16 January 2024

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

# *Guidance for co-legislators on key elements of legislative Proposals*

Draft for public consultation

# EXECUTIVE SUMMARY

Article 42 of Regulation (EU) 2018/1725 requires the EDPS to be consulted on legislative and other Proposals with an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data. The purpose of this guidance is to offer practical advice to the Commission, European Parliament and Council on the main elements to consider with regards to legislative Proposals that imply the processing of personal data.

Any legislative proposal that implies the processing of personal data must comply with the Charter of Fundamental Rights of the European Union, including the right to respect for private and family life and the right to protection of personal data. Where the interference is serious, there is a greater need for clear and precise rules governing the scope and application of the measure as well as accompanying safeguards.

The EDPS considers that decisions on essential principles and modalities that impact fundamental rights should in principle be taken at the level of legislative proposals ('basic acts') so as to ensure that such decisions are taken within a full legislative procedure. When considering a legislative proposal that would entail the processing of personal data, the following key elements should therefore be carefully considered:

- whether the proposal defines the objective(s) and the purpose(s) of the processing in a manner that is specific, explicit and legitimate;
- whether the roles and responsibilities of actors involved in the processing of personal data are clearly defined;
- whether the necessity and proportionality of the proposed measures is clearly demonstrated;
- the categories of personal data that would be processed and the categories of data subjects concerned;
- the duration for which personal data would be processed;
- any disclosure of personal data to public authorities or third parties; and
- any restrictions to the rights of data subjects.

For legislative proposals that do not give rise to a serious interference, the EDPS considers that the categories of personal data, categories of data subjects concerned and storage duration can be defined either at the level of the basic act or (further) specified at the implementation stage through implementing and/or delegated acts.

The guidance included in this document is indicative of the approach taken by the EDPS in the majority of cases, having regard to his advisory practice to date. A case-by-case assessment remains necessary and different approaches may be called for in light of the specific subject matter or nature of the proposal. Finally, it should be noted that the guidance applies specifically to opinions delivered by the EDPS to the co-legislator and the Commission prior to the final adoption of legislative acts or delegated or implementing acts. It incorporates policy considerations and should not be considered as checklist for supervisory purposes, i.e. when the EDPS exercises his powers pursuant to Article 58 of Regulation (EU) 2018/1725.

# TABLE OF CONTENTS

# 1. INTRODUCTION

1. A proposed legislative or other measure that implies the processing of personal data must comply with primary EU law, and in particular with Articles 7 (respect for private and family life[1]) and Article 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union ("Charter").

2. Personal data may only be processed – not only by the State, but by any other actor – if the standards set out in paragraphs 2 and 3 of Article 8 of the Charter are met, i.e.

   (i) the processing is fair and lawful, for specified purposes;

   (ii) transparency is ensured by giving the individuals rights to access and rectification; and

   (iii) control by an independent authority is ensured.

3. Both Articles 7 and 8 of the Charter must be read in conjunction with Article 52(1) of the Charter[2], which allows limitations to fundamental rights, provided that such limitations:

   (i) be provided for by law;

   (ii) respect the "essence" of the right(s);

   (iii) genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others; and

   (iv) subject to the principle of proportionality, are necessary[3] [4].

4. The Court of Justice of the European Union ("CJEU") has held in the vast majority of the cases dealing with legislative acts that the processing of personal data limited both the right to the protection of personal data and the right for respect of private life[5]. The CJEU has also held that for the establishment of a limitation "*it does not matter whether the*

---

[1] *Article 7 generally corresponds to Article 8 of the European Convention on Human Rights (ECHR).*

[2] *With regard to the fundamental rights to privacy and data protection, see for example judgment of 8 April 2014, Joined Cases Digital Rights Ireland C-293/12 and Landesregierung, C-594/12, EU:C:2014:238.*

[3] *Article 52(1) follows Article 8(2) of the ECHR which establishes that there shall be no interference by a public authority with the exercise of the right to privacy except such as is in accordance with the law and if necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

[4] *See also the EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, and the EDPS Necessity toolkit on assessing the necessity of measures that limit the fundamental right to the protection of personal data.*

[5] *See for instance, judgment of 9 November 2010, Joined Cases Volker und Markus Schecke, C-92/09 and C-93/09, EU:C:2010:662, par. 55 and judgment of 24 November 2011, Joined Cases Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD), v Administración del Estado, C-468/10 and C-469/10, EU:C:2011:777, par. 41. The CJEU held only in one case that there was no limitation on the right to private life when the personal data related to salaries were processed by the employers for their original purpose, see judgment of 20 May 2003, Joined Cases Rechnungshof et al v. Österreichischer Rundfunk, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, par. 74.*

*information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way*"[6].

5. The requirements of Article 8 of the Charter are further reflected in various instruments of EU data protection law, in particular those adopted pursuant to Article 16 of the Treaty of the Functioning of the European Union, including the EUDPR, GDPR, Directive (EU) 2016/680[7] ("LED") and Directive 2002/58/EC[8] ("ePrivacy Directive")[9]. Compliance with Article 8 of the Charter should be assessed by specific reference to the system of safeguards laid down in those instruments[10]. These rules are the benchmark for the legislator, and any derogations from those rules should in general be avoided or, at the very least, appropriately justified[11].

6. As regards the processing of personal data that is deemed necessary for the fulfillment of a legal obligation and/or for the performance of a task carried out in the public interest or in the exercise of official authority entrusted to the controller, there must be a legal basis in Union or Member State law[12]. Such a legal basis must be **clear and precise** and its application must be **foreseeable** to persons subject to it[13].

7. Proposals that give rise to a serious interference with the fundamental rights to data protection and privacy should be distinguished from others. Where the interference is serious, there is a greater need for clear and precise rules governing the scope and application of the measure as well as accompanying safeguards. In other words: **the greater the interference entailed by the proposed act, the most robust and detailed the rules and the safeguards should be.**

8. Assessing the seriousness of the interference is also an integral part of the proportionality assessment, which involves measuring the seriousness of the interference with the fundamental rights to respect for private life and to the protection of personal data which that processing involves and to determine whether the importance of the objective of

---

[6] Österreichischer Rundfunk, note 5 and Digital Rights Ireland, note 2, par. 33; EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, p. 7.

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

[8] 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).

[9] The proposal for an ePrivacy Regulation is still pending.

[10] C. Docksey and G. Zanfir-Fortuna, "Article 16. Protection of Personal Data", in H.-J. Blanke and S. Mangiaeli (eds.), Treaty on the Functioning of the European Union - A commentary, Vol. I: Preamble, Articles 1-89, Springer, 2021, par. 10. For a discussion of a particular role that Article 16 TFEU, and by extension the GDPR, play in the EU legal order, see Advocate General Szpunar Opinion in Case C-33/22 Österreichische Datenschutzbehörde, at para. 63 et seq.

