EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data

19 December 2019

Table of Contents

I. The purpose of these Guidelines and how to use them

Fundamental rights, enshrined in the Charter of Fundamental Rights of the European Union (hereinafter, '**the Charter'**), form part of the **core values** of the European Union, which are also laid down in the Treaty on the European Union (hereinafter, 'TEU')[1]. Among these rights are the fundamental rights to privacy and the protection of personal data enshrined in Articles 7 and 8 of the Charter. These fundamental rights must be respected by EU institutions and bodies including when they design and implement new policies or adopt any new legislative measure. Other fundamental rights norms also play an influential role in the EU legal order, in particular those set out in the European Convention for the Protection of Human Rights and Freedoms (hereinafter, '**the ECHR'**)[2].

The **conditions for possible limitations** on the exercise of fundamental rights are among the most important features of the Charter because they determine **the extent to which the rights can effectively be enjoyed**[3].

The **necessity** and **proportionality** of a legislative measure entailing a limitation on the fundamental rights to privacy and the protection of personal data are an essential **dual requirement** with which any proposed measure that involves processing of personal data must comply. However, ensuring that **data protection** becomes an **integral part of EU policy-making** requires not only an understanding of the principles expressed in the legal framework and in the relevant case-law, but also a **practical and creative focus** on solutions to complex problems, with often competing policy priorities[4].

The **Court of Justice of the European Union** (hereinafter, 'the CJEU') has recognised that EU legislation is often required to meet **several public interest objectives** which may sometimes be contradictory and require a **fair balance** to be struck between the various public interests and fundamental rights protected by the EU legal order[5]. Such rights and interests, as

---

[1] Article 2 TEU states that "[t]he Union is founded on the values of respect for **human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities**". In addition, Article 6(1) TEU recognises the **rights, freedoms and principles set out in the Charter**, which has the same legal value as the treaties (emphasis supplied).

[2] Article 6(3) TEU states that "fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the **constitutional traditions common to the Member States**, shall constitute **general principles of the Union's law**" (emphasis supplied).

[3] Article 52(1) of the Charter states that "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

[4] See **Policy paper "EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience"**, 4 June 2014, available at: https://edps.europa.eu/data-protection/our-work/publications/papers/edps-advisor-eu-institutions-policy-and-legislation_en.

[5] Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI:EU:C:2008:54, para. 68. In joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, Advocate General Saugmandsgaard Øe explained in his Opinion, ECLI:EU:C:2016:572 para. 247, that "*[t]his requirement of proportionality within a democratic society - or proportionality stricto sensu- flows both from Article 15(1) of Directive 2002/58 and Article 52(1) of the Charter, as well as from settled case-law: it has been consistently held that a measure which interferes with fundamental rights may be regarded as proportionate only if the disadvantages caused are **not disproportionate** to the aims pursued*" (emphasis supplied). In para. 248 he also pointed out that the requirement of proportionality in this particular case of retention of large amount of data "*[o]pens a debate about the values that must prevail in a democratic society and, ultimately, about what kind of society we wish to live in*".

enshrined in the Charter, may include: the right to life (Article 2) and to the integrity of the person (Article 3); the right to liberty and security (Article 6); freedom of expression (Article 11); freedom to conduct a business (Article 16); the right to property, including intellectual property (Article 17); the right of access to documents (Article 42).

These Guidelines are intended to **help with the assessment of compliance** of proposed measures with EU law on data protection. They have been developed to better equip EU policymakers and legislators responsible for **preparing or scrutinising measures that involve the processing of personal data** and limit the rights to protection of personal data and to privacy. They aim at assisting policy makers and legislators, once they have identified the measures which have an impact on data protection and the priorities and objectives behind these measures, in finding solutions which minimise conflict between these priorities and are proportionate.

