieldwork was finalised on 13 March 2020. The final Audit Report on the Supervision of the processing of personal data by Europol by the European Data Protection Supervisor was issued on 24 September 2020.

The auditors recognised the ongoing efforts of the EDPS to improve the governance arrangements and internal control systems for the Supervision of Europol. The EDPS has put in place the necessary processes for managing the supervision of the processing of personal data by Europol in compliance with its regulation. However, the Internal Audit Service concludes as a result of its audit that a number of significant weaknesses exist that could negatively impact the effectiveness and efficiency of these processes. It found significant weaknesses relating to the follow-up of EDPS recommendations, the IT security controls applied to Europol-related information and with regard to IT security governance. The IT-related weaknesses should be seen in the context of the current small size of the EDPS' IT operations and its limited capacity for implementing IT controls to mitigate risks stemming from handling sensitive non- classified and classified information. As a consequence, the IAS issued 6 recommendations for implementation by the EDPS.

On 15 October 2020, the EDPS has proposed and sent to the IAS an action plan for following up all IAS recommendations and on 21 October 2020, the IAS acknowledged the action plan considering it was adequate to mitigate the risks identified. The ICC ensured a close follow up regarding the deadlines agreed and the content, to be able to upload accordingly the IAS database, Team Central.

During 2021, EDPS successfully completed most of the action plan, under the coordination of the ICC between EDPS responsible functions and IAS. Thanks to the implementation of these actions, the EDPS improved its IT security posture not only with regard to the Europol Supervision activities but horizontally across all EDPS activities involving IT security and cybersecurity. Some indicative examples include, a revamped EDPS information security policy, a Risk Management Framework supported by a Risk Assessment tool, new topic specific security policies such as Acceptable Use Policy and Access Control Policy and improved regular user awareness activities, including specialized cybersecurity trainings.

At the time of the issuance of this AAR 2021, the IAS has closed four out of the six recommendations, while one is awaiting review and another one has been downgraded from "very important" to "important" due to the progress made in 2021. The EDPS expects to finalise the implementation of this last recommendation by mid-2022.

Recommendation / Issue type	Relevance	Status
Follow-up of EDPS recommendations by Europol	Very important	Closed
Controls for handling EUCI within the context of supervisory activities	Very important	Closed
Service provider management	Very important	Closed
IT Security Governance	Downgraded from very important to important due to progress made	Open
Establishing the supervisory strategy	Important	Closed
Technical guidelines for performing supervisory activities	Important	Ready for review

In July 2021 the IAS launched an in-depth risk assessment of the EDPS in order to establish the IAS Strategic audit plan in the EDPS for the next three years. In the context of this assessment, the ICC in collaboration with the EDPS responsible functions provided the necessary information to the IAS. After the risk assessment exercise, the IAS selected two audit topics for 2022-2024, namely (1) Risk assessment methodology for the planning of EDPS audits; (2) Governance arrangements for IT services provided by the European Parliament to the EDPS. Moreover, the IAS has identified the following potential reserve audit topic, i.e. Methodology for carrying out investigations.

4.9.3 ICS monitoring situation

The EDPS follows 14 of the 16 ICS established by the European Commission (see EDPS decisions 2012 and 2015). The ICS are regularly monitored and a report is issued annually to keep management up to date with their implementation. The ICS decision was revised on 12 November 2019 in order to update the legal framework applicable to the EDPS. A newly revised ICS decision was adopted on 6 October 2020 indicating that the EDPS relies on the internal audit capability provided by the European Commission (see point 4.6 above).

The last ICS report was issued on 11 April 2022. According to the ICC's report, the ICS monitoring situation at the EDPS was the following: The EDPS report on the implementation of the ICS shows that the level of internal control is satisfactory and effective. IAS and Court of Auditors recommendations are closely monitored and implemented. The same goes with other action plans and expected deliverables. The EDPS will continue to ensure a regulatory and organisational framework in line with the legitimate expectations linked to its growing importance in the panorama of EU institutions.

4.9.4 Follow-up to the European Parliament's discharge resolution of 2020

On 22 October 2021, the EDPS provided answers to the 2020 discharge questionnaire. A document of 38 pages is available on request. The related hearing on the 2020 discharge took place at the European Parliament on 08 November 2020.

At the issuance date of the AAR, the report is not tabled yet for plenary and no date can be given for the circulation yet. The EDPS is therefore waiting for the final report of the discharge.

4.10 Conclusions on the effectiveness of internal control

In light of the information above, with all observations of the Court of Auditors being implemented, the authorising officer by delegation considers that the internal control system is operating appropriately; bearing in mind the level of expenditure and budget handled by the institution, and thus gives the necessary assurance to his annual statement.

5. Reservations and impact on the statement

5.1 Materiality criteria

In order to establish the Statement of Assurance the AOD applies the materiality criteria adopted by the Court of Auditors.

5.1.1. Objectives of materiality criteria

The materiality threshold gives the AOD a basis on which to establish the significant weaknesses that require a formal ²¹ reservation to his statement. The assessment of a weakness falls to the qualitative and quantitative judgment of the authorising officer by delegation, who remains responsible for the statement of assurance, including the reservations made.

The purpose of this chapter is to define the qualitative and quantitative criteria for determining the level of materiality.

5.1.2. Qualitative criteria

The following parameters were used to establish significant weaknesses:

- significant/repeated errors without mitigation;
- weakness in the internal control system;
- insufficient supporting documents;
- material problems identified by the Court of Auditors or the Internal Audit Service;
- problems of reputation;

²¹ The Commission (COM (2003)28 of 21 January 2003) considers that only 'material' reservations can be used to qualify the annual statement.

5.1.3. Quantitative criteria

Once a significant weakness has been identified, quantitative criteria must be applied to determine the level of materiality. This level will be used to determine whether the weakness 'merits' being reported.

- margin of error
- maximum amount of risk.

The Court of Auditors uses a 2% materiality threshold. Should the residual risk of an error be higher, the institution must explain the reasons for this.

The EDPS has decided on 2% of annual appropriations as the materiality threshold in this regard, namely: EUR 389.539,96 €.

