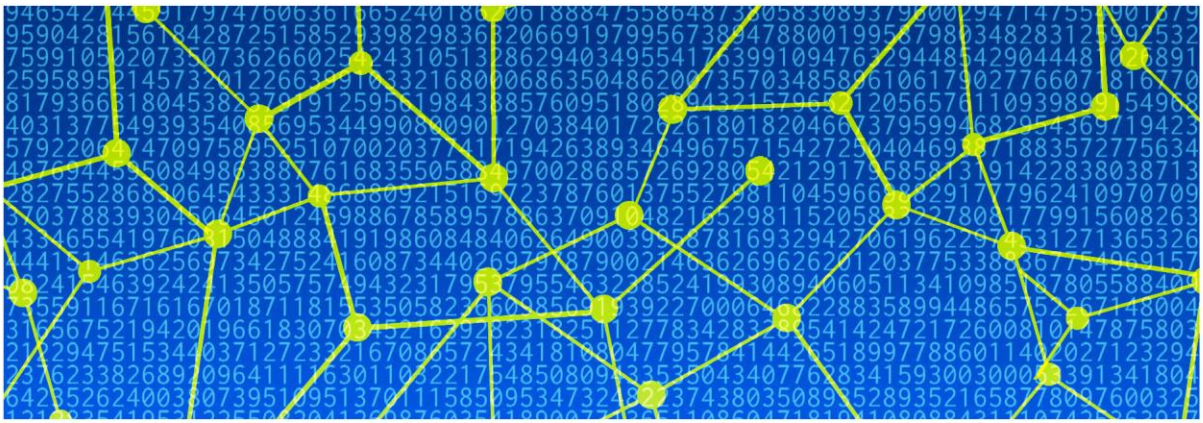

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 5/2017

Upgrading data protection rules for EU institutions and bodies

EDPS Opinion on the proposal for a Regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

EDPS

15 March 2017

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion expresses the ongoing commitment of the EDPS committed to work with the European Parliament, Council and Commission to ensure that current rules set out in Regulation 45/2001 are brought into line with the General Data Protection Regulation and that a revised framework becomes applicable as the same time as the GDPR in May 2018 at the latest.

Executive Summary

A new generation of data protection standards is being promulgated by the European Union. The adoption almost one year ago of the General Data Protection Regulation and the Directive for the police and justice sectors represented the most ambitious endeavour of the EU legislator so far to secure the fundamental rights of the individual in the digital era. Now is the time for EU institutions themselves to lead by example in the rules that they apply to themselves as data controllers and data processors. Over the past 18 months the EDPS has initiated dialogue with EU institutions at the highest level to prepare them for the new challenges on data protection compliance, emphasising the new principle of accountability for how data is processed. With this Opinion the EDPS aims to bring twelve years' experience of independent supervision, policy advice and advocacy in suggesting improvements to the proposed Regulation on personal data processing by EU institutions and bodies.

Regulation 45/2001 has served as a bellweather providing directly applicable obligations for controllers, rights for data subjects and a clearly independent supervisory body. The EU now must ensure consistency with the GDPR through an emphasis on accountability and safeguards for individuals rather than procedures. Some divergence of rules applicable to EU institutions data processing is justifiable, in the same way as public sector exceptions have been included in the GDPR, but this must be kept to a minimum.

Essential however, from the perspective of the individual, is that the common principles throughout the EU data protection framework be applied consistently irrespective of who happens to be the data controller. It is also essential that the whole framework applies at the same time, that is, in May 2018, deadline for GDPR to be fully applicable.

The EDPS was consulted by the Commission on the draft proposal in line with a long-standing arrangement between our institutions. We consider that the Commission has achieved overall a good balance of the various interests at stake. This Opinion sets out a number of areas in which the proposal could be further improved. We argue for improvements to the proposed regulation, particularly regarding the restrictions to the rights of the data subject and provision for EU institutions to use certification mechanisms in certain contexts. With respect to our own tasks and powers as an independent body, the proposal appears to strike a reasonable balance and to reflect the normal functions of an independent Data Protection Authority under the Charter of Fundamental Rights and as reaffirmed in recent case law of the Court of Justice, whether as enforcer, complaints handler and adviser to the legislator on policies affecting data protection and privacy.

We encourage the EU legislator to reach agreement on the proposal as swiftly as possible so as to allow EU institutions to benefit from a reasonable transition period before the new Regulation can become applicable.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty of the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[2],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[3], and in particular Articles 28(2), 41(2) and 46(d) thereof,

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[4], and to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[5],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1.1 Context

1. On 10 January 2017, the European Commission adopted a Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC[6] ("the Proposal").

2. The fundamental right to the protection of personal data is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union ("the Charter") and Article 16 of the Treaty on the Functioning of the European Union ("the TFEU").

3. The European Data Protection Supervisor ("EDPS") is the independent supervision authority responsible for ensuring that European institutions, bodies, offices and agencies ("EU institutions") comply with data protection law when processing personal data[7]. The requirement to provide for independent control in the EU data protection system is enshrined in primary law, in both Article 16(2) TFEU and Article 8(3) of the Charter. The Court of Justice has consistently emphasised that control by an independent authority is an essential component of the right to data protection and laid down the criteria for such independence[8]. In particular, the supervisory authority must act with complete

independence, which implies a decision-making power independent of any direct or indirect external influence[9] and freedom from any suspicion of partiality[10].

4. The main legal instrument applicable to the processing of personal data by EU institutions is Regulation (EC) No 45/2001[11] ("Regulation 45/2001"), complemented by Decision No 1247/2002/EC[12].

5. Following the conclusion on 27 April 2016 of the protracted negotiations on the new EU data protection framework -the General Data Protection Regulation ("the GDPR") and the Directive for the police and justice sectors- this Proposal (alongside the Commission proposal for a Regulation on Privacy and Electronic Communications ("ePrivacy Regulation"[13]) marks the beginning of a crucial phase in the process of completing this EU data protection framework. It aims to align the provisions of Regulation 45/2001 with the rules laid down in the GDPR in order to create a stronger and more coherent data protection framework in the Union and to enable both instruments to be applicable at the same time[14]. In addition, the Proposal also incorporates the new rules for the protection of terminal equipment of end-users, laid down in the Commission proposal for the new ePrivacy Regulation.

6. In the Strategy 2015-2019, the EDPS committed to working with the European Parliament, Council and Commission to ensure that current rules set out in Regulation 45/2001 are brought into line with the GDPR and that a revised framework enters into force by the beginning of 2018 at the latest. The EDPS welcomes that he has been consulted informally by the Commission before the adoption of the Proposal and that the proposal seems to have taken account of many elements raised in his informal contributions to date. He finds the current Proposal more than satisfactory from the point of view of maximum alignment with the GDPR, unless narrowly defined specificities of the EU public sector justify otherwise, and particularly appreciates the balance of the various interests at stake achieved by the Commission.

7. While this Opinion indicates a number of areas in which the proposal could be further improved, the EDPS encourages the EU legislator to reach agreement on the Proposal as swiftly as possible so as to allow EU institutions to benefit from a reasonable transition period before the new Regulation can become fully applicable.

1.2 Objectives of the Proposal and timing

8. In the past, the EDPS has recommended that the substantive rules for EU institutions be incorporated in the (then) draft GDPR[15]. The EU legislator chose another option: a separate legal instrument applicable to EU institutions aligned with and applicable at the same time as the GDPR. The EDPS supports this approach: it would be inacceptable if the European Commission and the other EU institutions were not bound by rules equivalent to those which will soon become applicable at Member State level. Moreover, it would be undesirable for the EDPS to supervise compliance of EU institutions with substantive rules which would be inferior to the rules supervised by his counterparts at national level, especially given that the EDPS will be a member of the future European Data Protection Board ("EDPB")[16].

9. The future rules applicable to personal data processing by EU institutions should therefore be aligned with the provisions of the GDPR, unless narrowly interpreted specificities of the

public sector justify otherwise. In this regard, the EDPS welcomes recital 5 to the Proposal which stressed the need for maximum alignment possible and clarifies that, "*[w]henever the provisions of this Regulation are based on the same concept as the provisions of [the GDPR], those two provisions should be interpreted homogenously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of [the GDPR]*.".