The EDPS would underline the responsibility of the legislator to assess the proportionality of a measure. The present Guidelines therefore do not intend to provide, nor can they provide, a definitive assessment as to whether any specific proposed measure might be deemed proportionate. Rather, they offer a **practical, step-by-step methodology** for assessing the proportionality of new legislative measures, providing explanations and concrete examples. They respond to requests from EU institutions for guidance on the particular requirements stemming from Article 52(1) of the Charter.

The Guidelines **complement** the EDPS Toolkit "Assessing the necessity of measures that limit the fundamental right to the protection of personal data" (hereinafter, '**the Necessity Toolkit**')[6] and deepen, with respect to the rights to privacy and to the protection of personal data[7], existing guidance produced by the European Commission, the Council of the EU and the European Union Agency for Fundamental Rights (hereinafter, 'FRA'), on the limitations of fundamental rights in general, concerning, for example, impact assessments and compatibility checks[8].

[6] EDPS, "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit", 11 April 2017, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[7] In these Guidelines, reference is often made to 'data protection' to refer both rights to **privacy** and to the **protection of personal data**. We point out however that these are distinct rights. On the difference between the two, see: https://edps.europa.eu/data-protection/data-protection_en.

[8] See European Commission **Tool#24** on **Fundamental Rights & Human Rights as part of the Better Regulation Toolbox**, available at: http://ec.europa.eu/smart-regulation/guidelines/tool_24_en.htm
and the more in depth analysis provided in **Commission Staff Working Paper**, **Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments**, SEC (2011) 567 final, available at: http://ec.europa.eu/smart-regulation/impact/key_docs/docs/sec_2011_0567_en.pdf.
See also **Council Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council preparatory bodies**, 5377/15, 20 January 2015, available at: https://www.consilium.europa.eu/media/30209/qc0214079enn.pdf
and **FRA Handbook** "**Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level"**, Guidance, May 2018, available at: http://fra.europa.eu/en/publication/2018/national-guidance-application-eu-charter.
These documents cover all fundamental rights, hence they also refer to several CJEU case-law examples relating to the rights enshrined in Articles 7 and 8 of the Charter.

The aim of these Guidelines is to explore in greater depth, and provide relevant examples of, issues relating to the impact on the fundamental rights to privacy and the protection of personal data, zooming in and complementing in particular **Tool#24** of the Commission **Better Regulation Toolbox** and the **Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments**.

The EDPS observes that, in recent years, the protection of personal data has gained momentum and is increasingly acknowledged as a dimension that must be considered by the legislator in all policy areas and for almost all Commission initiatives. This is not just due to an increased public awareness, but to the **greatly increased capacity of data processing** (which would have seemed harmless until recently) **to severely impact the life of each and every citizen**.

To facilitate the Commission's effort to take this key dimension into account, **proactively**, **already at the moment of the preparation of the Impact Assessment**, reference is also made, in the operational part of these guidelines, to the **terminology of the Commission Impact Assessment Methodology** (that is: ***Drivers; Causes; Problem Definition; Impact***).

The EDPS, also given the complexities and specificities of this exercise, **is committed and ready to assist the Commission services, including by contributing to the Impact Assessment work**, in providing a source of valuable information relating to data protection as fundamental right.

The Policy and Consultation Unit of the EDPS can be contacted on any questions on this guidance and on how to assess the impact on the fundamental rights to privacy and to the protection of personal data of legislative acts. For this purpose, you can contact the functional e-mail address of the Policy and Consultation Unit: POLICY-CONSULT@edps.europa.eu.

It is essential to highlight that **necessity and proportionality**, even though strictly linked to each other (both conditions must be fulfilled by the legislation), entail **two different tests**. This is made evident in section III of the present Guidelines presenting the practical step-by-step checklist for proportionality, whereby we provide the first holistic view of the **overall workflow.**

The Guidelines consist of an **introduction**, which sets out its content and purpose, a **legal analysis** of the proportionality test applied to the processing of personal data and a **practical step-by-step checklist** for assessing the proportionality of new legislative measures. The checklist is the core of the Guidelines and can be used autonomously.