11 With regard to the CJEU case law developed in connection to Article 15 of the ePrivacy Directive (i.e. admitted derogations by MS law to the principle of confidentiality for objectives of general public interests), see Digital Rights Ireland, note 2; judgment of 21 December 2016, Joined Cases *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970; judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788; judgment of 6 October 2020, Joined Cases *La Quadrature du Net and Others*, C-511/18 and C-512/18, EU:C:2020:791; Opinion of 15 January 2020, *Ordre des barreaux francophones et germanophone and Others*, C-520/18, EU:C:2020:7; and judgment of 2 March 2021, *Prokuratuur*, C-746/18, EU:C:2021:152.

[12] Article 6(3) GDPR; Article 5(2) EUDPR and Article 8(1) LED.

[13] See also Recital 41 GDPR and Recital 23 EUDPR. These provisions complement the requirements of Article 7 and 8 of the Charter, as interpreted by the CJEU, according to which any interference must be be provided for by law which is clear, precise and foreseeable.

general interest pursued by the processing is proportionate to the seriousness of the interference[14].

## 2. ASSESSING THE SERIOUSNESS OF INTERFERENCE

9. The CJEU has advanced several criteria to determine the seriousness of an interference with the right to the protection of personal data and the right for respect of private life. In particular, it has considered the following elements as relevant when qualifying an interference as (particularly) serious or significant:

- Nature of the personal data at issue, in particular of any processing of special categories of data[15] or data which is otherwise sensitive[16];
- Nature of, and specific methods for, the processing of the data at issue, in particular of the number of persons having access to those data and the methods of accessing them[17];
- The ability to draw precise conclusions concerning the private lives of the individuals concerned (profiling)[18];
- The lack of awareness of the data processing on the part of the person concerned[19];
- Large-scale processing of personal data[20];
- The ability to monitor individuals' behaviour (likely to generate feeling of constant surveillance)[21];
- Public accessibility of the information[22];
- Likely adverse effect on other fundamental rights[23];
- Automated processing of data involving pre-established models and criteria[24].

---

[14] *Judgment of 1 August 2022, OT and the Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, par. 98. See Section 5.*
[15] *CJEU judgment of 24 September 2019, GC and Others (De-referencing of sensitive data), C136-17, EU:C:2019:773, par. 44; judgment of 25 January 2018, Bevándorlási és Állampolgársági Hivatal, C-473/16; EU:C:2018:36, par. 59-63; judgment of 22 June 2021, Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, par. 74-75.*
[16] *Judgment of the Court of 11 December 2019, Asociația de Proprietari bloc M5A-ScaraA; C-708/18, EU:C:2019:1064, par. 57-63; OT and the Vyriausioji tarnybinės etikos komisija, note 14, par. 99.*
[17] *OT and the Vyriausioji tarnybinės etikos komisija, note 14, par. 99.*
[18] *Ministerio Fiscal, note 9, par. 54-61; Tele2 Sverige and Watson and Others, note 11, par. 99; judgment of 5 April 2022, Commissioner of the Garda Síochána e.a, C-140/20; EU:C:2022:258, par. 44-45; judgment of 13 May 2014, Google Spain and Google, C 131/12, EU:C:2014:317, par. 80; Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, par. 128.*
[19] *Tele2 Sverige and Watson and Others, note 11 and Digital Rights Ireland, note 2.*
[20] *Digital Rights Ireland, note 2, and La Quadrature du Net and Others, note 111111.*
[21] *Digital Rights Ireland, note 2.*
[22] *Google Spain and Google, note 18; OT and the Vyriausioji tarnybinės etikos komisija, note 14, par. 99-105.*
[23] *La Quadrature du Net and Others, note 11.*
[24] *See Opinion 1/15 (EU-Canada PNR Agreement), note 18, and judgment of 21 June 2022, Ligue des droits humains v. Conseil des ministres, Case C-817/19, EU:C:2022:491, par. 194-195.*

10. The examples above are not exhaustive and a case by case assessment remains relevant. As a rule of thumb, the criteria developed by the WP29/EDPB to determine whether the processing is "likely to result to high risk" can (also) help to assess the seriousness of the interference (e.g. processing of special categories of data or data of a highly personal nature, matching or combining of datasets, etc.)[25]. In most cases, processing meeting two or more criteria should be considered as likely amounting to a serious interference.

11. The following sections provide an overview of **the main elements to consider with regards to a legislative or other measure that implies the processing of personal data**. When applying this "checklist" in practice, it is important to take into account whether the act is:

    (1) a basic legislative act (a Regulation or a Directive) ("Basic Act") or

    (2) an implementing or delegated act (Commission Implementing Decision, Commission Implementing Regulation, Commission Delegated Regulation,... ) ("Implementing or Delegated Act")[26]; or

    (3) a recommendation or proposal to the Council pursuant to Article 218 TFEU (i.e. agreements between the Union and third countries or international organisations).

12. In addition, it is important to keep in mind that the guidance provided in the following sections is **indicative** of the approach taken by the EDPS in the majority of cases, having regard to his advisory practice to date. That being said, a **case-by-case assessment remains necessary** and different approaches may be called for in light of the specific subject matter or nature of the proposal.

# 3. OBJECTIVE AND PURPOSE

13. The objective(s) and purpose(s) of the processing that would result from a legislative proposal should be **specified, explicit and legitimate**[27]. To make sure this is the case, the following questions should be considered:

    - Is the objective of the proposed measure *sufficiently clear*?
    - Is the purpose of the processing *explicitly and specifically described* in the enacting terms ("operative text") of the proposal?
    - If further processing is envisaged, is its purpose *compatible* with the original one?

---

[25] *See Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p. 9-11.*

[26] *For more information see also section 6.*

[27] *This is the so-called purpose limitation principle, currently set out in Article 5(1)(b) GDPR; Article 4(1)(b) EUDPR and Article 4(1)(b) LED. See also Article 72 (2) EUDPR, which requires that "Specific Union legal acts regulating processing within the scope of this Chapter shall specify at least the objectives of processing, (...) the purposes of the processing (...)." Similarly, Article 8(2) LED specifies that "Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, (...) and the purposes of the processing."*

14. To be considered "explicit", the purpose of the processing should be clearly specified in the Basic Act, by either:

    - explicitly indicating the purpose of the processing as such[28]; or

    - resulting unambiguously from the explicit wording of the proposal, provided that the wording does not leave any possible doubt regarding the purpose(s) for which the personal data may be processed[29].