5.1.4. Criteria of the Internal Audit Service

A 'table of significance' is added to the internal auditors' report. In this table, a distinction is made between recommendations and observations on the one hand, and levels of importance on the other: critical, very important, important and desirable. According to the internal auditors, only 'critical' level observations **may** result in a reservation in the statement given in the annual activity report. For the EDPS, there are no observations at this level, as indicate in Section 4.9.2 above.

5.2 Reservations

No reservation.

5.3 Conclusion

Based on the above, the Director of the EDPS Secretariat has issued the annual statement with no reservation.

6. Statement of assurance from the authorising officer by delegation

I, the undersigned, Leonardo CERVERA NAVAS, Director of the EDPS Secretariat, as Authorising Officer by Delegation, hereby declare that the information contained in this report is true and faithful.

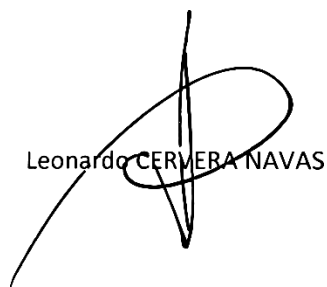
I state that I have had reasonable assurance that the resources allocated to the activities described in this report have been used for the purposes anticipated and in accordance with the principle of sound financial management, and that the control procedures

established provide the necessary guarantees as to the legality and regularity of the underlying operations.

This reasonable assurance is based on my own judgment and on the information available to me, such as the results of the self-evaluation and the report of the Internal Audit Service.

I confirm that I am not aware of any matter not reported that might be harmful to the institution's interests.

Signed at Brussels on 11 April 2022



Leonardo CERVERA NAVAS

7. Annexes

Annex 1: Summary of annual activity report

The Financial Regulation (Article 74.9)²² provides that the annual activity report for the financial year of the authorising officer of Union institutions, Union bodies, European offices and agencies shall be published by 1 July of the following financial year on the website of the respective Union institution.

Following the report on discharge in respect of the implementation of the general budget of the European Union for the financial year 2016 issued on 26 March 2018, the European Parliament requested to set a deadline for the submission of the annual activity reports of 31 March of the year following the accounting year. Due to certain external factors, this report has been adopted on the 11 April 2022.

Alongside this, Article 60 of Regulation (EC) No 2018/1725 provides that the EDPS shall submit an annual report on his/her activities to the European Parliament, the Council and the Commission. The proposal is thus to summarise the authorising officer by delegation's annual activity report and include this summary in the activity report that is provided for in Article 60 of Regulation (EC) No 2018/1725:

Overall, the European Data Protection Supervisor considers that the internal control systems in place provide reasonable assurance as to the legality and regularity of the operations for which the institution is responsible.

The European Data Protection Supervisor will ensure that his authorising officer by delegation continues his efforts to guarantee that the reasonable assurance given in the statement attached to his activities report is effectively backed up by appropriate internal control systems.

²² Financial Regulation, Article 74(9): The authorising officer by delegation shall report to his or her Union institution on the performance of his or her duties in the form of an annual activity report containing financial and management information, including the results of controls, declaring that, except as otherwise specified in any reservations related to defined areas of revenue and expenditure, he or she has reasonable assurance that:

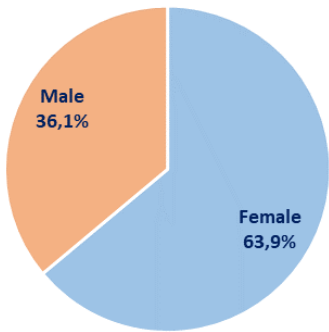
- (a) the information contained in the report presents a true and fair view;
- (b) the resources assigned to the activities described in the report have been used for their intended purpose and in accordance with the principle of sound financial management; and
- (c) the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

The annual activity report shall include information on the operations carried out, by reference to the objectives and performance considerations set in the strategic plans, the risks associated with those operations, the use made of the resources provided and the efficiency and effectiveness of internal control systems. The report shall include an overall assessment of the costs and benefits of controls and information on the extent to which the operational expenditure authorised contributes to the achievement of strategic objectives of the Union and generates EU added value. The Commission shall prepare a summary of the annual activity reports for the preceding year.

The annual activity reports for the financial year of the authorising officers and, where applicable, authorising officers by delegation of Union institutions, Union bodies, European offices and agencies shall be published by 1 July of the following financial year on the website of the respective Union institution, Union body, European office or agency in an easily accessible way, subject to duly justified confidentiality and security considerations.