10. At the same time, alignment with the GDPR can be neither full, nor automatic. The GDPR includes numerous clauses allowing Member States to maintain or introduce specific legislation in certain areas, including for public authorities[17]. In those cases where the GDPR provides specific rules for public authorities[18] or leaves room for implementation of its provisions by Member States, the Proposal can be considered to play a role comparable to a national law "implementing" the GDPR, as for example in Article 9 "*Transmissions of personal data to recipients other than Union institutions and bodies*" or Article 66 "*Administrative fines"* of the Proposal (see section 2.8.1 below). In addition, it is important to ensure that the high level of protection currently applicable to EU institutions is maintained. Hence the need to maintain certain specificities of Regulation 45/2001, such as in Article 25 *Restrictions* (see section 2.3.1 below) and Article 44 *Designation of a Data Protection Officer* (see section 2.4.5.1 below).

11. Apart from substantive alignment with the GDPR, it is essential that the revised rules become fully applicable at the same time as the GDPR i.e. on 25 May 2018. The existing network of Data Protection Officers ("DPO") provides for an efficient channel of information sharing and cooperation. Consequently, the EDPS is confident that compliance could be achieved following a relatively short transition period, e.g. three months.

12. The principle of accountability underpinning the GDPR -as well as the present Proposal- goes beyond simple compliance with the rules and implies a culture change. To facilitate the transition, the EDPS launched an "accountability project". In this context, the EDPS was in contact over the course of 2016 and 2017 with seven key EU institutions and bodies to help prepare in due time for the GDPR application.

1.3 Scope and relationship with other legal instruments

13. The EDPS has on several occasions in the past called on the Commission to propose a robust and *comprehensive* system which would be ambitious and enhance the effectiveness and *coherence* of data protection in the EU, so as to ensure a sound environment for further development in the years to come[19]. The Commission chose a different approach and proposed a separate legal instrument for data protection in the law enforcement area[20]. A number of proposals for legal acts introducing separate "standalone" data protection regimes followed[21].

14. The EDPS acknowledges that the current, albeit fragmented, legal framework for personal data protection is the best outcome achievable today[22]. The EDPS understands that the present Proposal would continue to apply to those EU institutions which fall within the scope of Regulation 45/2001 today[23] (essentially, all former 1st and 2nd "pillar" [24] institutions, bodies, offices and agencies), but would not, as such, affect the existing or pending "standalone" regimes[25]. Such regimes will be impacted by the present proposal only if and to the extent this is explicitly provided for in the relevant legal instrument. The EDPS takes note of this approach, but suggests that this is stated more explicitly in the

preamble to the Proposal and, possibly, also in its Article 2 *Scope*. At the same time, the EDPS would stress that the fragmentation and increasing complexity of the legal framework for data processing by the various EU institutions active in the former first and third "pillars" is not a fully satisfactory outcome and may need to be addressed by the EU legislator in the medium term.

15. Regulation 45/2001 provides for measures aiming at the protection of privacy and confidentiality of communications in cases where the EU institutions are in control of the infrastructure used for communication. To this end, it includes some provisions covering parts of the regulatory scope of Directive 2002/58/EC ("ePrivacy Directive")[26], and establishes the principle that rules for the protection of fundamental rights should be applied in a consistent and harmonious way throughout the Union, referring to relevant instruments as the Directive on privacy and electronic communications[27]. The need to ensure the same level of privacy and confidentiality of communications involving EU institutions remains unchanged, and therefore the principle of consistent and harmonious application should be maintained. The EDPS therefore considers that the Proposal should ensure that the relevant rules of the GDPR and the future ePrivacy Regulation will apply to EU institutions *mutatis mutandis*. This should include both the preservation of confidentiality and privacy with respect to communication services controlled by EU institutions, as well as other principles of the future ePrivacy Regulation, such as the protection of terminal devices and other rules, e.g. regarding tracking and spam.

16. Finally, while EU data protection legislation also applies to the European Economic Area, and participating EFTA countries are obliged to establish independent supervision authorities according to the GDPR, the EFTA institutions are not subject to any specific data protection rules and supervision, even though they are exchanging personal data with EU institutions. The EDPS considers that the present Proposal might be an opportunity to address this issue.

2. ANALYSIS OF THE PROPOSAL

2.1 Chapter I - General provisions

17. The EDPS notes that Article 1 *Subject-matter and objectives* and Article 2 *Scope* are modelled according to the corresponding provisions of the current Regulation 45/2001 rather than the GDPR. As such, this does not pose fundamental problems, as the terminology used is updated in line with the GDPR, where appropriate.

18. The EDPS welcomes the fact that in Article 3 *Definitions* a reference is made to definitions in Article 4 of GDPR, with the exception of terms which reflect the specific institutional context of the Proposal, including "Union institutions and bodies" and "controller".

2.2 Chapter II - Principles

19. The EDPS takes note that the Proposal no longer includes an equivalent provision to Article 7 of Regulation 45/2001 on transfers within or between EU institutions. That provision allowed such transfers only when they were necessary for the legitimate performance of a task covered by the competence of the recipient, it defined the shared responsibility for transfers on request of the recipient and stated that transferred data shall only be used for the purpose for which they were transferred. Even though there are no specific rules for this situation in the Proposal, they follow implicitly from the principles for processing

personal data in Article 4 of the Proposal: personal data shall be processed lawfully, be limited to what is necessary and in a way that ensures protection against unauthorised of unlawful processing (including disclosure). However, considering the pedagogical effect that Article 7 of Regulation 45/2001 had[28], the EDPS would recommend the inclusion of a provision equivalent to Article 7 of Regulation 45/2001.

20. The provision of information society services to children, which would render Article 8 of the Proposal applicable, are not part of the core business of EUI. Nevertheless, given the broad scope of the Proposal and the large variety of EU institutions and their processing operations, it cannot be excluded that such a provision becomes relevant in the future. The EDPS therefore supports its inclusion in the Proposal. However, recognising that the age threshold pursuant to Article 8 GDPR is 16 years (with the possibility for Member States to set a lower threshold but not below 13 years), and keeping in mind the need for a high level of protection, the EDPS considers that the appropriate threshold in Article 8 of the Proposal should be 16 years. In particular, the EDPS notes that the examples given in recital 21 do not justify the lower threshold proposed by the Commission.

21. The EDPS welcomes Article 9 of the Proposal "*Transmissions of personal data to recipients, other than Union institutions and bodies, established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680*" which reflects the specific context of the EU public sector and guarantees that the current level of protection is maintained in the Proposal. Article 9 corresponds to Article 8 of Regulation 45/2001. Article 8(2) of Regulation 45/2001 imposes additional conditions which must be fulfilled by Union institutions before personal data can be transferred to controllers subject to the GDPR (or to the Directive for law enforcement[29]): the transfer must be necessary and the data subject's rights and freedoms and legitimate interests must not be prejudiced. This is an important guarantee which offers data subjects a high level of protection of their personal data vis-à-vis transfers from Union institutions. Moreover, it has become the cornerstone of the Court of Justice case law[30] on balancing the principle of public access to documents enshrined in the Treaty and in Regulation 1049/2001[31] with the right to personal data protection[32].

22. Furthermore, the EDPS considers that Article 11 *Processing of personal data relating to criminal convictions and offences* should not refer to "Union law, which may include internal rules". For a justification, the EDPS refers to his comments in section 2.3.1 below.

2.3 Chapter III - Rights of the data subject

2.3.1 Article 25 Restrictions

2.3.1.1 Scope of possible restrictions

23. Article 25 of the Proposal corresponds to Article 23 GDPR and, as its counterpart, plays an important role in the overall system of data protection rules, allowing for certain exceptions ("restrictions") to be applied where it is necessary and justified. The EDPS welcomes the fact that it would not be possible to restrict application of the rights laid down in Article 23 "*Right to object*" and Article 24 "*Automated individual decision-making, including profiling*" of the Proposal. This is in line with the present approach under Article 20(1) of Regulation 45/2001 (which excludes the application of restrictions with respect to Articles

18 and 19) and corresponds to the need to maintain the current high level of protection under Regulation 45/2001 (see also section 1.2 above).