15. **The purposes of the processing should be established in the enacting terms ("operative text") of the proposal of the Basic Act**. It is not sufficient that the purpose of the processing is only explicitly indicated in (or results unambiguously from) the Explanatory Memorandum or recitals accompanying the enacting terms of the proposal.

16. Processing for a purpose other than that for which the personal data have been collected is governed by Article 6(4) GDPR[30], Article 4 (2) and (3) and Article 9 LED and Article 6 EUDPR respectively and should be addressed accordingly.

17. An **Implementing or Delegated Act** should not introduce processing operations for a purpose which is not sufficiently supported by the Basic Act[31]. Where an Implementing or Delegated Act concerns the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, the Implementing or Delegated Act may provide *greater specificity* to the purpose of the processing (and should do so if the provisions of the Basic Act do not articulate the purpose(s) of the processing with sufficient precision). An Implementing or Delegated Act should not, however, introduce an entirely new or unrelated purpose.

*Example:* EDPS Opinion 1/2019 on two legislative proposals relating to combating VAT fraud

The Commission's proposals on the fight against VAT fraud in the context of "e-commerce" included recitals specifying the purpose of the processing operations envisaged by them. However, EDPS recommended specifying the purpose in the operative text of the Proposals to avoid any risk of function-creep and the use of information for other purposes, such as controlling purchase habits of the consumers.

[28] *For example by using wording: "personal data collected … shall be processed for the purpose of …" or similar wording to this effect.*
[29] *Article 6(3) GDPR explicitly states that when the processing of personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, the purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of par. 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. See also judgment of 24 February 2022, "SS" SIA v. Valsts ieņēmumu dienests, Case-175/20, EU:C:2022:124, par. 69.*
[30] *See also Article 25 EUDPR and Article 23 GDPR.*
[31] *When assessing whether the processing envisaged by a draft Implementing Act is sufficiently supported by the Basic Act, one should also take into account the nature of the interference with the rights to data protection and privacy. If the interference is serious, the scope and application of the measure (as well as the accompanying measures) should have already been clearly provided for in the Basic Act.*

# 4. ROLES AND RESPONSIBILITIES

## 4.1. Roles

18. Both the GDPR and EUDPR distinguish among different types of actors involved in the processing of personal data: controller, processor and joint controllers[32]. These concepts provide the very basis upon which responsibility for compliance with EU data protection law is allocated.

    - A **"controller"** is any entity[33] which, alone or jointly with others, determines the purposes and means of the processing of personal data[34].

    - Where two or more controllers jointly determine the purposes and means of processing, they shall be **joint controllers**[35].

    - A **"processor"** is defined as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller[36].

19. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law[37]. Although not explicitly confirmed by the GDPR, the LED or EUDPR, the EDPS considers that similar considerations apply in case of joint controllers and/or processors.

20. Ensuring clarity of the role of each actor involved in the processing of personal data is important to promote transparency of processing and the effective exercise of data subject rights. Moreover it is key to enable a determination of who will be responsible for what (see further section 4.2 below). Determining the role of controller from the outset also helps to avoid any possible problems of interpretation in assessing the role[38].

21. The EDPS recommends **assigning the role of controller already in the Basic Act whenever possible**[39] **and appropriate**. The same applies for any **joint controllers** or **processors** who may be involved in the processing (where applicable).

---

[32] *EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 (hereinafter the EDPS GLS on C/P) and EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (hereinafter the EDPB GLS on C/P). The LED contains the same distinction. However, no guidelines are available to date.*

[33] *Under the GDPR, the "entity" can be a "*natural or legal person, public authority, agency or other body*" (Article 4(7) GDPR). Under the EUDPR, an entity can be "*Union institution or body or the directorate-general or any other organisational entity*" (Article 3(8) EUDPR). Article 3(10) EUDPR defines Union institutions and bodies as "*the Union institutions, bodies, offices and agencies set up by, or on the basis of, the TEU, the TFEU or the Euratom Treaty*". Under the LED, a "*controller" shall be a "competent authority" (Article 3(8), as defined by Article 3 (7) LED.

[34] *Article 3(8) EUDPR; Article 4(7) GDPR and Article 3(8) LED.*

[35] *Article 28(1) EUDPR; Article 26(1) GDPR and Article 21 LED.*

[36] *Article 3(12) EUDPR; Article 4(8) GDPR and Article 3(9) LED.*

[37] *Article 3(8) EUDPR; Article 4(7) GDPR and Article 3(8) LED.*

[38] *EDPS GLS on C/P, p. 8.*

[39] *Where it is not possible to do so (e.g., the Basic Act has already been adopted), the designation can also be done by way of an Implementing or Delegated Act.*

22. When a proposal establishes a legal obligation or a task in the public interest that requires processing of personal data involving multiple actors (e.g., a proposal requiring exchange of personal data between national public authorities an EU bodies, a provision that requires setting up a common repository at EU level, etc.), the proposal should as a rule identify the roles of the entities that will be involved in the processing.

NB: the designation of an entity as controller, joint controller or processor should take place in the enacting terms ("operative text") of the proposal rather than in the recitals accompanying the enacting terms of the proposal.

*Example:* EDPS Formal comments on the Proposal for a Regulation of the European Parliament and of the Council establishing a collaboration platform to support the functioning of Joint Investigation Teams and amending Regulation (EU) 2018/1726.

The Proposal for a Regulation establishing a collaboration platform to support the functioning of Joint Investigation Teams specified that the competent national and Union authorities shall be considered as "controllers" with regard to the processing of personal data in the platform. To avoid ambiguity, the EDPS recommended to clarify whether the identified controllers should be considered as "joint controllers" and, if so, to provide for the arrangement envisaged by Article 21 LED. While detailed arrangements to ensure compliance with data protection requirements may be further defined by way of an implementing act if necessary, the EDPS considered that the Proposal should in any case unambiguously identify the roles of each entity involved as controller, joint controller or processor respectively.

## 4.2. Responsibilities

23. The GDPR, the LED and EUDPR each require controllers, joint controllers and/or processors to clearly establish their respective obligations. When a proposal establishes a legal obligation or a task in the public interest that entails processing of personal data involving joint controllers and/or processors, it may be appropriate to specify the respective obligations of the entities involved, possibly by way of a Delegated or Implementing Act.

### *a) Joint controllers*

24. Joint controllers are obliged to determine the respective responsibilities for compliance with their data protection obligations by means of an arrangement between them, in particular as regards the exercising of the rights of the data subject and their respective duties.