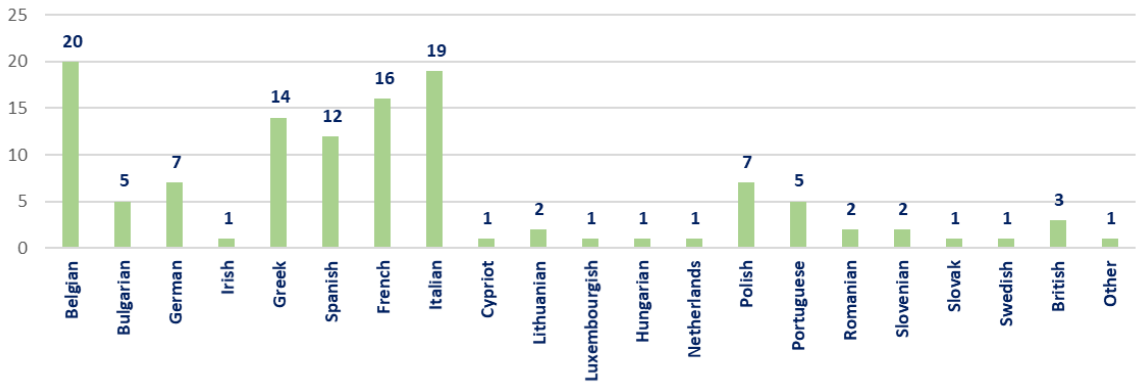
Annex 2: Human resources at the EDPS

Staff members per gender



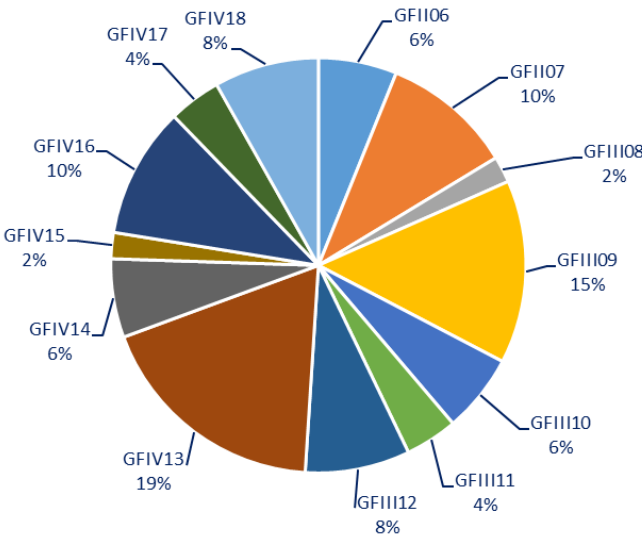
Data on 31/12/2021

Staff Members per nationality

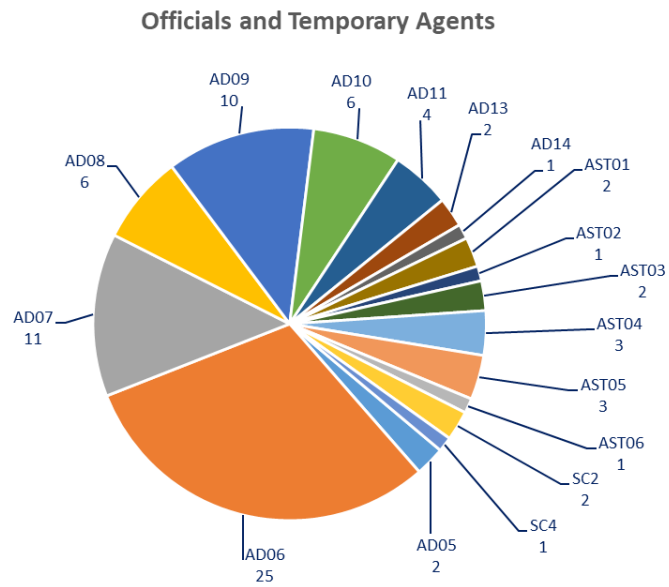


Data on 31/12/2021

Contract Agents



Data on 31/12/2021



Data on 31/12/2021

Annex 3: Budget 2021

TITLE 1 - EXPENDITURE RELATING TO PERSONS WORKING WITH THE INSTITUTION		2020 (after transfers)	Execution 2020	2021 (after transfers)	2021 vs 2020	2021 vs 2020 (%)	execution 2021 (%)
Chapter 10	Members of the institution						
Article 100	Remuneration, allowances and other entitlements of Members						
	Item 1000 Remuneration and allowances	432,047.00	80.88%	416,168.00	-15,879.00	-3.68%	96.50%
	Item 1001 Entitlements on entering and leaving the service	2,647.00	100.00%	0.00	-2,647.00	-100.00%	
	Item 1002 Temporary allowances	331,925.00	0.00%	0.00	-331,925.00	-100.00%	
	Item 1003 Pensions	0.00		0.00	0.00		
	Item 1004 Provisional appropriation	0.00		0.00	0.00		
	TOTAL Article 100	766,619.00	45.93%	416,168.00	-350,451.00	-45.71%	96.50%
Article 101	Other expenditure in connection with Members						
	Item 1010 Further training	25,000.00	0.00%	15,000.00	-10,000.00	-40.00%	8.07%
	Item 1011 Mission expenses, travel expenses and other ancillary expenditure	59,394.00	12.09%	33,000.00	-26,394.00	-44.44%	15.15%
	TOTAL Article 101	84,394.00	8.51%	48,000.00	-36,394.00	-43.12%	12.94%
	TOTAL Chapter 10	851,013.00	42.21%	464,168.00	-386,845.00	-45.46%	87.86%
Chapter 11	Staff of the institution						
Article 110	Remuneration, allowances and other entitlements of officials and temporary staff						
	Item 1100 Remuneration and allowances	6,720,765.00	81.76%	6,405,000.00	-315,765.00	-4.70%	93.46%
	Item 1101 Entitlements on entering, leaving the service and on transfer	50,000.00	81.39%	110,000.00	60,000.00	120.00%	94.80%
	Item 1102 Overtime	0.00		0.00	0.00		
	Item 1103 Special assistance grants	0.00		0.00	0.00		
	Item 1104 Allowances and miscellaneous contributions in connection with early termination of service	0.00		0.00	0.00		
	Item 1105 Provisional appropriation	0.00		0.00	0.00		
	TOTAL Article 110	6,770,765.00	97.14%	6,515,000.00	-255,765.00	-3.78%	93.48%
Article 111	Other staff						
	Item 1110 Contract staff	1,073,815.00	99.93%	1,444,000.00	370,185.00	34.47%	98.39%
	Item 1111 Cost of traineeships and staff exchanges	285,440.00	83.41%	207,111.00	-78,329.00	-27.44%	94.09%
	Item 1112 Services and work to be contracted out	52,748.00	78.12%	54,889.00	2,141.00	4.06%	100.00%
	TOTAL Article 111	1,412,003.00	95.77%	1,706,000.00	293,997.00	20.82%	97.92%
Article 112	Other expenditure in connection with staff						
	Item 1120 Mission expenses, travel expenses and other ancillary expenditure	105,000.00	15.75%	72,500.00	-32,500.00	-30.95%	45.14%
	Item 1121 Recruitment costs	6,789.00	82.25%	6,789.00	0.00	0.00%	50.41%
	Item 1122 Further training	80,000.00	67.07%	83,000.00	3,000.00	3.75%	51.55%
	Item 1123 Social service	0.00		0.00	0.00		
	Item 1124 Medical service	14,844.00	100.00%	21,000.00	6,156.00	41.47%	100.00%
	Item 1125 Union nursery centre and other day nurseries and after-school centres	108,577.75	100.00%	83,000.00	-25,577.75	-23.56%	100.00%
	Item 1126 Relations between staff and other welfare expenditure	9,422.25	100.00%	88,000.00	78,577.75	833.96%	97.66%
	TOTAL Article 112	324,633.00	64.26%	354,289.00	29,656.00	9.14%	75.89%
	TOTAL Chapter 11	8,507,401.00	83.41%	8,575,289.00	67,888.00	0.80%	91.64%
	TOTAL TITLE 1	9,358,414.00	79.67%	9,039,457.00	-318,957.00	-3.41%	91.44%