The Guidelines are based on the **case-law**[9] of the CJEU, the European Court of Human Rights (hereinafter, 'the ECtHR'), Opinions of the EDPS and of the Article 29 Working Party (hereinafter, 'WP29') as well as on guidelines of the European Data Protection Board (hereinafter, 'the EDPB').

Together with the **Necessity Toolkit**, we seek with the Guidelines to provide for **a common approach to the assessment of necessity and proportionality** of legislative measures with respect to the right to privacy and to the protection of personal data.

II. Legal analysis: the proportionality test applied to the rights to privacy and to the protection of personal data

1. The **test of proportionality** in assessing the legality of any proposed measure involving processing of personal data

Article 8 of the Charter enshrines the fundamental **right to the protection of personal data**. The right is **not absolute** and **may be limited**, provided that the limitations comply with the requirements laid down in Article 52(1) of the Charter. The same analysis applies to the **right to respect for private life** enshrined in Article 7 of the Charter[10].

To be lawful, any limitation to the exercise of the fundamental rights protected by the Charter must comply with the following **criteria**, laid down in Article 52(1) of the Charter:

- it must be **provided for by law**,

[9] For an overview of the relevant **case-law** of the CJEU and ECtHR, see **FRA Handbook on European data protection Law**, 2018 edition, available at: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law.
See also the "Factsheet - Personal data protection", issued in September 2018 by the ECtHR, available at: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[10] In joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Hartmut Eifert*, Advocate General Sharpston explained in her Opinion, ECLI:EU:C:2010:353, para. 73, that *"[l]ike a number of the classic ECHR rights, the right to privacy is **not an absolute right**. Article 8(2) ECHR expressly recognises the possibility of exceptions to that right, as does Article 9 of Convention No 108 in respect of the right to protection of personal data. Article 52 of the Charter likewise sets out (in general terms) similar criteria that, if fulfilled, permit exceptions to (or derogation from) Charter rights*" (emphasis supplied). This approach was confirmed by the judgment of the CJEU, ECLI:EU:C:2010:662, paras 48-50.
On the right to the protection of personal data as 'not absolute', see Recital 4 of Regulation (EU) 2016/679 ('the General Data Protection Regulation', hereinafter, 'GDPR'): "The processing of personal data should be designed to serve mankind. The **right to the protection of personal data is not an absolute right**; it must be considered **in relation to its function in society** and **be balanced against other fundamental rights, in accordance with the principle of proportionality**" (emphasis supplied).
On the difference between **absolute rights** (such as the prohibition of torture and inhuman or degrading treatment or punishment as enshrined in Article 4 of the Charter) and **rights subject to limitations** (such as the right to privacy and to the protection of personal data), see Commission Staff Working Paper, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC (2011) 567 final, page 9 and FRA handbook "Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level", Guidance, May 2018, page 70.
An important consequence of this distinction is that **absolute rights cannot be limited and therefore are not subject to a balance with other rights or interests**. Hence, in cases where the **right to privacy concurs with** (goes in the same direction of) **an absolute right** (for example, the right not to be subject to torture), **both (concurring) rights will not be subject to balance** with other rights or interests (for example, national security).

- it must **respect the essence** of the rights,
- it must **genuinely meet objectives of general interest** recognised by the Union or the need to protect the rights and freedoms of others,
- it must be **necessary** - the focus of the Necessity Toolkit, and
- it must be **proportionate** - the focus of these Guidelines.

This list of **macro-criteria** sets out the required **order of the** lawfulness **assessment** of a limitation on the exercise of a fundamental right.

1. First it must be examined whether the law that provides for a limitation is **accessible and foreseeable**[11]**.** If this requirement is not satisfied, then the measure is unlawful and there is no need to proceed further with its analysis[12].