25. The arrangement between joint controllers may take the form of an Implementing or Delegated Act, but may of course also be included in the Basic Act (e.g. in the form of an Annex). While detailed arrangements to ensure compliance with data protection requirements may be further defined by way of an Implementing or Delegated act, it may be appropriate to also include certain elements and safeguards in the Basic Act itself, taking into account the nature of the interference.

*Example:* EDPS Formal comments on a Proposal for a Regulation of the European Parliament and of the Council establishing the European Union Single Window Environment for Customs and amending Regulation (EU) No 952/2013

The Proposal for a Regulation establishing the European Union Single Window Environment for Customs and amending Regulation (EU) No 952/2013 specified that the Commission shall be a joint controller within the meaning of Article 28(1) EUDPR and customs authorities and partner competent authorities shall be joint controllers within the meaning of Article 26(1) GDPR. The EDPS welcomed that Article 7(3) of the Proposal provided for a minimum list of responsibilities by the joint controllers to ensure that the joint processing is compliant and that implementing acts would provide for a joint controllership arrangement.

26. Additional recommendations concerning the elements to be addressed by the joint controller arrangement (e.g. handling of requests and informing data subjects, management of security incidents...) can be found in the EDPS and EDPB guidelines[40].

27. If the Basic Act itself does not provide for a comprehensive arrangement, an empowering provision (i.e. a provision of the Basic Act empowering the European Commission to adopt implementing or delegated Acts) may be useful[41].

### *b) Processor(s)*

28. Where the processing is to be carried out on behalf of a controller, it shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller[42].

29. The LED, the EUDPR and GDPR specify additional elements that must be incorporated in the legal act between the controller and processor[43].

30. The legal act that is binding on the processor with regard to the controller may take the form of an Implementing or Delegated Act, but may of course be included in the Basic Act (e.g. in the form of an Annex). If the Basic Act itself does not yet address all the required elements, an empowering provision may be useful[44].

---

[40] *See in particular at pages 27 and 28 of EDPS GLS on C/P and par. 162 onwards of EDPB GLS on C/P.*
[41] *It should be recalled that the obligation for joint controllers to put in place an arrangement in any event exists by virtue of direct applicability of the GDPR, EUDPR or LED, so including an empowering provision is not a legal requirement and may not be appropriate in all cases.*
[42] *Article 29(3) EUDPR; Article 28(3) GDPR and Article 22(3) LED.*
[43] *See further also at page 19 of the EDPS GLS on C/P and par. 113 onwards of EDPB GLS on C/P.*
[44] *It should be recalled that the obligation put in place a contract or legal act that is binding on the processor with regard to the controller in any event exists by virtue of direct applicability of the GDPR, EUDPR or LED, so including an empowering provision is not a legal requirement and may not be appropriate in all cases.*

# 5. NECESSITY AND PROPORTIONALITY

31. A limitation of the exercise of a fundamental right guaranteed by Charter must, in addition to being "provided by law", also satisfy the requirements of necessity and proportionality. The criteria provided under Article 52(1) of the Charter and Article 8(2) ECHR for a lawful limitation on the right to the respect for private life are similar in this regard[45].

32. First, it must be established that the measure is intended to meet objectives of general interest recognised by the European Union, within the meaning of Article 52(1) of the Charter. If that is the case, it should first be determined whether the envisaged measure is appropriate, i.e. is capable of attaining the objective pursued. Very often, this is not a difficult test to pass[46].

33. Second, the measure should be **necessary** to achieve these objectives. The necessity test involves determining whether the objective of general interest pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects[47]. In this regard, it should be noted that case law of the CJEU applies a strict necessity test for any limitations on the exercise of the rights to personal data protection and respect for private life with regard to the processing of personal data[48].

34. Once it is established that the envisaged measure may be considered as "necessary", the next step is to assess its **proportionality in the strict sense**. Assessing proportionality in the strict sense involves assessing the seriousness of the interference with the fundamental rights to respect for private life and to the protection of personal data and determining whether the importance of the objective of general interest pursued by the processing is proportionate to the seriousness of the interference. An objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue[49].

35. In order to assess the seriousness of that interference, account must be taken, inter alia, of the nature of the personal data at issue, in particular of any sensitivity of those data, and

---

[45] *According to Article 52(3) of the Charter, the rights contained therein which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by that Convention. Consequently, as recalled by the CJEU in* La Quadrature du Net and others*, note11, par. 124, the jurisprudence of the ECtHR concerning rights which are also foreseen in the Charter must be taken into account, as a minimum threshold of protection to interpret corresponding rights in the Charter. According to the last sentence of Article 52(3) of the Charter, however, "[t]his provision shall not prevent Union law providing more extensive protection".*

[46] *See however also the judgment of 22 June 2021,* Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504, par. 114 (where the Court it is even questionable whether the legislation at issue in the main proceedings is appropriate for achieving the aim it pursues).*

[47] OT and the Vyriausioji tarnybinės etikos komisija*, note 14, par. 85. Establishing necessity implies establishing the "suitability" of the envisaged measure: if the measure cannot be considered as reasonably effective to achieve its objective, it also cannot be considered as necessary.*

[48] *Judgment of 16 December 2008,* Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy.*, C-73/07, EU:C:2008:727, par. 56,* Volker und Markus Schecke*, note6, par. 77 and 86. Within these constraints, the EU legislator remains free to make political choices. However, judicial review of any exercise of that discretion is likely to be particularly strict in the context of mass data processing affecting a very large number of persons, as well as the access to and use of such data by law enforcement authorities. See in particular,* Digital Rights Ireland*, note 2, par. 57-61,* Tele2 Sverige and Watson and others*, note 9, judgment of 6 October 2020,* Privacy International*, C-623-17, EU:C:2020:790,* La Quadrature du net and others*, note 11 and judgment of 5 April 2022,* G.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, ECLI:EU:C:2022:258, par.52.*

[49] *See also* G.D. v The Commissioner of the Garda Síochána and Others*, note 48, par. 52-53 and* La Quadrature du Net and others*, note 11, par. 130 -131.*

of the nature of, and specific methods for, the processing of the data at issue, in particular of the number of persons having access to those data and the methods of accessing them[50].

36. Once the seriousness of the inference has been determined, it should be assessed whether a fair balance has been struck between the importance of the objectives of general interest pursued and the individuals' fundamental rights to privacy and data protection. Taking into account safeguards that reduce the risks to the rights and freedoms individuals forms an integral part of this assessment.

37. It should be noted that the case law of the CJEU often integrates considerations of clarity and foreseeability ("quality of law") when assessing the necessity and proportionality of legislation.