TITLE 2 - BUILDINGS, EQUIPMENT AND EXPENDITURE IN CONNECTION WITH THE OPERATION OF THE INSTITUTION		2020 (after transfers)	Execution 2020	2021 (after transfers)	2021 vs 2020	2021 vs 2020 (%)	execution 2021 (%)
Chapter 20	Buildings, equipment and expenditure in connection with the operation of the institution						
Article 200	Rents, charges and buildings expenditure	2,192,454.00	68.51%	1,239,899.00	-952,555.00	-43.45%	98.68%
	TOTAL Article 200	2,192,454.00	68.51%	1,239,899.00	-952,555.00	-43.45%	98.68%
Article 201	Expenditure in connection with the operation and activities of the institution						
	Item 2010 Information technology equipment and services	543,559.00	96.58%	1,007,237.00	463,678.00	85.30%	63.89%
	Item 2011 Furnitures, office supplies and telecommunication costs	15,000.00	25.90%	38,000.00	23,000.00	153.33%	47.41%
	Item 2012 Other operating expenditure	313,490.00	96.37%	252,000.00	-61,490.00	-19.61%	88.49%
	Item 2013 Translation and interpretation costs	546,510.00	62.63%	509,000.00	-37,510.00	-6.86%	100.00%
	Item 2014 Expenditure on publishing and information	158,000.00	70.28%	102,500.00	-55,500.00	-35.13%	58.71%
	Item 2015 Expenditure in connection with the activities of the institution	144,000.00	46.85%	184,000.00	40,000.00	27.78%	43.92%
	Item 2016 Experts reimbursements	80,000.00	22.10%	50,000.00	-30,000.00	-37.50%	13.22%
	TOTAL Article 201	1,800,559.00	76.06%	2,142,737.00	342,178.00	19.00%	71.92%
	TOTAL CHAPTER 20	3,993,013.00	89.86%	3,382,636.00	-610,377.00	-15.29%	81.73%
	TOTAL TITLE 2	3,993,013.00	89.86%	3,382,636.00	-610,377.00	-15.29%	81.73%

TITLE 3 - EUROPEAN DATA PROTECTION BOARD (EDPB)		2020 (after transfers)	Execution 2020	2021 (after transfers)	2021 vs 2020	2021 vs 2020 (%)	execution 2021 (%)
Article 300 Rents, charges and buildings expenditure							
Item 3000 Rents, charges and buildings expenditure		0.00	0.00%	626,000.00	626,000.00		77.36%
TOTAL Article 300		0.00	0.00%	626,000.00	626,000.00		77.36%
Article 301 Remuneration, allowances and other entitlements of officials and temporary staff							
Item 3010 Remuneration and allowances		1,419,410.28	79.74%	1,446,000.00	26,589.72	1.87%	93.91%
Item 3011 Entitlements on entering, leaving the service and on transfer		61,361.72	100.00%	25,000.00	-36,361.72	-59.26%	84.94%
Item 3012 Allowances and miscellaneous contributions in connection with early termination of service							
TOTAL Article 301		1,480,772.00	80.58%	1,471,000.00	-9,772.00	-0.66%	93.76%
Article 302 Other staff							
Item 3020 Contract staff		811,788.00	94.98%	1,150,000.00	338,212.00	41.66%	93.30%
Item 3021 Cost of traineeships and staff exchanges		88,615.00	64.59%	90,000.00	1,385.00	1.56%	83.75%
Item 3022 Services and work to be contracted out		67,748.00	80.50%	64,000.00	-3,748.00	-5.53%	89.51%
TOTAL Article 302		968,151.00	91.18%	1,304,000.00	335,849.00	34.69%	92.45%
Article 303 Other expenditure in connection with staff of the Board							
Item 3030 Mission expenses, travel expenses and other ancillary expenditure		35,700.00	41.43%	45,000.00	9,300.00	26.05%	4.29%
Item 3031 Recruitment costs		6,000.00	49.36%	3,000.00	-3,000.00	-50.00%	98.13%
Item 3032 Further training		25,000.00	28.21%	30,000.00	5,000.00	20.00%	50.39%
Item 3033 Medical service		4,000.00	99.20%	4,000.00	0.00	0.00%	100.00%
Item 3034 Union nursery centre and other day nurseries and after-school centres		32,000.00	0.00%	32,000.00	0.00	0.00%	0.00%
TOTAL Article 303		102,700.00	28.01%	114,000.00	11,300.00	11.00%	21.04%
Article 304 Expenditure in connection with the operation and activities of the Board							
Item 3040 EDPB plenaries and sub-group meetings		858,500.00	13.33%	526,000.00	-332,500.00	-38.73%	7.24%
Item 3041 Translation and interpretation costs		1,599,436.00	54.32%	1,564,000.00	-35,436.00	-2.22%	84.04%
Item 3042 Expenditure on publishing and information		92,500.00	77.30%	130,000.00	37,500.00	40.54%	45.25%
Item 3043 Information technology equipment and services		677,500.00	70.20%	754,000.00	76,500.00	11.29%	86.80%
Item 3044 Furnitures, office supplies and telecommunication costs		20,000.00	51.29%	15,000.00	-5,000.00	-25.00%	9.01%
Item 3045 External consultancy and studies		177,600.00	42.31%	342,000.00	164,400.00	92.57%	98.85%
Item 3046 Other expenditure in connection with the activities of the EDPB		148,412.00	17.09%	65,000.00	-83,412.00	-56.20%	3.10%
Item 3047 Other operating expenditure				77,000.00	77,000.00		68.20%
Item 3048 EDPB Chair and Vice chairs expenses				53,100.00	53,100.00		12.31%
TOTAL Article 304		3,573,948.00	45.92%	3,526,100.00	-47,848.00	-1.34%	69.94%
TOTAL CHAPTER 30		6,125,571.00	61.15%	7,041,100.00	915,529.00	14.95%	78.95%
TOTAL TITLE 3		6,125,571.00	61.15%	7,041,100.00	915,529.00	14.95%	78.95%
TOTAL BUDGET		19,476,998.00	72.25%	19,463,193.00	-13,805.00	-0.07%	86.12%

