EUROPEAN DATA PROTECTION SUPERVISOR

Summary of 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

(The full text of this Opinion can be found in English, French and German on the EDPS website www.edps.europa.eu)

(2017/C 164/02)

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.

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 ([1]) ('the Proposal').

([1]) COM(2017) 8 final; 2017/0002 (COD) (later, '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 ([2]). 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 ([3]). In particular, the supervisory authority must act with complete independence, which implies a decision-making power independent of any direct or indirect external influence ([4]) and freedom from any suspicion of partiality ([5]).

4. The main legal instrument applicable to the processing of personal data by EU institutions is Regulation (EC) No 45/2001 ([6]) ('Regulation 45/2001'), complemented by Decision No 1247/2002/EC ([7]).

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' ([8])) 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 ([9]). 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 ([10]). 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

([2]) 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).
([3]) 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.
([4]) Case C-518/07 *Commission* v *Germany*, *supra* para. 19.
([5]) Case C-288/12 *Commission* v *Hungary*, *supra* para. 53.
([6]) See *supra* note 3.
([7]) 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).
([8]) 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).
([9]) See Article 98 and recital 17 of the GDPR.
([10]) See e.g. the EDPS Opinion of 7 March 2012 on the data protection reform package (OJ C 192, 30.6.2012, p. 7).

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') ([11]).

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 ([12]). In those cases where the GDPR provides specific rules for public authorities ([13]) 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 ([14]). The Commission chose a different approach and proposed a separate legal instrument for data protection in the law enforcement area ([15]). A number of proposals for legal acts introducing separate 'standalone' data protection regimes followed ([16]).

([11]) EDPS Opinion of 7 March 2012 on the data protection reform package, p. 6.

([12]) 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.'

([13]) 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.

([14]) 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).

([15]) See *supra* note 5.

([16]) 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, 24.5.2016, 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

14. The EDPS acknowledges that the current, albeit fragmented, legal framework for personal data protection is the best outcome achievable today ([17]). 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 ([18]) (essentially, all former 1st and 2nd 'pillar' ([19]) institutions, bodies, offices and agencies), but would not, as such, affect the existing or pending 'standalone' regimes ([20]). 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') ([21]), 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 ([22]). 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.

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

([17]) 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

([18]) See the list of EU institutions and bodies available at: http://publications.europa.eu/code/en/en-390500.htm

([19]) Regulation (EC) No 45/2001 already today applies to, inter alia, the European Defence Agency, European Union Institute for Security Studies, and the European Union Satellite Centre.

([20]) Europol, Eurojust, EPPO, *supra* note 21.

([21]) 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').

([22]) Recitals 10-12 ePrivacy Directive.

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.

Giovanni BUTTARELLI

European Data Protection Supervisor