38. For example, in order to satisfy the requirement of proportionality, the CJEU considers that *"the legislation must down clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted thereby ensuring that the interference is limited to what is strictly necessary"*[51].

39. As further clarified by the CJEU, the need for such safeguards is all the greater where personal data is subjected to automated processing and where the protection of the particular category of personal data that is sensitive data is at stake.

40. Given the crucial importance of necessity and strict proportionality to data protection, the EDPS published Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit and Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. See also the EDPS quick-guide to necessity and proportionality.

41. The following questions can additionally help to guide the assessment of necessity and proportionality:

    - Are the rules governing the scope and application of the measure **sufficiently clear and precise**? Is there sufficient legal clarity and certainty about the **scope and extent of the interference** (e.g., in terms of definitions, processing activities, actors involved etc.)?

    - Is it explicitly specified **what categories of data** will be collected or exchanged **by whom, and for how long**?

    - Is the data processing envisaged by the measure **adequate, relevant and not excessive** in relation to the purposes for which they are collected or further processed?

[50] OT and the Vyriausioji tarnybinės etikos komisija, *note14, par. 98 and following. See also section 2 above.*
[51] Ligue des droits humains v. Conseil des ministres, *note 24, para. 132.*

- Could any other, **less intrusive measure** achieve the desired outcome with less interference with the fundamental right at stake[52]?

- Are there any specific concerns related to processing of **sensitive data**, such as biometric data, health data, traffic and location data, criminal records, etc. or the **categories of data subjects** concerned (e.g., vulnerable persons)?

- Are there any specific concerns related to the use of **automated decision-making, profiling, or new technologies** like Artificial Intelligence[53]?

- Where a measure aims at protecting other public interests or fundamental rights, how are those **interests or rights balanced** with privacy and data protection[54]? Which **safeguards** are in place to reduce the risks to the rights and freedoms individuals?

*Example:* EDPS Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation ("Prüm II")

The European Commission adopted a Proposal for a Regulation on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council (the so-called "Prüm Decisions").

The EDPS noted that the proposed new Prüm framework does not clearly lay down essential elements of the exchange of data, such as the types of crimes, which may justify a query, and is not sufficiently clear about the scope of data subjects affected by the automatic exchange of data, e.g. whether the databases, subject to a query, contain data only of suspects and/or convicted persons, or also data of other data subjects, such as victims or witnesses.

The EDPS considered in particular that the automated searching of DNA profiles and facial images should be possible only in the context of individual investigations into serious crimes, instead of any criminal offence, as provided for in the Proposal. Furthermore, the EDPS considered it necessary to introduce in the Proposal common requirements and conditions concerning the data in the national databases that are made accessible for automated searches, taking due account of the obligation under Article 6 of the Law Enforcement Directive 680/2016 (LED) to make a distinction between different categories of data subjects (i.e. convicted criminals, suspects, victims, etc.).

The EDPS also considered that the necessity of the proposed automated searching and exchange of police records data was not sufficiently demonstrated. If such a measure is nevertheless adopted, even on voluntary basis, then additional strong safeguards would be required to comply with the principle of proportionality. In particular, given the data quality challenges, the future Regulation should, inter alia, explicitly define the types and/or the seriousness of crimes that may justify an automated query in the national police records.

[52] Volker und Markus Schecke, *note 6, par. 81.*
[53] Ligue des droits humains v. Conseil des ministres, *note 24, par. 194-195.*
[54] *For instance, in the area of law enforcement, the CJEU stated in* Ministerio Fiscal, *note11, par. 56-61, that, in accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as "serious".*

42. Without being exhaustive, the following subsections will highlight **specific points of attention** that should be considered when assessing whether a proposed measure complies with the requirements of necessity and proportionality, in particular as regards:

    (i) the categories of personal data concerned;

    (ii) the categories and the number of data subjects concerned;

    (iii) the duration of storage;

    (iv) disclosure of personal data to public authorities or third parties; and

    (v) restrictions the rights of data subjects.

## 5.1. (Categories of) personal data

43. The EDPS considers that the Basic Act should specify the (categories of) personal data in a comprehensive manner, especially if the proposal is likely to entail a serious interference with the rights to data protection and privacy[55]. In some cases, the specification of the personal data to be processed stems from an explicit **legal obligation**[56].

44. When a proposal specifies (the categories of) personal data involved, it should be ensured that the specified categories of data are **necessary and proportionate** to the objective pursued.

45. Where a proposal envisages processing of **special categories of personal data** or **personal data relating to criminal convictions and offences**, it should additionally be ensured that the conditions of Article 9-10 GDPR, Article 10-11 EUDPR and/or Article 10 LED are met.

46. Where the proposal specifies the categories of personal data involved, these categories should in principle be described in an **exhaustive manner**:

    - Open-ended formulations (e.g., "any other relevant data", "at least", ...) should be avoided;

    - Only more detailed data fields (sub-categories of data) falling under the already defined categories of data should be added through the adoption of Implementing or Delegated acts (the introduction of entirely new data categories by way of implementing act should be avoided, especially if the processing would constitute a serious interference with the rights and freedoms of individuals).

[55] *See also Article 25(2)(b) EUDPR and Article 23(2)(b) GDPR.*

[56] *See for instance Article 72 (2) EUDPR, which requires that "*Specific Union legal acts regulating processing within the scope of this Chapter shall specify at least the (...) **operational personal data to be processed**, (...)."*Similarly, Article 8(2) LED specifies that "*Member State law regulating processing within the scope of this Directive shall specify at least the (...) **personal data to be processed**, (...)."*

*Example:* EDPS Opinion 3/2022 on the Proposal for amending the Directive on the framework for the deployment of Intelligent Transport Systems in the field of road transport

The Proposal to amend the ITS Directive would empower the Commission to adopt specifications laying down the categories of traffic, travel or road that are personal data. In its opinion, the EDPS considered that the categories of personal data as well as the purposes for the processing of personal data in the context of the deployment of ITS services should be specified directly in the Proposal. The EDPS recognised that given the diversity of ITS and the variety of potential use cases, it could not be possible to fully detail each possible data category. However, only more detailed data fields (sub-categories of data) falling under the already defined categories of data should be added through the adoption of delegated acts. Moreover, the EDPS underlined that the purposes for which the categories of personal data may be processed should be clearly set out in the Proposal itself.

## 5.2. Categories of data subjects

47. Where the proposal entails a serious interference with the rights to data protection and privacy, the categories of data subjects should be specified in the Basic Act or appear unambiguously from the text.

48. In any event, it should be verified that the categories of data subjects affected appear as necessary and proportionate to the objective pursued.