[11] Under Article 52(3) of the Charter, "[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection". On the notion of '**provided for by law**' under Article 52(1) 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 joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, paras. 137-154 and in case C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, paras. 88-114. Hence, reference can be made, among others, to the ECtHR ruling in *Weber and Saravia v Germany*, para. 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 Recital 41 of the GDPR: "Such [a legal basis or] legislative measure should be **clear** and **precise** and its application should be **foreseeable to persons subject** to it, in accordance with the case-law of the Court of Justice of the European Union (...) and the European Court of Human Rights" (emphasis supplied).
- On the notion of "**foreseeability**" in the context of **interception of communications,** see ECtHR case, *Zakharov v Russia*, para. 229: "The Court has held on several occasions that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures." (emphasis supplied) In the same sense, most recently, see *Big Brother Watch and others v United Kingdom*, ECtHR, 13 September 2018, para. 306.
- See also *Shimovolos v Russia* case, ECtHR, 21 June 2011.

[12] See ECtHR case, *Benedik v. Slovenia*, para. 132: "the Court is of the view that the law on which the contested measure, that is the obtaining by the police of subscriber information associated with the dynamic IP address in question (...), was based and the way it was applied by the domestic courts **lacked clarity** and did not offer sufficient safeguards against arbitrary interference with Article 8 rights. In these circumstances, the Court finds that the interference with the applicant's right to respect for his private life was **not 'in accordance with the law'** as required by Article 8 § 2 of the Convention. Consequently, the Court **need not examine whether the contested measure had a legitimate aim and was proportionate**" (emphasis supplied).
See also case *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk*, ECLI:EU:C:2003:294, paras 77-80; Opinion of the Advocate General in the PNR Canada Opinion 1/15, ECLI:EU:C:2017:592**,** paras 191-192: "*So far as the retention of personal data is concerned, it must be pointed out that the legislation in question must, inter alia, continue to satisfy objective criteria that establish a connection between the personal data to be retained and the objective pursued (see, to that effect, judgments of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 93, and of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15,*

2. Secondly, if the measure has passed the test of the quality of the law under point 1 above, it must be examined whether the **essence of the right** is respected, that is, whether the right is in effect **emptied** of its basic content and the individual cannot exercise the right. If the essence of the right is affected, the measure is unlawful and there is no need to proceed further with the assessment of its compatibility with the rules set in Article 52(1) of the Charter[13].

3. Third, it must be examined whether the measure meets an **objective of general interest**. The objective of general interest provides the **background** against which the necessity of the measure may be assessed. As explained in the Necessity Toolkit, it is therefore important to identify the objective of general interest in sufficient detail to allow the assessment as to whether the measure is necessary.

4. The following step consists of assessing the **necessity** of a proposed legislative measure which entails the processing of personal data (necessity test)[14].

5. If this test is satisfied, the **proportionality** of the envisaged measure must be examined (proportionality test). The concept of proportionality is a well-established legal concept under EU law. It is **a general principle of EU law** which requires that "*the content and form of Union action shall **not exceed what is necessary to achieve the objectives** of the*

---

*EU:C:2016:970, paragraph 110). As regards the use, by an authority, of legitimately retained personal data, it should be recalled that the Court has held that EU legislation cannot be limited to requiring that access to such data should be for one of the objectives pursued by that legislation, but must also **lay down the substantive and procedural conditions governing that use** (see, by analogy, judgment of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 117 and 118 and the case-law cited).*"

[13] While the case-law is not abundant regarding the conditions under which **the essence** of a right is affected, it may be argued that this would be the case **if the limitation goes so far that it empties the right of its core elements** and thus prevents the exercise of the right.

- In case **C-362/14**, *Schrems*, ECLI:EU:C:2015:650, paras 94 and 95, the CJEU found that **the essence of the right to respect for private life and the right to an effective remedy** were affected: "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (...). Likewise, legislation **not providing for any possibility for an individual to pursue legal remedies** in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, **does not respect the essence of the fundamental right to effective judicial protection**, as enshrined in Article 47 of the Charter*" (paras. 94 and 95) (emphasis supplied). The Court did not further elaborate whether such a limitation was necessary, and **invalidated** -also on other grounds- **the Commission's Decision** on the adequacy of the Safe Harbour Principles.