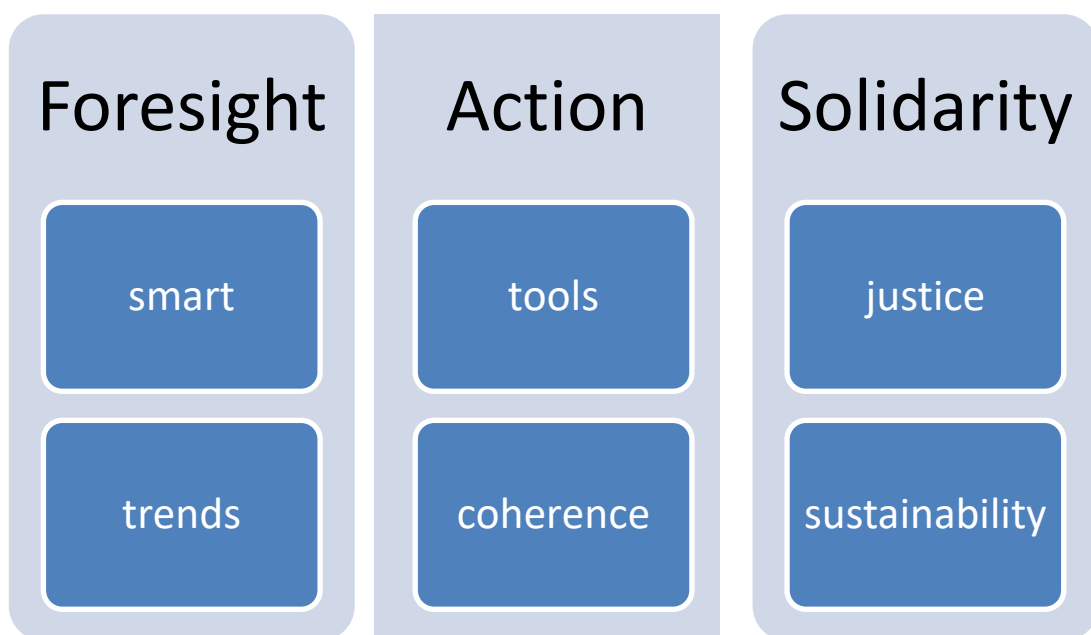
Annex 4: Detailed list of missions undertaken by the Supervisor (2021)

Wojciech Rafal WIEWIOROWSKI - 2021			
Mission Purpose	Date from	Date to	Cost €
43rd GPA - International conference - Mexico	18/10/2021	21/10/2021	23.75
Meeting at the Hague Europol	03/09/21	03/09/21	0 Cancelled
Meeting in Luxembourg EPPO, ECA CJEU Event in Warsaw, a lecture 22_23 September Event in Venice ASPEN	20/09/2021	25/09/2021	1553.97
Hearing - Public defence of Teresa Quintel's dissertation at Luxembourg	10/09/21	10/09/21	196.74
Mexico GPA virtual mission	18/10/2021	21/10/2021	0
Maastricht (NLD) Advanced Master in Privacy, Cybersecurity, Data Management and Leadership	11/10/21	11/10/21	54.08
Maastricht (NLD) Advanced Master in Privacy, Cybersecurity, Data Management and Leadership	15/10/21	15/10/21	54.08
Visit to the Spanish DPA, and event at the University (Madrid) Interview with El Pais	02/12/21	03/12/21	792.74

Annex 5: EDPS strategic objectives

The EDPS strategy describes how it intends to carry out its statutory functions and deploy the resources available to address these challenges. There are three pillars to the strategy, each reflecting its values.

- **Foresight:** the EDPS commitment to being a **smart** institution that takes the long-term view of **trends** in data protection and the legal, societal and technological context.
- **Action:** proactively develop **tools** for EUI to be world leaders in data protection. To promote **coherence** in the activities of enforcement bodies in the EU with a stronger expression of genuine European solidarity, burden sharing and common approach.
- **Solidarity:** the EDPS belief is that **justice** requires privacy to be safeguarded for everyone, in all EU policies, while **sustainability** should be the driver for data processing in the public interest.



Annex 6: EDPS strategic objectives and its Action Plan

Our objectives: what we aim to achieve by the end of 2024

The strategic objectives under the three pillars express what we intend to achieve by 2024. A number of strategic initiatives will support the achievement of those objectives. We will take more actions than can be described in this strategy; all of these will appear in our Annual Management Plan for each year of this mandate. This strategy is a live, iterative document. It will be kept under regular review as a reference point for our staff and stakeholders.

Foresight

EDPS to be a recognised and respected centre of expertise that helps understand the impact of the design, evolution, risks and deployment of digital technology on the fundamental rights to privacy and data protection.

1.1 Smart

We want to be a smart administration in a smart EUI environment

Knowledge is an essential asset for the EDPS to effectively support strategic objectives. However, we do not want to be a centre of excellence in a way that does not benefit the outside world. We want to share knowledge, expertise and contribute to the smart administration of the EUI environment.

Our aim is to use the best expertise and latest sustainable technology, to look after our people, promote diversity in all its forms, as well as being transparent and inclusive towards our stakeholders.

Hence, this part of the strategy is dedicated to outline the specific actions for this mandate.

To this extent, we will:

- Carefully monitor jurisprudence, pursue our interventions in cases before the Court of Justice of the European Union (CJEU).
- Make an inventory of the measures introduced by EUI during the Covid-19 crisis. Distinguishing those that have naturally developed from the measures that were only accelerated due to extraordinary circumstances. The latter should be recognised as temporary and discarded when the crisis is over.
- Plan a simple and short online training module for all new EUI staff and propose that this becomes compulsory. We will equip [Data Protection Officers \(DPOs\)](#) with the tools they need and help build a ‘satellite’ network of data protection experts.
- Organise evidence-based discussions on intrusive, emerging or hypothetical practices, such as eHealth, biometric technologies and automatic recognition systems, quantum computing, edge computing and blockchain.