24. At the same time, the EDPS observes that Article 25 of the Proposal would also render restrictions applicable to the right to confidentiality of electronic communications (Article 34 of the Proposal). This could result in a much more severe restriction of a fundamental right than those caused by the restrictions of the rights established by Articles 14 to 22[33], 38 and parts of Article 4 of the Proposal. While those restrictions would apply to certain modalities of the execution of the fundamental right to data protection as laid down in Article 8 of the Charter, a restriction of the right to confidentiality of communications would have an impact on an essential component of the fundamental right to privacy laid down in Article 7 of the Charter, i.e. "respect for communications". Accordingly, any restriction of this right would have to correspond to the high standards laid down in the ePrivacy Directive (or the forthcoming ePrivacy Regulation).

2.3.1.2 **Modalities for imposing restrictions**

25. Unlike Article 23 GDPR which requires restrictions to be laid down in Union or Member State law, Article 25(1) of the Proposal provides for the possibility of such restrictions by internal rules of EU institutions. The EDPS notes that restrictions by way of internal rules will only be possible "in matters relating to the operation of the Union institutions and bodies"[34].

26. In addition, Article 20 of Regulation 45/2001 in force today, provides for the possibility for EU institutions to impose *ad hoc* restrictions and lays down the conditions and safeguards under which a restriction may be applied in a specific case. Article 25(2) of the Proposal would maintain this possibility for the future. However, in the light of recent case law of the Court of Justice it appears doubtful that such measures would be considered compatible with the Charter, which did not have its current status as primary law at the time of adoption of Regulation 45/2001.

27. While the EDPS recognises the need for a certain degree of flexibility as regards certain data subjects' rights, he is concerned that Article 25 as proposed may not fulfil the requirements set out in the Charter and in the European Convention for Human Rights and Fundamental Freedoms ("ECHR"). According to Article 52(1) of the Charter, any *limitation on the exercise of the rights and freedoms recognised by the Charter* must be "provided for by law" (this corresponds to the expression "in accordance with the law" in Article 8(2) ECHR).

28. As mentioned above, Article 20 of Regulation 45/2001 contains a list of possible restrictions which is comparable to the one included in Article 25 of the Proposal. To date, as far as the EDPS is aware, the legality of this approach has not been subject to a legal challenge. Nevertheless, the EDPS considers that the EU institutions should comply with the highest standards in terms of protection of individual rights and freedoms, especially since the entry into force of the Charter as primary law in December 2009. According to well-established case law of the European Court of Human Rights ("ECtHR"), the expression "in accordance with the law" does not only necessitate compliance with domestic law, but also relates to the *quality* of that law, requiring it to be compatible with the rule of law. In particular, the domestic law must be *sufficiently clear in its terms to give*

citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures[35]. The same strict standard should be required for any restrictions that could be imposed by EU institutions subject to the Proposal. This view is reinforced by the fact that Article 23(2) GDPR imposes certain minimum requirements which must be met, where relevant, by the legislative measures of Union or Member State law that would impose such restrictions.

29. The large majority of the restrictions in Article 25(1) of the Proposal constitute not only restrictions on the application of the rights and obligations set out in the articles listed therein, but also *limitations on the exercise of the right to the protection of personal data* as set out in Article 8 of the Charter[36]. Consequently, the EDPS considers that, in order to ensure compliance with the quality of law requirements referred to above, Article 25(1) of the Proposal would need to be amended to the effect that only legal acts adopted on the basis of the Treaties should be able to restrict fundamental rights, thus imposing on EU institutions the same standards that would apply to Member States under the GDPR. Should *ad hoc* measures be considered necessary for specific cases, the Proposal should specify that any such *ad hoc* measures of EU institutions providing for restrictions shall be clear and precise, only of temporary validity for short periods and shall be published in the Official Journal of the EU. The rules for their enactment should be specified in the relevant legal act with precision. In addition, the EDPS should be consulted by the EU institution in question prior to the adoption of such measures, and judicial scrutiny of any such decision should be ensured, on request of the individual concerned or of the EDPS. A corresponding obligation to consult the EDPS should be inserted e.g. in Article 41 of the Proposal, or in a separate provision.

30. Furthermore, it should be clarified that acts of Union law which could restrict rights set out in Article 25, should comply with the same requirements on specificity and transparency as those laid down in Article 23(2) GDPR.

31. To the extent restrictions to Article 34 "*Confidentiality of electronic communications*" are contemplated, the EDPS calls on the EU legislator to ensure that the possible restrictions of the fundamental right to privacy with regard to communications by EU institutions in their own operations follows the same standards as laid down in Union law as interpreted by the Court of Justice in this domain. The EDPS suggests to ensure that the restriction of this fundamental right is the subject of a separate provision which mirrors the standards set by the ePrivacy Directive (and the pending Commission proposal for a Regulation on Privacy and Electronic Communications). Furthermore, any restriction of this fundamental right may only be enacted through legislative acts adopted on the basis of the Treaties, and by no means through internal rules of EU institutions. The status of confidentiality of communications as an essential component of the fundamental right to privacy enshrined in Article 7 of the Charter underlines the inadequacy of subordinate instruments to restrict rights granted by primary law[37].

32. Regarding Article 25(3) and (4) of the draft proposal, the EDPS welcomes the fact that the data subject rights potentially affected by restrictions for purposes of scientific or historical research or archiving purposes correspond to those covered by Regulation 45/2001 today. Nevertheless, the EDPS considers it necessary to ensure that these restrictions fulfil the same conditions as the corresponding provisions of Article 89 GDPR.

33. Finally, the EDPS welcomes the fact that the draft proposal maintains in Article 25(6) to (8) the provisions corresponding to Article 20(3) to (5) of Regulation 45/2001.

2.4 Chapter IV - Controller and processor

2.4.1 Section 1

34. The EDPS considers that paragraph 5 of Article 31 "*Records of processing activities*" of the Proposal should provide for an *obligation* for EU institutions to keep their records of processing activities in a central register, and to make such registers publicly accessible (such public registers would not include the security measures adopted by the institutions in their processing operations). Today, all registers of processing operations by EU institutions can be inspected by any person *directly* or *indirectly* through the EDPS (Article 26 of Regulation 45/2001) and several registers are publicly accessible on the internet[38]. The Proposal should provide for this obligation for EU institutions in order to maintain a high level of protection, and in order to foster transparency and accountability, as well as to facilitate supervision activities[39]. At the very least, to achieve these purposes, the *direct* and *indirect* inspection possibility through the EDPS of records kept by controllers should be added to Article 31(3) of the Proposal. Given the increased transparency of the DPO function[40], it may also be useful to provide for indirect access through the DPO since he is practically speaking closer to data subjects and the controller than the EDPS as external supervisory authority.

35. The EDPS takes note that, compared to the GDPR, all references to codes of conduct have been removed when they concern entities other than a "*processor who is not an EU institution*". The EDPS welcomes that the use of certificates and codes of conduct by service providers to EU institutions is thus explicitly recognized, and it allows the current practice to rely on such measures as an indication of the appropriateness of an organisation offering services to EU institutions. The EDPS considers, however, that the exclusion of usage of such tools altogether by EU institutions is not appropriate. While codes of conduct as self-regulatory instruments may not seem adequate for EU institutions operating within a clear legal framework provided by EU legislation, certification mechanisms, e.g. certifying compliance with generally accepted standards, may be a very useful instrument as they are currently in different contexts. In particular smaller EU agencies and bodies can benefit from such schemes to demonstrate compliance with specific obligations, and the task of the supervisory authority could also be simplified by permitting EU institutions to make use of certification (but not codes of conduct) by adding the respective provisions *mutatis mutandis* to the relevant Articles of the Proposal, including Article 26 "*Responsibility of the controller*", Article 27 "*Data protection by design and by default*", as well as to Article 33 "*Security*" (see also section 2.4.2.1 above).