- In joined cases **C-293/12 and C-594/12,** *Digital Rights*, ECLI:EU:C:2014:238 para. 39 , the CJEU found that the **essence of the right *to respect for private life*** was **not affected** since the Data Retention Directive **did not allow the acquisition of knowledge *of the content*** of electronic communications (but only of 'metadata').

The CJEU similarly found that **the essence of the right to *the protection of personal data*** was not affected because the Data Retention Directive provided for the **basic rule that appropriate organisational and technical measures should be adopted against accidental or unlawful destruction, loss or alteration of the retained data** (paras. 39 and 40). Only following the assessment that the essence of the fundamental right at stake was not compromised did the Court proceed to examine **the necessity** of the measure.

- In joined cases **C-203/15 and C-698/15**, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, para. 123, the Court stated that the **deprivation of review**, by an independent authority, of compliance with the level of protection guaranteed by EU law could also **affect the essence of the right to the protection of personal data** as this is expressly required in Article 8(3) of the Charter and *"[i]f that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data*".

[14] For our analysis of the **necessity test**, see the EDPS Necessity Toolkit, available at: https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.

treaties"[15] (emphasis supplied). It is 'built upon' the constitutional traditions of several Member States[16].

Under Article 52(1) of the Charter, "subject to the principle of proportionality, limitations [on the exercise of fundamental rights] may be made only if they are necessary (...)". According to settled case-law of the CJEU, "*the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives*"[17]. Hence **proportionality in a broad sense** (as referred to by the CJEU) encompasses **both the necessity** and **the appropriateness** (**proportionality *in a narrow sense***) of a measure, that is, the extent to which there is a logical link between the measure and the (legitimate) objective pursued[18].

For a measure to respect the principle of proportionality enshrined in Article 52(1) of the Charter, **the advantages resulting from the measure should not be outweighed by the disadvantages** the measure causes with respect to the exercise of fundamental rights. It therefore "***restricts the authorities*** *in the exercise of their powers by requiring* ***a balance to be struck*** *between the* ***means*** *used and* ***the intended aim (or result reached)***"[19].

Indeed, in the *Digital Rights* judgment[20], the CJEU has ruled that the **discretionary power of the legislator** is reduced when restricting fundamental rights: "*where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference*"[21]. Replying in substance to the

[15] See Article 5(4) TEU.

[16] The principle was developed by the CJEU in case *Internationale Handelsgesellschaft*, **C-11/70,** ECLI:EU:C:1970:114. Similarly to the German administrative law, also at EU level, the test for establishing the necessity and proportionality of a measure is composed of three steps: (i) appropriateness; (ii) necessity; and (iii) proportionality *stricto sensu*. See in this regard, C. Bagger Tranberg, *Proportionality and data protection in the case law of the European Court of Justice*, International Data Privacy Law, 2011, Vol. 1, No. 4, page 240.

[17] Case C-62/14, *Gauweiler (OMT)*, ECLI:EU:C:2015:400, para. 67. See also C-331/88, *Fedesa and others*, ECLI:EU:C:1990:391, para. 13: *"As to review of proportionality, the principle of proportionality, which is one of the general principles of Community law, requires that measures adopted by Community institutions do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued*.".

[18] As possible example of **proportionality in a broad sense**, encompassing both the necessity and the proportionality tests, see C-594/12, *Digital Rights*, whereby necessity (para. 65: "*"It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is* ***strictly necessary****."*) and proportionality (para. 69: "*Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of* ***proportionality*** *in the light of Articles 7, 8 and 52(1) of the Charter."*) are distinctly addressed by the CJEU. In other words, the CJEU concludes on the proportionality *after* having analysed the necessity.