- Engage with experts from the public health community in the EU and other international organisations, to better understand the needs for epidemiological surveillance and accurately measure the efficiency and purpose of the tools being developed with regard to personal data protection (e.g. by developing together practical guidance on data protection by design).
- Continue to facilitate discussions between data protection experts, regulators and the research community, including ethics boards, to ensure that data protection enhances the efforts of genuine scientific research.
- Collaborate more closely with academia and independent researchers by setting up a research visitor programme, hosting events and supporting summer academies in close cooperation with the EDPB and other DPAs. We will encourage and facilitate more exchanges between our staff and DPAs and between DPAs themselves.
- Publish case law digests concerning data protection and privacy at EU level.
- Keep exchanging information and best practices with international organisations and interlocutors in third countries.
- To study and prioritise the impacts of data processing practices on individuals and groups, especially those in vulnerable situations, such as refugees and children.
- Invest in knowledge management to ensure the highest quality of our work and to recruit a diverse, inter-disciplinary and talented workforce.

1.2 Trends

We want to know what is going on and what is going to happen

The EDPS places strategic importance on integrating the technological dimension of data protection into our work. As a data protection supervisory authority, we must closely examine both the potential risks and opportunities offered by these advances, understand the possibilities of new technologies and, at the same time, encourage the integration of data protection by design and data protection by default in the innovation process.

We aim to explain in a simple way the interaction between these trends, and to include data protection in the new EU skills agenda. In our work with the EDPB, as well as an advisor to the EUI, we focus on areas where the interests of data protection interacts with technology and other areas of law, including competition law, consumer law, finance and payment services.

The EDPS is uniquely positioned to monitor developments in the [Areas of Freedom, Security and Justice \(AFSJ\)](#). This is particularly emphasised through our role as supervisory authority of Europol, Eurojust, EPPO, Frontex, EASO²³ or eu-LISA²⁴.

²³ EASO : European Asylum Support Office

²⁴ The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

- We will actively follow the evolution of data processing practices and technology that may have an impact on privacy and data protection. We will continue to issue reports on emerging technology issues. Moreover, we will promote the understanding of what is the 'state of the art' of a specific technology, such as anonymisation, encryption, and network security.
- Where the European Commission proposes measures with data protection implications, we will continue to provide legal advice regarding compliance with the EU Charter and the principles of data protection set out in applicable legislation.
- We will focus on the potential impact of technology-driven policy, as recently demonstrated in our [opinions](#) on the European Commission's "White paper on Artificial Intelligence: A European approach to excellence and trust", and the European Commission's Communication on "A European strategy for data".
- Where EUI intend to deploy new technologies, we will systematically request them to clearly explain the impact of these technologies and their risks on individuals and groups.
- We will alert EUI and the public when digital technology is deployed in a way that does not respect the essence of the fundamental rights of personal data protection, privacy and other rights and freedoms enshrined in the EU Charter of Fundamental Rights.
- We strive to do this in close collaboration with the European Commission, other EUI and agencies active in related areas, such as the Fundamental Rights Agency (FRA) or the European Agency for Cybersecurity (ENISA), via updated Memoranda of Understanding (MoU).
- We will build on existing initiatives such as the [Internet Privacy Engineering Network \(IPEN\)](#) and consolidate the network for technology expertise among data protection authorities in Europe. We aim to develop core knowledge on how essential and emerging technologies work. This will include talking to innovators in the private sector.
- We will invest special attention to the development of eHealth services at EU level.
- We will develop a consistent and targeted communications strategy with various stakeholders to address the COVID-19 pandemic's newest developments and data protection issues. In 2022, we will host a conference on how to safeguard individuals' rights in a world that will, hopefully, be recovering from this current crisis.

Action

EDPS to support EUI to continue to lead by example in safeguarding digital rights and responsible data processing.

2.1 Tools

We are going to use the tools we have and develop new ones

Privacy and data protection are cornerstones in any democratic society based on the rule of law and fundamental rights. Likewise, a free internet society depends on the design of technology. This is particularly relevant whenever the EU adopts laws and policies related to the processing of personal data, or when EUI process personal data.

Personal data have and will continue to play an important role in the fight against the COVID-19 pandemic. Our laws, such as the GDPR and the ePrivacy rules, allow for the processing of personal data for public health purposes, including in times of emergency. Data protection law is well-equipped to help support the public good, and do not represent an obstacle, in fighting the virus. It is certainly possible to build technological solutions, which are compliant with the legal data protection framework. Some recent application show that societies can take up technologies while upholding privacy and data protection rights. It remains paramount that EUI and Member States continue to actively engage with DPAs.

Certain processing activities are however, by their nature, highly risky, they may even violate the essence of fundamental rights and freedoms and should be suspended or stopped altogether, i.e. when broad internet content monitoring interferes with privacy and freedom online. Being a supervisory authority, we must be equipped to monitor and anticipate problems and quickly respond to operational situations, policy and legal questions. We recognise DPOs of EUI as the emissaries of positive change in how data is handled.

The outsourcing of tasks by EUI to providers of communications services and digital tools is an operational reality, and often a necessity. This, however, creates risks for data protection and good administration, particularly where there are few or no viable alternatives to monopoly providers with questionable standards on privacy and transparency.

The EU and European public administrations have considerable leverage to bring about real change to business models which are not consistent with EU values, fundamental rights and data protection rules. This was particularly relevant when an enforcement action was launched in 2019 concerning EUI contracts with software providers. There is now a renewed appetite for coordinated support to the European industry and for data to be processed according to our European values.

In this sense, our commitments are as follows, we will:

- Promote data protection by design and by default, to be implemented irrespective of the technology deployed or the political priorities.
- Develop effective oversight mechanisms, particularly on technologies and tools, when these are deployed in the common fight against COVID-19, to empower and not control, repress or stigmatise citizens.
- Contribute to developing strong oversight, audit and assessment capabilities for technologies and tools, which are increasingly “endemic” to our digital ecosystem

(e.g., profiling, machine learning, AI). We will provide guidance on personal data processing using automated decision-making systems and AI.