2.4.2 Section 2

36. In general, the content in Chapter IV Section 2 regarding security of personal data and data breaches is aligned with the GDPR. The EDPS notes two main differences: the lack of reference to certification and codes of conduct as a means to demonstrating compliance and the addition of elements of the future ePrivacy Regulation as obligations for EU institutions.

37. As regards certification, the observations made above on Section 1 apply to Section 2.

38. The EDPS welcomes that provisions related to responsibilities of a controller in case of a personal data breach (cf. Articles 33 and 34 of the GDPR) are included in the draft proposal and in particular the explicit obligation to inform the DPO.

2.4.2.1 Article 33 Security of processing

39. The EDPS notes that while Article 33 is generally aligned with Article 32 GDPR on the security of processing, the draft proposal does not allow the EU institutions to use codes of conduct or certification as a way to demonstrate compliance with the Regulation. The only reason provided in the text is that "*[...] the Union institutions and bodies should not adhere to codes of conduct or certification mechanisms*" (Explanatory memorandum). While the adherence to codes of conduct may indeed not be appropriate for EU institutions operating under Union law, there seem to be no compelling reasons to prevent that EU institutions can be certified according to international standards on security and privacy, as it has already been the case[41]. The possibility, not the obligation, for EU institutions to obtain a certification to demonstrate compliance with generally accepted standards for security requirements can be useful both for EU institutions and for the EDPS when assessing accountability and compliance. Standards play an important role in demonstrating that measures are state of the art. Allowing certification for EU institutions may also facilitate cooperation with organisations outside the EU which sometimes could insist on compliance with relevant international standards.

2.4.2.2 Article 34 Confidentiality of electronic communications

40. Article 34 obliges EU institutions to ensure the confidentiality of communications as an essential component of the fundamental right to privacy enshrined in Article 7 of the Charter. This mirrors the approach taken in Regulation 45/2001, which incorporates provisions on rights and obligations as they were laid down at the time of its adoption in Directive 97/66/EC[42], the predecessor instrument of the ePrivacy Directive. Regulation 45/2001 was never updated to reflect the considerable development of the electronic communications technology and the corresponding adaptations of the electronic communications framework, in particular the ePrivacy Directive.

41. The replacement of Regulation 45/2001 by the new proposed instrument is the long awaited opportunity to bring the rights of individuals under the protection of the fundamental right of privacy of communications when EU institutions are acting to the same standard as it is applied for any other organisation. Therefore the EDPS welcomes the clarifications provided in Articles 34 "*Confidentiality*", 35 "*Protection of information related to end-users' terminal equipment*" and 36 "*Directories of users*" of the Proposal. Already the current ePrivacy Directive provides for some obligations that apply not only to providers of electronic communications services, but aim to protect individuals against interference with their fundamental rights regardless of the nature of the interfering party (e.g. integrity of terminal devices, use of communications for direct marketing). With the proposal for the ePrivacy Regulation an extension of the scope of services covered may be envisaged, taking account of communications services as part of more general information society services. As such features might also appear in the context of services provided by EU institutions, they should be subject to similar safeguards and obligations as other organisations, with the exception of provisions clearly applicable only to providers of electronic communications services in the strict sense.

42. The EDPS would stress that EU institutions should be under the same obligations as any other controller to respect the confidentiality of communications. They should be under an effective supervision and enforcement regime which, as in other domains, should be enacted by the competent supervisory authority for data protection, i.e. the EDPS. They should not be granted special privilege to restrict this essential fundamental right and should therefore be subject to similar conditions as national administrations, i.e. the requirement of specific legal acts adopted in accordance with the Treaties and not by simple administrative acts.

2.4.2.3 Article 35 Protection of information related to end users' terminal equipment

43. The EDPS welcomes the inclusion of this provisions in the proposal; it refers to the corresponding Article of the proposal for a new ePrivacy Regulation and obliges EU institutions to protect the information on terminal equipment. Such clarification is necessary, as communications equipment, in particular mobile devices, is an important working tool in the EU institutions too. However, it is essential to consider how the relationship between the end-user and the terminal equipment must be construed: neither *ownership* nor *possession* of the terminal equipment constitute a pre-condition for an effect on the privacy of an individual (in view that private and institutionally provided terminals are used interchangeably). The EDPS also notes that the provision relies on a definition of end-user from the proposed Electronic Communications Code[43], which may or may not when adopted lead to the intended level of protection for data related to user terminals. In any event, the level of protection granted under the Proposal should not depend on the final outcome of a separate legislative process. For these reasons, the EDPS considers that the word 'end-user' should be deleted from the text of the Article without replacement.

2.4.2.4 Article 36 Directories of users

44. The inclusion of a limitation of directories to what is strictly necessary, and the obligation to EU institutions to prevent the use for these directories for direct marketing is very welcome. Again, this provision brings EU institutions to the same rights and obligations as any other entity. This is in line with the general principle that EU institutions should respect the rules and principles of Union law.

2.4.2.5 Article 37 Notification of a personal data breach to the EDPS and Article 38 Communication of a personal data breach to the data subject

45. The EDPS welcomes Articles 37 and 38 on data breach notification/communication which are generally aligned with Articles 33 and 34 GDPR, with some minor adaptations to reflect that the EDPS is the supervisory authority concerned and the fact that there will be an information of the DPO in all cases.

2.4.3 Section 3

2.4.3.1 Article 40 Prior consultation

46. Article 40(4) of the Proposal provides that the Commission may adopt by means of an implementing act a list of cases subject to prior consultation of the EDPS. The EDPS welcomes the flexibility of such a measure so that the list can be updated as the case may be. The EDPS considers that, in view of their impact on individuals, automated individual decisions adopted pursuant to Article 26 of the Proposal should in any event be among the cases subject to prior consultation of the EDPS pursuant to Article 40 of the Proposal, as

such decisions may have the purpose or effect of depriving individuals of a right or a benefit, and under Regulation 45/2001 they are considered risky and subject to prior checking[44].

2.4.4 Section 4

47. As set out in section 2.3.1 above regarding Article 25 *Restrictions*, the EDPS considers that in principle only legal acts adopted on the basis of the Treaties should be able to restrict fundamental rights. Should the EU legislator nevertheless consider *ad hoc* measures necessary for specific cases, the EDPS should be consulted by the EU institution in question prior to the adoption of such *ad hoc* restrictions. A corresponding obligation to consult the EDPS should be inserted e.g. in Article 41 of the Proposal, or in a separate provision.

2.4.4.1 Article 42 Legislative consultation

2.4.4.1.1 Scope and modalities of legislative consultation

48. Currently, under Article 28(2) of Regulation 45/2001, the Commission has an obligation to consult the EDPS whenever it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. The scope of this advisory task is broad and covers not only the processing of personal data by EU institutions, but also advising EU institutions on all matters concerning the processing of personal data[45]. The EDPS' approach to fulfilling his advisory and consultative role has been set out in a *Policy paper* "*The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience*"[46].

49. As the EDPS faces the challenge of providing effective advice on the basis of increasingly limited resources, a strategic approach to our advisory task has been developed. Given the significant number of legislative proposals issued by the Commission, the EDPS establishes a list of priorities[47] on a yearly basis, flagging a limited number of strategic issues, on which he wishes to concentrate our efforts. It is important to stress in this context that, although the obligation to consult the EDPS is incumbent on the European Commission, the principal addressees and beneficiaries of our advice and expertise are all EU co-legislators, notably the European Parliament and the Council[48].

50. Against this background, the EDPS welcomes the fact that the Proposal includes a separate article dedicated to the role of the EDPS as an advisor to EU institutions. He also welcomes that recommendations or proposals to the Council pursuant to Article 218 TFEU, as well as delegated and implementing acts are explicitly included within the scope of the obligation of the Commission to consult the EDPS. This is broadly in line with the existing practice, but the clarification will contribute to more uniform application of this approach across the various Commission services.