*Example:* EDPS Formal comments on a Proposal for a Commission Implementing Decision amending Implementing Decision (EU) 2017/253 as regards alerts triggered by serious cross-border threats to health and for the contact tracing of passengers identified through Passenger Locator Forms.

The comments concerned the draft Commission Implementing Decision amending Implementing Decision (EU) 2017/253 as regards alerts triggered by serious cross-border threats to health and for the contact tracing of passengers identified through Passenger Locator Forms (PLF). While Recital 16 of the draft Implementing Decision referred to the processing of personal data of "cross-border passengers", Recital 17 stated that the processing of personal data would concern "infected passengers". From the draft Implementing Decision, the EDPS understood that all cross-border passengers' data would be processed and transmitted within the PLF exchange platform. Thus, the EDPS recommended explicitly clarifying in the aforementioned recitals whether the categories of data subjects would be limited to infected passengers only or might also concern other cross-border passengers for the purpose of SARS-CoV-2 contact tracing.

## 5.3. Storage duration

49. According to the storage limitation principle, the GDPR, EUDPR and the LED[57] provide for personal data to be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".

50. In accordance with the CJEU case law[58], the determination of a storage duration must be based on objective criteria. Different storage duration should be set for the different categories of data stored "on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned"[59].

51. Despite the objective nature of the determination of storage duration periods, in practice the legislator enjoys a certain margin of appreciation in defining an appropriate retention period, because no mathematical formula can determine with absolute precision the duration of storage which is necessary to achieve a given objective. Thus, **the defined period must be reasonably defined, having regard to the purposes of the processing.** The period of time should be closely put in relation to the purpose pursued and must be justified so as to ensure that the storage is limited to what is strictly necessary for the purposes pursued, and in practice it should be as short as possible. Sufficient evidence should be produced to that effect, for example by including the necessary justification in the impact assessment accompanying the proposal.

52. When assessing the relevance of the storage, attention should be drawn on whether the data stored could become outdated and irrelevant to serve the purposes (such as health data stored for public health purposes). Where the level of quality of the stored data cannot be ensured during the same length of time, it is **recommended to evaluate if a shorter data storage duration would be more suitable.**

53. The envisaged storage duration should be **specified unambiguously**. The mere reference to the deletion of data when "no longer required" is not sufficient to ensure consistency and legal certainty.[60] A storage duration may be specified:

    - by indicating the *exact* number of months/years for which the data shall be retained (e.g., "for five years");

---

[57] *Article 4(1)(e) EUDPR; Article 5(1)(e) GDPR and Article (4)(1)(e) LED. Article 72 (2) EUDPR explicitly requires that "Specific Union legal acts regulating processing within the scope of this Chapter shall specify at least the (...) time limits for storage of the operational personal data or for periodic review of the need for further storage of the operational personal data." Article 5 LED explicitly requires Member States to provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. See also Article 25(2)(f) EUDPR and Article 23(2)(f) GDPR.*

[58] Digital Rights Ireland, *note 2, par. 64.*

[59] Digital Rights Ireland, *note 2, par. 63.*

[60] *In the EDPS Opinion on the Commission proposal for a Directive of the European Parliament and of the Council amending Directive 2005/36/EC on the recognition of professional qualifications and Regulation [...] on administrative cooperation through the Internal Market Information System, the EDPS stated that "*[t]he proposed reference to deletion when 'no longer required' is helpful but — in our view — not sufficient to ensure consistency and legal certainty. The EDPS therefore recommends that the Proposal specify a sufficiently short retention period for the information exchanged.*" (par. 39) "*Alternatively, if legislators opt for 'long-term' storage in the IMI-file of the prohibition, the EDPS recommends that the Proposal should, at a minimum, clearly require that the issuing authority deletes any reference to the prohibition once the prohibition is no longer in effect (for instance, as the result of an appeal or because the prohibition was limited in time).*" *(par. 41).*

- by indicating the *maximum* number of months/years for which the data may be retained, provided that it does not prejudice the application of the general principle of storage limitation (e.g., "no longer than necessary for the purpose of XYZ and in any event no longer than five years");

- alternatively, in particular in the context of the LED, indicating the time period (months/years) for conducting a periodic review of the need for further storage of the personal data.

54. Where the proposal entails a serious interference with the rights data protection and privacy, the storage duration of the personal data should be specified in the Basic Act. While the criteria allowing the determination of the storage duration shall be laid down in the basic act, the concrete duration may be further defined by Implementing or Delegated Acts, on the basis of these objective criteria.

*Example:* EDPS Formal comments on a proposal for a Regulation establishing a European single access point (ESAP) providing centralised access to publicly available information of relevance to financial services, capital markets and sustainability

The Proposal determined that information referred to in Article 1(1) thereof remained available to the European single access point (ESAP) for at least 10 years, unless it was stated otherwise in the relevant legal act that required the information to be made public. In terms of personal data, it should not be retained and made available for longer than 5 years, unless stated otherwise in the relevant legal act. Finally, the Proposal specified that the collection bodies shall take appropriate technical and organisational measures to ensure that the information is not retained or made available for longer than provided for in Article 5(1)(f).

The EDPS welcomed the introduction of a clear maximum duration for the storage of personal data by the collection bodies. He regretted, however, that neither the Proposal nor the explanatory memorandum provided objective reasons for justifying the established duration. In order to avoid interpreting the Proposal as defining by default "the period necessary" under certain existing acts as 5 years and thus potentially leading to an extension of the maximum storage periods beyond the period necessary, the EDPS recommended specifying that the collection bodies must ensure that personal data submitted to them "shall not be retained and made available for longer than necessary and in any event not for longer than 5 years, unless stated otherwise in the legal acts referred to in Article 1(1), point (a)" of the Proposal.

## 5.4. Disclosure of personal data to public authorities or third parties

55. The GDPR, EUDPR and the LED[61] require personal data to be collected for specified purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation). If a proposal foresees **access of the competent national authorities**

[61] *Article 4(1)(b) EUDPR; Article 5(1)(b) GDPR and Article (4)(2) and (3) and Article 9 LED.*

to the data processed, such access constitutes a further interference with the fundamental right to respect for private life.[62]

56. Each time a proposal entails the sharing of data with public authorities or third parties, it should be clearly specified[63]. Any legislative measure authorising the exchange, communication or access to personal data by third parties should **clearly designate the third parties who may have such access or to whom the data may be communicated**, as well as the **purpose** for which the data shall be disclosed.

57. The public authorities or third parties to whom the personal data shall be disclosed must be specified in the Basic Act. An Implementing or Delegated Act may not introduce a new disclosure of personal data to a public authority or third party which is not sufficiently supported by the Basic Act[64].