- Support the idea of a moratorium on the deployment, in the EU, of automated recognition in public spaces of human features, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, so that an informed and democratic debate can take place.
- Reinforce the central role of the controller in relation to [processors](#) and sub-processors in EUI, both by raising awareness and, more formally, by providing advice on possible standard contractual clauses.
- Aim to minimise our reliance on monopoly providers of communications and software services, to avoid detrimental lock-in and work with other EUI and other public administrations in the EU so they can do the same. We will call on EUI and other public administrations in the EU to review their external contracts on digital products, software, services and technology to achieve compliance as required by EU data protection laws. We will explore how to deploy free and open source software and solutions.
- Review previous authorisations for transfers to third countries and adopt standard data protection clauses.
- Continuously assist EUI by demonstrating and developing bespoke privacy tools and solutions. This also involves giving advice when [Data Protection Impact Assessments \(DPIAs\)](#) are necessary.
- Publish standardised information about personal data breaches that are notified to us, including the types of organisations involved and the number of people affected.
- Use our enforcement powers to ensure EUI websites and mobile apps are complying with EU law, particularly in respect of third party tracking.
- Closely monitor the ongoing process that makes EU systems ‘interoperable’, with a particular focus on the access and processing of personal data (Europol, Frontex et al.), in collaboration with national supervisory authorities where needed, to ensure effective supervision.
- Launch, explore and explain, as a follow up to the ‘[Necessity Toolkit](#)’ and ‘Guidelines on [Proportionality](#)’, the concept of the ‘essence’ of the rights to privacy and data protection, based on the jurisprudence of the Court of Justice and growing scholarship in this area.

2.2 Coherence

We do not protect data - we protect human beings

The GDPR is directly applicable throughout the EU. Nevertheless, it provides Member States with the possibility to further legislate their respective laws. This could compound the fragmentation of national approaches. The EDPB exists to check and avoid such fragmentation.

The EDPS has a unique dual role as a full member and provider of the EDPB's secretariat. We will exercise this role creatively, seeking to represent the wider EU interest, and contribute to the success of the EDPB, as well as ensuring the consistent application and enforcement of the GDPR and [the Data Protection Law Enforcement Directive](#). We aim to develop with other DPAs a common set of tools.

The EU has not completed its updating of the data protection framework for the digital age. EU legal gaps remain, where specific data protection rules are either absent – for the processing of personal data by the Common Foreign and Security Policy (CFSP) mission as referred to in [Articles 42\(1\), 43 and 44 TEU](#), or fragmented police and judicial cooperation in criminal matters, as well as Europol and EPPO. Such a situation undermines the possibility of achieving a consistent approach to protecting individual's personal data in the EU. We will interpret the applicable rules in the spirit of the GDPR, and we will apply the principles of the Regulation in areas where specific rules are missing.

We need up-to-date - but also technologically neutral - rules on the protection of [confidentiality](#) of electronic communications. Sustainable economic growth cannot be achieved through the infinite monetisation of people's private conversations or indiscriminate retention of all communications data.

Personal data supports privacy, as well as other rights and freedoms, such as freedom of expression and non-discrimination. We recognise the synergies between the enforcement of data protection and other rules applicable to the digital economy, especially concerning consumer and competition law, and will carry on our work to ensure that they are mutually reinforced.

EUI are already making use of new and emerging technologies. In the interest of a coherent approach throughout the EU, the EDPS recommends that any new EU regulatory framework, such as potential AI, will apply both to EU Member States and to EU institutions, offices, bodies and agencies.

Data protection and privacy are the foundations for democracy in a time of digitisation. To this end, we will:

- Continue to build the capacity of the EDPB, both as a member and as a provider of its secretariat, to ensure that, by 2025, the GDPR is recognised as a model for all democracies around the world - a formidable blueprint to strengthen the trust and respect in the digital society.
- Call for a stronger expression of genuine European solidarity, burden sharing and common approach to ensure the enforcement of our data protection rules. The EDPS supports the establishment of a Support Pool of Experts within the EDPB, which would assist DPAs dealing with resource-heavy and complex cases.
- Contribute to the review of Regulation (EU) 2018/1725, scheduled for April 2022, and make a strong case to address the gaps and discrepancies that continue to exist. In the meantime, the EDPS will interpret any specific rules in the spirit of Regulation (EU) 2018/1725.
- Closely monitor the use of new tools involving data analytics and artificial intelligence by Europol and other agencies in the AFSJ, in compliance with the

mandate assigned to them by law, while promoting solutions to protect individuals' rights and freedoms.

- Call for a coherent approach regarding new EU regulatory frameworks on the use of new technologies so that EUI are subject to the same rules as those applied in EU Member States.
- Supervise EPPO as new actor in the criminal justice area, and especially its relations with Europol and Eurojust.
- Call for the adoption of the proposed ePrivacy Regulation, but not to the detriment of existing protections.
- Contribute to the establishment of the Digital Single Market where European rules on privacy and data protection, as well as competition law, are fully respected. We will also make sure that the rules on the access and use of data are fair, practical and clear.
- Develop European and international cooperation measures, and promote joint enforcement actions and active mutual assistance, by concluding - when necessary - Memoranda of Understanding with DPAs.

Solidarity

The EDPS promotes a positive vision of digitisation that enables us to value and respect all individuals. The full potential of data shall be dedicated to the good of society and with respect to human rights, dignity and the rule of law.

3.1 Justice

We actively promote justice and the rule of law.

Solidarity, being aware of shared values, interests and objectives, is at the heart of the EU project. As an EU institution, the EDPS is committed to upholding the rule of law and democracy. As an independent data protection supervisory authority, we act in line with these values. When we believe that these are threatened, we speak up, and vigorously defend them. Likewise, we take action if the independence of other DPAs and the 'collective independence' of the EDPB are jeopardised.