51. The EDPS is concerned that the wording used in Article 42(1) of the Proposal, "*[f]ollowing the adoption of proposals*" (as opposed to "*[w]hen it adopts a legislative proposal*" in Article 28(2) of Regulation 45/2001) might put into question the long-standing commitment of the European Commission to consult the EDPS on draft proposals in an informal manner, usually at the stage of the inter-service consultation[49]. Experience of the past years shows that the EDPS' interventions are most effective when he is able to provide input at an early stage, before the College of Commissioners takes a final decision on a legislative proposal, another measure or a policy document. Informal exchanges between the EDPS and the Commission services at working level at such early stages of preparation

allow both sides to better understand their respective objectives and concerns, including political considerations at stake, and jointly work towards solutions which are fully compliant with the rights to privacy and data protection and which will be capable of withstanding possible future challenges before the Court of Justice. Our strategic approach to issuing formal Opinions also means that input at the informal stage is often the most effective opportunity in practice to provide a contribution on data protection matters[50].

52. Given the importance of informal consultation, the EDPS would welcome a recital in which the Commission would reiterate its commitment to this long-standing practice. He would also support that the Proposal maintains the wording of Article 28(2) of Regulation 45/2001 ("when it adopts") which allows a broader margin of manoeuvre in his regard.

53. Furthermore, the EDPS observes that the requirement of "*impact on the protection of individuals' rights and freedoms with regard to the processing of personal data*" appears inconsistent with the approach in Article 57(1)(c) GDPR which strengthens the advisory role of national Data Protection Authorities by tasking them with advising relevant national authorities, in accordance with national law, on "*legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing*" of personal data. The EDPS underlines that these powers granted to national supervisory authorities constitute "necessary means" for the Supervisory authorities to perform their duties[51]. The EDPS considers that, in line with the overall objective to achieve maximum alignment with the GDPR, the same criterion "*relating to the protection...*" should be used in Article 42(1).

2.4.4.1.2 Cooperation with the EDPB in the field of legislative consultation

54. The Proposal also stipulates in Article 42(2) that where a proposal is "*of particular importance for the protection of individuals' right and freedoms with regard to the processing of personal data*", the Commission may also consult the EDPB and the two bodies will coordinate "*with a view to issue a joint opinion*". The EDPS welcomes this provision as he is committed to increasing the synergy with national colleagues in accordance with the general provisions on cooperation among DPAs, as reinforced by the GDPR. Already today, when setting his legislative consultation priorities, the EDPS specifically avoids unnecessary duplication of opinions coming from the Article 29 Working Party on the one hand, and from the EDPS on the other, including the sharing of his priorities with the Article 29 Working Party.

55. In those rare cases where opinions on the same topic are issued by both bodies, the advice is designed to be complementary and offers an analysis from different angles, as illustrated by the Opinions on remotely-piloted aircrafts (drones)[52] or the Opinions on the revision of the ePrivacy Directive[53]. For instance, where the EDPS focuses on legislative instruments at EU level and aims at providing a future-oriented vision, the Article 29 Working Party typically advises on matters directly related to ensuring consistent application of Directive 95/46/EC[54].

56. In addition, further procedures for ensuring coordination between the EDPS and the EDPB will also be covered in the EDPB Rules of Procedure[55] and a Memorandum of Understanding[56], currently under preparation.

57. In view of the above, the EDPS considers that Article 42 provides sufficient clarification as to the respective tasks of the EDPS and the EDPB to avoid unnecessary duplication in the future.

58. According to Article 42(4) of the draft proposal, the obligation to consult the EDPS does not apply where the Commission is required to consult the European Data Protection Board (EDPB) pursuant to the GDPR. This is notably the case for adequacy decisions (Article 45(3) GDPR) or delegated acts on standardised privacy icons. However, more than the nature of the act (adequacy decisions, delegated act), it is a consistent approach to substance that matters: this would plead for a consistent consultation of EDPS for instance on an international agreement and on an adequacy decision, both concerning the level of protection of a third country. The EDPS therefore recommends amending slightly Art 42(4) so that the relevant phrase would read "*Article 42(1)* shall not apply (...)". This would mean that, when the Commission is obliged to consult the EDPB, it shall not be *obliged* to consult the EDPS but it may still do so if relevant. In such cases, the coordination procedure foreseen in Article 42(2) would apply.

2.4.5 Section 5

2.4.5.1 Article 44 Designation of the Data Protection Officer

59. The EDPS welcomes the possibility in Article 44(2) for EU institutions to designate one single Data Protection Officer ("DPO") for several of them, which is appropriate in the EU institutional context. Indeed, EU institutions which are geographically close to each other and are similar in activity, structure, tasks and procedures may benefit from a shared and easily accessible DPO.

60. Article 44(4) provides that the DPO may be a staff member or fulfil the tasks on the basis of a service contract. This provision mirrors Article 37(6) GDPR and abolishes the limitation to appoint an EU institution's staff member as DPO[57]. While article 37(6) GDPR does not draw a distinction between public authorities and other entities on this outsourcing possibility, the EDPS considers that such an outsourcing approach is not suitable in a targeted Regulation applicable to EU institutions exercising public authority. Indeed, the Proposal foresees a key function for the DPO in ensuring the application of its provisions. By contrast to external service providers, EU institutions' staff members are composed of officials, temporary agents and contract agents who are subject to the rights and obligations governed by EU law[58]. Those staff members are expected to live up to the highest standards of professional ethics and to remain independent at all times[59]. Also, the DPO role requires a high level of confidentiality that could be best maintained by an internally appointed DPO subject to the EU Staff Regulations and Conditions of Employment. Furthermore, the EDPS' experience has shown that knowledge of the institution, its mandate and functions, the management and staff, and the processing operations is essential for the DPO of an EU institution to perform his or her functions effectively, thus a staff member seems to be most suited to exercise this function. Besides that, it is not obvious to see how such an outsourcing possibility could result in added benefits or safeguards for data subjects or controllers; by contrast a geographic or organisational distance may be seen as obstacle to receive effective and prompt assistance or guidance. The EDPS therefore recommends the deletion of Article 44(4) second alternative ("*or fulfil the tasks on the basis of a service contract*").

2.4.5.2 Articles 45 and 46 Position and tasks of the DPO

61. The EDPS welcomes the fact that, while consistent with the corresponding provisions of the GDPR, these Articles have been supplemented with elements from the current Regulation 45/2001 and its Annex.

62. In addition, the EDPS considers that Article 45 explicitly grants the DPO access to all personal data and to all information necessary for the performance of his or her tasks in order to render his or her investigation powers operational[60].

63. Finally, Article 46 should be supplemented by the sentence currently present in Article 24(1) of Regulation 45/2001: "[The data protection officer] *shall ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations*". This would reinforce the role of the DPO who has to exercise his or her tasks in an independent manner, also in relation to his or her management.

2.5 Chapter V - Transfer of personal data to third countries or international organisations

2.5.1 Article 52 International cooperation for the protection of personal data

64. Article 52, mirrors almost exactly Article 50 of the GDPR. In order to reflect current practice (e.g., regarding activities in the context of Council of Europe, the OECD, and international organisations workshops) the EDPS recommends adding the following elements:

> "*(e) monitor relevant international developments, insofar as they relate to the protection of personal data, in particular in the framework of international organisations;*
>
> *(f) promote international awareness and understanding of the risks, rules, safeguards and rights in relation relating to the processing of personal data.*".

2.6 Chapter VI - The European Data Protection Supervisor

2.6.1 Establishment and structure

65. The EDPS considers that the choice of the most appropriate structure for the institution is the exclusive prerogative of the EU legislator. He nevertheless wishes to stress that the current setup, resulting from a political compromise, is rather unique among European data protection supervisory authorities (which typically fall into one of two categories: a single supervisor or a collegial body). Over the past 12 years the EDPS has worked out internal arrangements allowing it to function effectively, but he has no specific objections to the approach taken in the Proposal.