58. The legislative act should lay down **objective criteria** in order to define the **circumstances and conditions** under which the competent national authorities are to be granted access to the data at issue[65] and by which to determine the limits of data sharing with the public authorities and their subsequent use. It should also specify **the substantive and procedural conditions** relating to such sharing and subsequent use. In particular, the legislation providing for access by competent authorities should:

    - **impose minimum safeguards**, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse.

    - be **legally binding under domestic law** and,

    - in particular, must indicate in **what circumstances and under which conditions a measure providing for the processing of such data may be adopted**, thereby ensuring that the interference is limited to what is strictly necessary[66].

*Example:* EDPS Opinion 1/2021 on the Proposal for a Digital Services Act

Article 21 of the Proposal for a Digital Services Act required online platforms to promptly inform the law enforcement or judicial authorities as they become aware of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place.

---

[62] *As regards Article 8 of the ECHR, see judgement of 26 March 1987, Leander v. Sweden, no. 9248/81, CE:ECHR:1987:0326JUD000924881, par. 48; judgement of 4 May 2000, Rotaru v. Romania [GC], no. 28341/95, CE:ECHR:2000:0504JUD002834195, par. 46 and judgement of 29 June 2006, Weber and Saravia v. Germany no. 54934/00, CE:ECHR:2006:0629DEC005493400, par. 79. For Article 7 of the Charter, see CJEU, Digital Rights Ireland, note 2, par. 35.*

[63] *The legislation providing for the exchange or communication of data may be the one on which the third parties base themselves to process the data in question.*

[64] *It is not excluded, however, that an implementing or delegated act identifies more specially the relevant entities to whom the personal data shall be disclosed, provided the disclosure is authorised by the Basic Act (e.g., the Basic Act makes reference to "the competent authority in the Member States" and the Implementing or Delegated Act establishes a list of the specific authorities in question).*

[65] Tele2 Sverige and Watson and *others*, *note 11, par. 119 and the case law cited.*

[66] Digital Rights Ireland, *note 2 and* « SS » SIA v. Valsts ieņēmumu dienests, *note 29, par. 83-84.*

In his opinion, the EDPS welcomed the delineation of the criminal offences which may give rise to a reporting obligation, i.e. "serious criminal offences involving a threat to the life or safety of persons". However, the EDPS recommended further specifying, by listing in an Annex, any other criminal offences (other than child sexual abuse mentioned in Recital 48) that meets this threshold and may give rise to a notification obligation, as well as clearly defining what "relevant information" is in order to ensure legal certainty for all parties involved, including the platforms themselves.

## 5.5. Disclosure of personal data involving international transfers

59. Where a proposal indicates that there may be **international transfers** of personal data to third countries, due regard should also be given to the conditions for transfers pursuant of Chapter V GDPR, Chapter V and Article 94 EUDPR and Chapter V LED.

60. Furthermore, it should be borne in mind that most of the legal acts establishing Union large-scale IT systems in the field of the JHA lay down a prohibition of the transfer of the data stored in them to third countries or international organisations, with some clearly defined exceptions[67].

## 5.6. Restrictions on data subject rights

61. Where the proposed legislative act entails restrictions on data subject, such restriction must comply with the criteria above laid down in **Article 52(1) of the Charter**. In addition:

    - Restrictions **by EUIs** are regulated under **Article 25 EUDPR**: any restriction has to be either based on a legal act adopted on the basis of the Treaties or, in the absence of such legal basis, in matters relating to the operation of EUIs, on the internal rules of the EUIs.

    - Restrictions **at Member States level** are regulated under **Article 23 GDPR** and **Articles 13(3)** and **15 LED**.

62. Any restrictions under the GDPR and the LED must be provided for by law, which implies, in particular, that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned. It shall be clear, precise and its application foreseeable to the persons whose personal data is affected. This means that the latter shall be able to identify the circumstances and conditions of such restrictions[68].

63. For more information on restrictions under Article 25 EUDPR and Article 23 GDPR, see EDPS Guidance on Article 25 of Regulation 2018/1725 and EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR.

[67] *See for example Article 65 of Regulation (EU) 2018/1862 (SIS), Article 31 of Regulation (EC) No 767/2008 (VIS), Article 41 of Regulation (EU) 2017/2226 (EES), Article 65 of Regulation (EU) 2018/1240 (ETIAS) and others.*
[68] « SS » SIA v. Valsts ieņēmumu dienests, *note 29, par. 52 onwards, in relation to the GDPR.*

# 6. BASIC ACTS VS, IMPLEMENTING OR DELEGATED ACTS

64. When assessing a proposal that would entail the processing of personal data, it is very important to bear in mind whether the proposed act is a Basic Act or an Implementing or Delegated Act[69].

65. A significant number of consultations under Article 42(1) EUDPR concern draft Implementing or Delegated acts (Articles 290 and 291 TFEU). Many of these acts are technical in nature and are often interrelated (e.g. several implementing and/or delegated acts may define specific aspects and functionalities of the same large-scale IT system).

66. Article 290 TFEU specifies that the "**essential elements**" of an area shall be reserved for the legislative act (i.e. the Basic Act). The CJEU has further clarified that "essential elements" of basic legislation are those which, in order to be adopted, require political choices falling within the responsibilities of the EU legislature[70]. For example, the adoption of rules requiring conflicting interests at issue to be weighed up on the basis of a number of assessments, may not be conferred on the Commission[71]. When it exercises delegated or implementing powers, the Commission must fully respect the essential elements of the enabling act[72].

67. In accordance with the GDPR, the legal basis for the processing does not necessarily require a legislative act adopted by a parliament[73]. Nevertheless, the EDPS considers that decisions on essential principles and modalities that impact fundamental rights should be taken at the level of the Basic Act so as to ensure that such decisions are taken within a full legislative procedure, which ensures more democratic control and includes the appropriate checks and balances[74]. Decisions that have a major impact on the privacy and data protection of individuals **should be decided by European Parliament and Council, particularly for proposals that may entail a serious interference with data protection and privacy rights**.