When planning strategies on democracy and human rights, the EU should promote digital justice and privacy for all. Privacy and data protection can never be traded for access to essential services. Data protection is one of the last lines of defence for vulnerable individuals, such as migrants and asylum seekers approaching EU external borders. Although the EU has accumulated a patchwork of measures in the areas of police and judicial cooperation and border management, the legal framework remains fragmented, creating unnecessary discrepancies. This puts unwarranted constraints on the EDPS' supervisory and enforcement powers.

Fundamental rights are necessary because they protect those less likely to have the means to fully defend themselves. In the so-called gig economy, workers and consumers

find themselves governed by algorithms that make decisions based on data collected about them, with limited ability to understand or challenge those decisions. Women, people of colour and those with disabilities are routinely discriminated against, and this is reinforced by the proliferation of algorithmic decision-making.

We recognise the need for individuals to have greater control over whether data about them is collected, and, if so, how and for what purpose their personal data is processed. Where the digital environment becomes more complex, responsibility falls on controllers and enforcers to avoid any data practices that harm the rights or interests of the individuals concerned. The burden of proof should not fall on those individuals to understand risks and take action.

In complex scenarios, '[consent](#)' should not be relied upon because it indicates obvious power imbalances between the controller and the individual's rights to data protection. We are convinced that EU data protection legislation provides other lawful grounds for processing.

A misguided debate continues on the appropriateness of the concept of personal 'data ownership'. This is unlikely to be compatible with the Charter of Fundamental Rights and will not empower individuals in a digitised society. We believe data protection 'disrupts' the markets for personal data, where data as a commercial or political asset is monetised or used to manipulate people. DPAs acting collectively should be an agent for such positive changes.

In this context, we will actively:

- Stress that privacy and data protection are an integral part of the rule of law and can never be treated in isolation. We will take actions if the independence of other DPAs or the 'collective independence' of the EDPB are jeopardised.
- Advocate for the fundamental rights to data protection and privacy to be at the heart of the Conference on the Future of Europe. We will also support the efforts to integrate data protection considerations in the [European Democracy Action Plan](#), as a safeguard for independent journalism, lawful dissent and political activism.
- Continue to enforce EUI compliance with the rules, to protect those who are in a position of weakness, such as minors or displaced persons near or at the EU's external border. Indeed, they have as much of a right to data protection and privacy as anyone else.
- Identify discrepancies in the standards of data protection within EU law in the Areas of Freedom, Security and Justice (AFSJ) and we will consistently enforce the rules.
- Encourage the European Commission to further harmonise the data protection rules on processing operational data (Chapter IX of the Regulation 2018/1725), including in the context of the [Europol Regulation](#) review.
- Advise EU lawmakers to safeguard data protection and privacy in [the New Pact on Migration and Asylum](#).

- Keep contributing to the European Commission's proposals related to combatting discrimination.
- Provide guidance to EUI on policies and measures (such as the [Digital Services Act](#)) that hold private companies accountable for manipulation and amplification serving private gain, but to avoid blanket monitoring and censorship of speech that inevitably interferes with the rights to privacy and data protection.
- Building on our experience with the [Digital Clearinghouse](#) and other fora, we will work with the EDPB, the European Commission and the relevant EUI to establish practical cooperation and joint enforcement between digital regulators on specific cases and learn lessons from the past.
- Actively contribute to the development of a common EU vision on digitisation and technology. For example, determining how AI can be used for humankind and re-engineered along the lines of EU rights and values and alongside strict liability rules; so that manufacturers and controllers are held responsible for damage caused by defects in their products, even if the defect resulted from autonomous decisions after its entry on the market. In the interest of a coherent approach throughout the EU, the EDPS recommends that any new regulatory framework should apply to both EU Member States and EUI. Where EUI use AI, they should be subject to the same rules as those applied in EU Member States.
- Regularly engage in the debate on digital ethics, emphasising the need to not only comply with the law, but to also consider the effects of data processing by controllers in EUI and elsewhere, on individuals, groups and society; including shared values and the environment.
- Promote diversity in all discussions on data protection, including those we organise ourselves. We will ensure gender balanced representation among speakers and panellists in the conferences or events we organise.

3.2 Sustainability

We know there is only one world

Data processing and data protection have to go green.

The EDPS is a socially-responsible organisation. Our values are to treat people – our employees, the people whose activities we supervise, the individuals whose data is processed by EUI, our stakeholders - and the natural environment around us, with respect.

The ongoing development of AI and blockchain based technologies, as well as illegal tracking and profiling of individuals generate an increasing amount of dangerous waste, due to short-lived connected goods, combined with exponential carbon footprint emissions. This is a great source of concern in light of the [EU Green Deal](#) and data protection in this new decade.

Enforcing personal [data minimization](#) and responsible data processing can be part of the solution to help counteract these damaging trends. There should be competition on the most beneficial ways to use data, not on who can collect the most.

The redistribution of wealth and its practical application are bound to change with the continuous evolution of social norms, politics, and culture. As highlighted by [the EDPS' Preliminary Opinion](#) on scientific research and data protection, there is growing concern about how digitisation has contributed to the exponential growth in data generation; while also concentrating the control of the means for converting that data into valuable knowledge in the hands of a few powerful private companies. There are growing calls for regulated access across the EU to privately-held personal data for research purposes exclusively serving the public interest to improve health care, advance health research and address the climate crisis or growing social inequalities. While the [Open Data Directive](#) organises the access to public sector information to foster competition and economic innovation; access to privately held data by non-profit stakeholders to foster social and solidarity innovation and scientific research in the public interest deserves specific attention as well. Current barriers to such access reveals the need for a broader debate on a data redistribution policy for the digital age, to maximise societal benefits of data sharing initiatives, in compliance with the European fundamental rights framework. To address these challenges, we will:

- Convey a deeper understanding of the impact of digitisation on our world.
- Encourage broader and long-term view of the future of data protection in a period of environmental crisis, growing inequalities and geopolitical tensions.
- Pay particular attention to our energy consumption, emissions due to the travelling of officials (missions), procurement and commuting to and from work, promoting telework.
- Engage in the debate on data sharing to advocate for a data redistribution policy for the digital age based on a rigorous proportionality tests and appropriate safeguards - including anonymisation and pseudonymisation - against misuse and unlawful access.