66. The EDPS notes that paragraph 4 of Article 54 *Appointment of the EDPS* of the Proposal regarding the cessation of duties of the EDPS differs from the current Article 42(4) of Regulation 45/2001 and does not fully correspond to the wording of Article 53(3) GDPR, either. In order to guarantee full independence of the institution, he recommends that the wording of the provision is clarified, as follows:

- Article 54(4)(a) should refer to the expiry of the term of office (see Article 53(3) GDPR);
- in Article 54(4)(b) a reference to Article 54(6) should be added;
- Article 54(4)(c) a reference to Article 54(5) is added (in line with Article 42(4) of Regulation 45/2001).

2.6.2 Article 58 *Tasks*

67. The EDPS welcomes the Proposal in so far as the tasks of the EDPS have generally been aligned with tasks of national supervisory authorities set forth in Article 57 GDPR.

68. However, there is no equivalent rule to Article 57(1) (m-q) GDPR on the EDPS role on codes of conduct and certification, while EU institutions may use processors who rely on these instruments to demonstrate compliance. As evidenced by multiple public procurement notices, certification against generally accepted standards is an important tool in the selection of service providers, including processors of personal data, to ascertain that the bidding party is capable of complying with certain conditions required by law. Increasingly, EU institutions such as the Commission and ENISA are facilitating the creation of standards, certification schemes and also codes of conduct which are meant to provide reassurance to controllers and data subjects. Often data protection compliance and accountability are core criteria for such instruments[61]. In order to ensure that such measures, which will continue to be used by EU institutions when assessing the appropriateness of a service provider, are designed in such a way that they are adequate for EU institutions, the EDPS should have the possibility to contribute to their development. The effort invested in the development of such tools would be more than counterbalanced by the fact that the assessment of practical cases of administrative measures can be simplified when an external assessment of compliance with a relevant standard or code of conduct is present.

69. The EDPS considers that such tasks are unlikely to be covered by the catch-all clause of Article 58(1)(q) stipulating that the EDPS shall "*fulfil any other tasks related to the protection of personal data*", and therefore recommends that the Proposal be aligned with Article 57 of the GDPR, as described above.

70. In addition, it is important to explicitly provide in the new Regulation that the EDPS shall be responsible for monitoring the EU institutions' obligation to respect the confidentiality of electronic communications. As explained above, the supervision and enforcement of respect for this fundamental right by EU institutions should follow the same principle as for any other organisations, i.e. it should be ensured by the competent independent supervisory authority for the protection of personal data, in this case the EDPS. EU institutions should have the same rights and obligations as other public administrations and should have no special privileges in that respect. The present Proposal is the appropriate instrument to ensure that EU institutions are bound not only by the rules of the GDPR, but also by those of the forthcoming instrument following from the proposal for the ePrivacy Regulation. The Proposal should therefore mirror the provisions on supervisions and enforcement from that draft Regulation.

71. The EDPS understands that the reference to the monitoring of relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies (Article 58(1)(h) of the

Proposal) include the ethical dimension and societal issues arising from the evolution of digital technologies.

72. Pursuant to Article 58(1)(a), processing operations by the Court of Justice of the European Union acting in its judicial capacity fall outside the scope of the EDPS supervision. Though under Article 55(3) of the GDPR national DPAs are not necessarily the supervisory authorities for national courts with regard to judicial activities, Member States (including those where the DPA is currently performing these tasks) must keep or identify a new solution to comply with Articles 16(2) TFEU and Article 8(3) of the Charter, and entrust a truly independent supervision mechanism. The EDPS therefore encourages the EU legislator to take the opportunity of the new Regulation to identify soon, in cooperation with the Court of Justice, a suitable solution to the lack of control by an independent authority.

2.6.3 **Article 59 *Powers***

73. The EDPS notes that the Proposal does not include a provision equivalent 58(3)(c) GDPR which grants national supervisory authorities the power to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation. In order to ensure consistency with Article 40(4) of the Proposal (which grants the Commission the possibility to determine, by means of an implementing act, a list of cases in which the controllers shall consult with, and obtain prior authorisation from, the EDPS in relation to processing for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health), the EDPS should have the corresponding power to authorise such processing referred to in Article 40(4) of the Proposal.

74. The EDPS welcomes Article 59(5) of the Proposal which essentially maintains the powers currently laid down in Articles 47(1)(h) and 47(1)(i) of Regulation 45/2001 to refer the matter to the Court of Justice and to intervene in actions brought before the Court.

75. In this respect, the word "actions" has been interpreted to exclude preliminary ruling proceedings[62]. However, on several occasions the Court has invited the EDPS to answer questions or provide information on the basis of Article 24 of its Statute. The need for expert advice can only grow with the entry into effect of the GDPR and an increase in the number of questions referred to the Court of Justice by national courts. The EDPS therefore recommends changing the word "actions" to "proceedings" and including a reference in the recitals that the EDPS shall, at the request of the Court, supply all information or advice, which the Court considers necessary for the proceedings.

76. The EDPS welcomes Article 55(6) of the Proposal stipulating that the EDPS shall have its seat in Brussels. This is essential so as to ensure the proximity which, by the nature of his tasks, must exist between the EDPS and the EU institutions subject to his supervision, and in order to facilitate the smooth performance of his duties[63].

2.7 Chapter VII - Cooperation and Consistency

2.7.1 Article 62 Coordinated supervision by the EDPS and national supervisory authorities

77. The EDPS highly welcomes the approach of a single coherent model of coordinated supervision for EU large scale information systems and where specific model of cooperation are envisaged as regards data processing by EU agencies. This will contribute to the comprehensiveness, effectiveness and coherence of data protection supervision and ensure a sound environment for further development in the years to come.

78. The EDPS understands that the objective is to use this model both for the supervision of future systems and for existing ones. He notes that recital 65 specifically mentions that "*[T]he Commission should therefore, where appropriate, submit legislative proposals with a view to amending Union legal acts providing for a model of coordinated supervision, in order to align them with the coordinated supervision model of this Regulation*". The EDPS would welcome such a streamlining.

2.8 Chapter VIII - Remedies, liability and penalties

79. The EDPS welcomes the fact that certain specificities of Regulation 45/2001 concerning the legal environment within which EU institutions operate have been maintained in the Proposal, for example through minor adjustments like a reference to "non-judicial remedy" in Article 63(1), or by maintaining provisions of Regulation 45/2001 such as Article 65 *Right to compensation*, *Article* 68 *Complaints by Union staff* and *Article* 69 *Sanctions*.

2.8.1 Article 66 Administrative fines

80. Pursuant to Article 83(7) GDPR, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. At present, national supervisory authorities of at least three Member States have the power to impose fines on public sector bodies[64] and several others are considering it as part of the ongoing GDPR implementation process. In the present proposal, the Commission decided to follow these Member States by granting the EDPS the power to impose administrative fines (Article 66). The EDPS welcomes this provision. The EDPS considers that depriving the EU supervisory authority of the possibility to impose administrative fines, where appropriate, would result in EU institutions enjoying a privileged position compared to public sector institutions in many Member States.

81. The EDPS notes in this respect that, in line with recital 70, fines would constitute "a sanction of last resort", to be imposed in case of non-compliance with one of the other corrective measures under Article 59(2)(d) to (h) and (j). However, Article 58(2)(i) GDPR provides for administrative fines *in addition to*, or *instead of* measures referred to in the same paragraph. The possibility to impose fines in the same way as the GDPR would be an effective and dissuasive addition to the existing range of enforcement powers[65] and would be used with extreme caution. The EDPS also notes that while Article 66 now only refers to "*...points **(d)** to (h) and (j) of Article 59(2)*", the Explanatory Memorandum refers to "*Article 59(2)**(a)** to (h) and (j)*" and, in this context, explicitly states that "*Article 66 builds on Article 83 of Regulation (EU) 2016/679...*". Therefore, the possibility to impose fines should apply in relation to any corrective measure imposed by the EDPS under Article

59(2). The legislator may also consider, in addition, the possibility for the EDPS to impose fines directly, and not as a last resort, in exceptional cases concerning particularly serious infringements of the Regulation with intentional or gross negligence character.

82. In addition, the EDPS notes that fines under Article 66 would be significantly lower than those provided for under Article 83(4) to (6) GDPR. He takes note of this approach given that, unlike the GDPR, the Proposal does not target operators pursuing in principle gainful activities. Moreover, fines of this order of magnitude, while having an undoubtedly deterrent effect, would not in any case risk jeopardising day-to-day functioning of the EU institution in question.