---

[69] *Additional information on Implementing and Delegated Acts can be found at https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?spaceKey=REGISTRY&title=Comitology. See also 'Understanding delegated and implementing acts', EPRS briefing, July 2021.*

[70] *Judgment of 11 May 2017, Dyson v Commission, C-44/16 P, EU:C:2017:357, par. 61.*

[71] *Judgment of 5 September 2012, Parliament v Council, C-355/10, EU:C:2012:516, par. 64, 65 and 76; judgment of 26 July 2017, Czech Republic v Commission, C-696/15 P, EU:C:2017:595, par. 78;* Dyson v Commission, *note70, par. 61 and 62.*

[72] Dyson v Commission, *note70, par. 65. See also Council Non-Binding Criteria for the application of Articles 290 and 291 of the Treaty on the Functioning of the European Union — 18 June 2019.*

[73] *Recital 41 GDPR. On the notion of "provided for by law" under Article 52(1) of the of the Charter, the criteria developed by the ECtHR should be used as suggested in several CJEU Advocates General Opinions, see for example the Opinions in* Tele2 Sverige and Watson and Others, *Joined Cases C-203/15 and C-698/15, EU:C:2016:572, par. 137-154 and the Opinion of Advocate General of 14 April 2022,* Scarlet Extended, *C-70/10, EU:C:2011:255, par. 88- 114. Hence, reference can be made, among others, to the ECtHR ruling in* Weber and Saravia v Germany, *note62, par. 84: "The Court reiterates that the expression "in accordance with the law" within the meaning of Article 8 § 2 [of the ECHR] requires, firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law." See also judgment of 27 April 2022 from the General Court,* Robert Roos v. European Parliament, *Joined Cases T-710/21, T-722/21 et T-723/21, EU:T:2022:262, par. 64 onwards.*

[74] *Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, par. 24.*

68. If the proposal concerns a Basic Act which does not entail a serious interference with the right to data protection, the EDPS considers that it is possible to delegate the determination of certain modalities of the processing to the Commission (for more details see the table under section 8)[75]. If the proposal does not provide for any Implementing or Delegated Act, however, the requisite safeguards will in any event need to be included in the Basic Act or an empowering provision should be added.

69. Since only very technical (practical) details should be left to be decided under the administrative autonomy of the EU body involved in the processing of personal data (e.g. by the Management Board of a decentralised Agency), explicit empowerment to administrative bodies to lay down provisions that regulate the interference with fundamental rights should be avoided, as this matter should be reserved to the legislator and, at most, to the Commission[76].

70. When dealing with a proposal for a Delegated or Implementing Act, it is also important to assess its legal basis and scope. In that regard, the following questions should be considered:

    - What would be the legal basis of the Implementing or Delegated Act?

    - Would the draft Implementing or Delegated Act be within the scope laid down in the basic act?

71. In addition, it is recommended to check whether there has been an EDPS Opinion on the Basic Act providing for the legislative delegation for the adoption of the Implementing or Delegated Act, or previous EDPS formal comments on related matters, e.g. formal comments on other implementing or delegated acts envisaged by the same Basic Act.

[75] *Needless to say, nothing prevents the legislator from introducing all the requisite safeguards in the Basic Act itself, even if the interference is not serious.*

[76] *As a result, empowerment provisions should in principle not extend to purely administrative decisions (e.g. decisions to be adopted by the board of directors of an EUI acting as controller).*

# 7. INTERFERENCES COMPLETED AT NATIONAL LEVEL

72. Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.

73. Especially when it comes to a Basic Act, it is important to consider whether Member States will further specify the interference or the details of its regime under their national law. Where this is the case, the details in the proposed act may be more limited than in case where the interference is governed exclusively (or primarily) by rules promulgated at EU level.

*Example:* EDPS Formal Comments on the Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence

The Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence aimed at establishing minimum rules concerning the definition of criminal offences and penalties in the areas of sexual exploitation of women, and children and computer crime. While the Proposal envisaged collection of personal data that may be deemed particularly sensitive, the processing of data would mainly taking place in the framework of the relevant criminal procedures and the rules on data protection transposed at national level from the LED.

74. Conversely, there may also be instances where a proposal envisages that Member States shall further specify the interference or the details of its regime under national law, whereas it would more appropriate to include additional elements directly in the proposal itself.

*Example:* Opinion 2/2023 on the Proposals for Directives on standards for equality bodies in the field of equal treatment

Two proposals for Directives on standards for equality bodies in the field of equal treatment envisaged that the choice of the legal basis for the processing of personal data by equality bodies should be left to the national transposition of the future directives. The EDPS recommended enhancing legal certainty for the equality bodies by considering Article 18 of the Proposals as the legal basis for the data processing and to make an explicit link to Article 9 GDPR with regard to special categories of personal data. He also recommended clarifying the scope of Article 18(1) of the Proposals to cover not only the collection but also the subsequent processing of personal data by equality bodies, as necessary, exhaustively listing all special categories of personal data within the meaning of the GDPR that may be processed on the basis of the Proposals as well as clarifying the suitable and specific measures to safeguard the fundamental rights and the interests of the data subject required in Article 9(2)(g) GDPR.

# 8. CHECKLIST PRIOR TO THE ADOPTION OF LEGISLATIVE ACTS OR DELEGATED OR IMPLEMENTING ACTS

*a) Elements to be found in the legal act where it does <u>not</u> constitute a serious interference with the rights to data protection and privacy of data subjects*

| (Essential) elements of the processing | In the EU basic act | In the implementing or delegated acts |
|---|---|---|
| Objective(s) and purpose(s) | Yes [but the purpose(s) may stem from the general economy of the act, if there is no ambiguity] | Additional specifications are possible provided that they comply with the purposes identified in the basic act (even if implicitly but surely). |
| Identification of the controller(s) | Yes [whenever possible/ appropriate] | Yes (if not already in the basic act and unless it would clearly exceed the delegation of powers) |
| (Categories of) processed personal data | Yes OR empowering provision<br><br>Not mandatory, unless explicitly provided for under secondary EU law[77] | Yes (if not already in the basic act and unless it would clearly exceed the delegation of powers) |
| Categories of data subjects | Yes OR empowering provision | Yes (if not already in the basic act and unless it would clearly exceed the delegation of powers) |

[77] *See section 5.1.*

*b) Elements to be found in the legal act where it constitutes a serious interference with the rights to data protection and privacy of data subjects*

| (Essential) elements of the processing | In the EU basic act | In the implementing or delegated acts |
|---|---|---|
| Objective(s) and purpose(s) | Yes [but the purpose(s) may stem from the general economy of the act, if there is no ambiguity] | No |
| Identification of the controller(s) | Yes [whenever possible/appropriate] | Yes (if not already in the basic act and unless it would clearly exceed the delegation of powers) |
| (Categories of) processed personal data | Yes | Depending on the intrusiveness of the measures, the Commission may receive the power to specify further the processed data. |
| Categories of data subjects | Yes [but the categories of data subjects can be deduced from other provisions of the act, provided that there is no ambiguity] | No |
| Max duration of the data storage or, at least, criteria for determining such duration | Yes | The Commission may be authorised to (further) determine the storage duration based on criteria defined by the legislators and to reduce the storage duration of data. |