83. The EDPS suggests aligning this provision to a maximum extent with the criteria set forth in Article 83 GDPR, in particular:
    - add a provision on due regard to be given to the intentional or negligent character of the infringement (see Article 69 *Sanctions* referring to both characters of such infringement and Article 83(2)(b) GDPR);
    - add a provision on due regard to be given to "any other aggravating or mitigating factor" (Article 83(2)(k) GDPR;
    - Articles 66(5) and (6) stipulating the rights of the parties and the due process implications are drafted more broadly than the corresponding provisions of the GDPR, without any obvious justification. The EDPS considers that there is no need for this level of specificity, especially given that recitals 63 and 64, read together with the European Code of Good Administrative Behaviour[66] and in combination with the EDPS Rules of Procedure, if necessary amended following the adoption of the present Proposal, would be sufficient to guarantee the rights of the parties and due process.

84. Finally, the wording "*access to the Supervisor's file*" in Article 66(6) should be clarified by referring to the access to the "investigation file maintained by the EDPS".

2.8.2 Article 67 Representation of data subjects

85. The EDPS welcomes the possibility for representative associations to act on behalf of individuals on the basis of a mandate, in line with Article 80(1) GDPR.

86. He strongly recommends, however, that such representative associations should be able to act on behalf of individuals even without a mandate (which is an option for Member States foreseen in Article 80(2) GDPR) with respect to submitting a complaint with the EDPS (but not as regards the exercise of the right to an effective judicial remedy under Article 64 of the Proposal).

2.9 Chapter X - Final provisions

2.9.1 EDPS and Regulation 1049/2001 on public access to documents

87. Pursuant to Article 15 TFEU, citizens of the Union, as well as any natural or legal person residing or having its registered office in a Member State, shall have a right of access to documents of the Union's institutions, bodies, offices and agencies, in accordance with applicable legislation. Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents[67] lays down the applicable legal framework for exercising this

right of access to documents. Article 56 of the EDPS Rules of Procedure[68] stipulates that the public shall have access to documents held by the EDPS in accordance with the principles laid down by Regulation (EC) No 1049/2001[69].

88. In order to ensure compliance with the EU primary law, as well as to reflect the existing practice, the EDPS recommends to insert in the Proposal an explicit clause rendering Regulation (EC) No 1049/2001 applicable to EDPS documents.

2.9.2 Providing for the use of existing tools for data exchange between national and EU authorities

89. Several provisions of the GDPR provide for electronic exchange between the national supervisory authorities, the EDPS, the EDPB and the Commission in cooperation and consistency procedures (e.g. Art. 47(3), 60(12), 61(9), 64(4), 75(6)d). In order to make the most efficient use of the budgetary resources of the Member states and the Union, reusable components of IT systems and infrastructure developed for similar tasks in other areas of Union law should be evaluated for potential re-use for the purposes of implementing the GDPR. In order to ensure that this option is not blocked by legal obstacles, the respective legal frameworks should be amended to allow such use where this is not currently the case. One instrument to be considered in this respect is the IMI Regulation 1024/2012[70].

3. CONCLUSIONS

90. Overall, the EDPS considers the Proposal successful in aligning the rules for EU institutions with the GDPR, while taking the specificities of the EU public sector into account. The high level of protection regarding data processing by EU institutions is generally preserved in the Proposal. The EDPS particularly appreciates the balance of the various interests at stake achieved by the Commission.

91. The EDPS considers that the Proposal should be further improved, notably regarding the modalities for restrictions under Article 25. In order to ensure compliance with the quality of law requirements referred to above, Article 25(1) of the Proposal would need to be amended to the effect that only legal acts adopted on the basis of the Treaties should be able to restrict fundamental rights, thus imposing on EU institutions the same standards that would apply to Member States under the GDPR. To the extent restrictions to Article 34 *Confidentiality of electronic communications* are contemplated, the EDPS calls on the EU legislator to ensure that the possible restrictions of the fundamental right to privacy of communications by EU institutions in their own operations follows the same standards as laid down in Union law as interpreted by the Court of Justice in this domain.

92. The EDPS welcomes the fact that the Proposal includes a separate article dedicated to the role of the EDPS as an advisor to EU institutions (Article 42 of the Proposal). He is, however, concerned that the wording "*[f]ollowing the adoption of proposals*" (as opposed to "*[w]hen it adopts a legislative proposal*" in Article 28(2) of Regulation 45/2001) might put into question the long-standing commitment of the European Commission to consult the EDPS on draft proposals in an informal manner, usually at the stage of the inter-service consultation. Given the importance of informal consultation, the EDPS would welcome a recital in which the Commission would reiterate its commitment to this long-standing practice. He would also support that the Proposal maintains the wording of Article 28(2) of

Regulation 45/2001 ("when it adopts") which allows a broader margin of manoeuvre in his regard. He considers that Article 42 as proposed provides sufficient clarification as to the respective tasks of the EDPS and the EDPB to avoid unnecessary duplication in the future.

93. The EDPS considers that the possibility to outsource the function of a DPO is not suitable for EU institutions exercising public authority. Consequently, Article 44(4) second alternative ("*or fulfil the tasks on the basis of a service contract*") should be deleted.

94. The EDPS welcomes Article 66 of the Proposal which would grant the EDPS the power to impose administrative fines. He considers that depriving the EU supervisory authority of the possibility to impose administrative fines, where appropriate, would result in EU institutions enjoying a privileged position compared to public sector institutions in many Member States.

95. The EDPS considers that certification mechanisms may be a very useful instrument for EU institutions and they are already being used in certain contexts, e.g. certifying compliance with generally accepted standards. References to the use of certification (but not codes of conduct) should therefore be added to Article 26 *Responsibility of the controller*, Article 27 *Data protection by design and by default*, as well as to Article 33 *Security*.

96. While this Opinion indicates a number of areas in which the proposal could be further improved, the EDPS would encourage the EU legislator to reach agreement on the Proposal as swiftly as possible so as to allow EU institutions to benefit from a reasonable transition period before the new Regulation can become applicable at the same time as the GDPR, in May 2018.

Brussels, 15 March 2017

(**signed**)

Giovanni BUTTARELLI

European Data Protection Supervisor

NOTES

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 119, 4.5.2016, p. 1 (later, "the GDPR").
[3] OJ L 8, 12.1.2001, p. 1.
[4] OJ L 350, 30.12.2008, p. 60.
[5] OJ L 119, 4.5.2016, p. 89.
[6] COM(2017) 8 final; 2017/0002 (COD) (later, "the Proposal").
[7] Article 286 EC rendered the (then) Community rules on data protection applicable to EU institutions and bodies and mandated the creation of a dedicated independent supervisory authority (later, the EDPS).
[8] Case C-518/07 *Commission v Germany*, EU:C:2010:125; Case C-614/10 *Commission v Austria*, EU:C:2012:631; Case C-288/12 *Commission v Hungary*, EU:C:2014:237; Case C-362/14 *Maximilian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650.
[9] Case C-518/07 *Commission v Germany*, *supra* para. 19.
[10] Case C-288/12 *Commission v Hungary*, *supra* para. 53.
[11] See *supra* note 3.
[12] Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, OJ L 183, 12.7.2002, p. 1.
[13] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 2017/0003 (COD).
[14] See Article 98 and recital 17 of the GDPR.
[15] See e.g. the EDPS Opinion of 7 March 2012 on the data protection reform package, OJ C 192, 30.6.2012, p. 7.
[16] EDPS Opinion of 7 March 2012 on the data protection reform package, p. 6.
[17] See in particular Article 6(3) and recital 10 to the GDPR: "*Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.*"
[18] E.g. last sentence of Article 6(1), Article 20(5), Article 27, Article 37, Article 41 or Article 46(2)(a) of the GDPR.
[19] See in particular the EDPS Opinion of 14 January 2011 on the Communication "A comprehensive approach on personal data in the European Union", OJ L 181, 22.6.2011, p. 1.
[20] See *supra* note 5.
[21] Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final, now adopted as Regulation 2016/794 and published in OJ L 135 24.05.2016, p. 53; Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, COM(2013) 534 final. See also the Council General approach [First reading] on the Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) available at: http://data.consilium.europa.eu/doc/document/ST-6643-2015-INIT/en/pdf.
[22] EDPS Opinion 3/2015 "Europe's big opportunity - EDPS recommendations on the EU's options for data protection reform", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-10-09_GDPR_with_addendum_EN.pdf.
[23] See the list of EU institutions and bodies available at: http://publications.europa.eu/code/en/en-390500.htm.
[24] Regulation 45/2001 already today applies to, *inter alia*, the European Defence Agency, European Union Institute for Security Studies, and the European Union Satellite Centre.
[25] Europol, Eurojust, EPPO, *supra* note 21.
[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, OJ L 201, 31.7.2002, p. 37, as amended (later, "the ePrivacy Directive").

[27] Recitals 10-12 ePrivacy Directive.
[28] See judgment of the Court of Justice in case F-46/09 *V v European Parliament*, ECLI:EU:F:2011:101, concerning an inter-institutional transfer of medical data between the European Commission and the European Parliament.
[29] *Supra* note 5.
[30] Judgment of the Court (Grand Chamber) of 29 June 2010 in Case C-28/08 P *European Commission v The Bavarian Lager Co. Ltd*, ECLI: EU:C:2010:378.
[31] See section 2.9.1.
[32] See also, in this context, Article 86 of the GDPR *Processing and public access to official documents*.
[33] Article 14 *Transparent information [...]*, Article 15 *Information to be provided where personal data are collected from the data subject*, Article 16 *Information to be provided where personal data have not been obtained from the data subject*, Article 17 *Right of access by the data subject*, Article 18 *Right to rectification*, Article 19 *Right to erasure ('right to be forgotten')*, Article 20 *Right to restriction of processing*, Article 21 *Notification obligation regarding rectification or erasure of personal data or restriction of processing*, Article 22 *Data portability*; Article 34 *Confidentiality of electronic communications*; Article 4 *Principles relating to processing of personal data*.
[34] Article 25(1) of the Proposal.
[35] *Malone v United Kingdom*, [1984] ECHR 10, para. 67; *Leander v Sweden*, [1987] 9 EHRR 433, paras. 50-51; *Halford v United Kingdom*, [1997] ECHR 32, para. 49.
[36] See in particular the criteria listed in Article 8 paragraph 2 of the Charter.
[37] See, by analogy, Case C-362/14 *Schrems*, *supra* note 8, paras. 53 and 101-102.
[38] E.g. European Commission, European Parliament, Council of the European Union have registers of processing operations accessible on the internet.
[39] In this context it shall be borne in mind that the introduction of the obligation for controllers and processors to maintain records replaces the current requirement of prior notifications to the EDPS and their documentation in a Register kept by the EDPS (Articles 25 and 46 under (i) of Regulation 45/2001).
[40] E.g. publication of DPO's contact details by EU institutions and mentioning of DPO's contact details in Privacy statements, see articles 44(5) and 15(1) under (b) of the Proposal.
[41] For example, EUIPO is certified for compliance with ISO 27001 and ISO 9001, (https://euipo.europa.eu/ohimportal/nl/news/-/action/view/3339887), ECHA and GSA have obtained certification for ISO 9001. (https://echa.europa.eu/view-article/-/journal_content/title/echa-awarded-iso-9001-2008-certificate, https://www.gsa.europa.eu/newsroom/news/gsa-extends-scope-iso-9001-certification).
[42] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30.1.1998, p.1.
[43] Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), COM(2016) 590 final/2.
[44] As to the slight difference in wording between Article 40 of the Proposal and Article 36 GDPR, the EDPS observes that, the Article 29 Working Party's upcoming guidance on the GDPR will most likely interpret Article 36 GDPR (together with the relevant recitals) to say that prior consultation should only be required in cases of "residual high risk", i.e. the same approach as in Article 40 of the Proposal (so not all processing operations that require a DPIA would also require prior consultation).
[45] See Order of the Court of Justice (Grand Chamber) of 17 March 2005 in Case C-317/04 *Parliament v Council*, ECLI:EU:C:2005:189: "*In accordance with the second subparagraph of Article 41(2) of Regulation No 45/2001, the Supervisor is to be responsible not only for monitoring and ensuring the application of the provisions of that regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, but also for advising Community institutions and bodies on all matters concerning the processing of personal data. That advisory task does not cover only the processing of personal data by those institutions or organs. For those purposes, the Supervisor carries out the duties provided for in Article 46 of that regulation and exercises the powers conferred on him by Article 47 of the regulation*."
[46] EDPS Policy Paper of 4 June 2014 "The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/14-06-04_PP_EDPSadvisor_EN.pdf.
[47] For 2017, see "EDPS Priorities for providing advice in 2017: The implementation of our advisory role to the EU legislator", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Priorities/17-02-15_EDPS_Priorities_2017_EN.pdf. The EDPS consultation priorities documents for the past ten years can be found at: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Priorities.

[48] For example, On 10 January 2017, the Council decided to consult the EDPS on a proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, see http://data.consilium.europa.eu/doc/document/ST-5005-2017-INIT/en/pdf. In response to this request, the EDPS issued Opinion 4/2017 of 14 March 2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content.
[49] Note of the Secretary General of the Commission to Directors-General and Heads of Service of 8 December 2006, SEC(2006) 1771.
[50] For example, in 2016 the EDPS issued 9 opinions (including 6 opinions on Commission legislative proposals), 2 sets of *formal* comments and 31 sets of *informal* comments. Both opinions and formal comments are transmitted to the European Parliament, the Council and the Commission, while informal comments are provided to the Commission in confidence, usually at the stage of inter-service consultation.
[51] See Case C-362/14 *Schrems*, *supra* note 8, para. 43.
[52] Article 29 Working Party on Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf; EDPS Opinion of 26 November 2014 on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-11-26_Opinion_RPAS_EN.pdf.
[53] Article 29 Working Party Opinion 03/2016 on the evaluation and review of the ePrivacy Directive, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf; Preliminary EDPS Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_EN.pdf.
[54] See e.g. the Article 29 Working Party Opinion 5/2012 on cloud computing available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf; and EDPS Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.
[55] Article 72(2) GDPR.
[56] Article 75(4) GDPR.
[57] See article 24 of Regulation 45/2001 and its Annex under 5.
[58] Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union.
[59] See Recital 4 of Regulation (EU, EURATOM) No 1023/2013 of the European Parliament and of the Council of 22 October 2013 amending the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union, OJ L 287 of 29.10.2013, p.15.
[60] See Annex to Regulation 45/2001 at 4: "*In performing his or her duties, the Data Protection Officer shall have access at all times to the data forming the subject-matter of processing operations and to all offices, data-processing installations and data carriers.*"
[61] Examples include codes of conduct, impact assessment templates and other standards in fields such as RFID, smart meters, mHealth devices and cloud computing.
[62] Order of the President of the Court of 12 September 2007, C-73/07 *Satakunnan Markkinapörssi and Satamedia*, ECLI:EU:C:2007:507.
[63] See Article 4 and recital 10 to Decision No 1247/2002/EC, *supra* note 12.
[64] Latvia, the Netherlands, and the United Kingdom.
[65] See Policy paper "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_EN.pdf.
[66] https://www.ombudsman.europa.eu/en/resources/code.faces#/page/1.
[67] OJ L 145, 31.5.2001, p. 43.
[68] OJ L 273, 15.10.2013, p. 41.
[69] See also recital 5 to Decision No 1247/2002/EC, *supra* note 12, stating that "*[t]he European Data Protection Supervisor is bound by Community law and should comply with Regulation (EC) No 1049/2001 [...]. He should thus be bound by the provisions of the Treaty concerning the protection of fundamental rights and freedoms, establishing that decision-making in the Union is to be as open as possible and providing for protection of personal data, in particular the right to privacy.*"

[70] Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation'), OJ L 316, 14.11.2012, p.1.