[19] K. Lenaerts, P. Van Nuffel, *European Union Law*, Sweet and Maxwell, 3rd edition, London, 2011, p. 141 (case C-343/09, *Afton Chemical*, para. 45; joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Hartmut Eifert*, ECLI:EU:C:2010:662, para. 74; cases C-581/10 and C-629/10, *Nelson and Others*, para. 71; case C-283/11, *Sky Österreich*, para. 50; and case C-101/12, *Schaible*, para. 29).

[20] Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

[21] Ibid. para. 47.

question 'What is **the extent of the (reduced) discretion of the EU legislator**?', the CJEU stated: "*[T]he EU legislation in question **must** lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data*"[22] (emphasis supplied).

This latter element (the balance to be struck) describes **proportionality in a narrow sense (*stricto sensu*)** and constitutes the proportionality test which is the subject matter of the present Guidelines. It should be clearly distinguished from necessity (see section III below), from both a conceptual and a practical viewpoint.

2. Clarifications on **the relationship** between proportionality and necessity

As specified in the Necessity Toolkit, "**necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal**". The necessity test should be considered as **the first step** with which a proposed measure involving the processing of personal data must comply. Should the draft measure **not pass** the necessity test, there is **no need to examine** its proportionality. A measure which is not proven to be necessary should not be proposed unless and until it has been modified to meet the requirement of necessity: in other words, **necessity is a pre-condition for proportionality**[23].

These Guidelines are hence based on the assumption that only a measure proved to be necessary should be assessed under the proportionality test. As mentioned in the Necessity Toolkit, in some recent cases, the CJEU **did not proceed in assessing proportionality** after finding that the limitations to the rights in Articles 7 and 8 of the Charter were **not** strictly necessary[24].

However, once a legislative measure is assessed to be **necessary**, it should then be examined according to its **proportionality**. **A proportionality test generally involves assessing what 'safeguards' should accompany a measure** (for instance, on surveillance) in order to reduce

---

[22] Ibid., para. 54.
- See also **EDPS Opinion 5/2015 Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record (PNR)´data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime**, pages 6-7: "In the context of the performance of a **proportionality test**, the **extent to which the EU legislature's discretion may prove to be limited** depends on a number of factors, including, in particular: the area concerned, the nature of the rights at issue, the nature and seriousness of the interference and the object pursued by the interference. The Court insisted that these limitations and safeguards are even more important where personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data." The EDPS Opinion is available at: https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf.

[23] In joined cases **C-465/00, C-138/01 and C-139/01**, *Rechnungshof*, ECLI:EU:C:2003:294 para. 91 , the CJEU held that: "*If the national courts conclude that the national legislation at issue is **incompatible** with Article 8 of the Convention, that legislation **is also incapable of satisfying the requirement of proportionality** in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46*" (emphasis supplied).

[24] In joined cases **C-293/12 and C-594/12**, *Digital Rights*, ECLI:EU:C:2014:238, the CJEU first stated that proportionality consists of the steps of appropriateness and necessity (para. 46). It then established that the limitation with the rights protected in Articles 7 and 8 of the Charter were **not necessary** (para. 65) and therefore concluded that the limitations were not proportionate (para. 69).
- Similarly, in case **C-362/14**, *Schrems*, ECLI:EU:C:2015:650, paras. 92 and 93, the CJEU analysed necessity and found the Safe Harbour Decision to be invalid, without making **any reference to proportionality** before reaching this conclusion (para. 98).

the risks, posed by the envisaged measure to the fundamental rights and freedoms of the individuals concerned, to an 'acceptable'/proportionate level.

Another factor to be considered in the assessment of proportionality of a proposed measure is **the effectiveness of existing measures** over and above the proposed one[25]. If measures for a similar or the same purpose already exist, their effectiveness should be systematically assessed as part of the proportionality assessment. Without such an assessment of the effectiveness of existing measures pursuing a similar or the same purpose, the proportionality test for a new measure cannot be considered as having been duly performed.

3. **Conclusion**: proportionality in data protection law. A 'fact-based' concept requiring case-by-case assessment by the EU legislator

The "emergence of a requirement of proportionality" has been considered "**one of the most striking developments** over the last decade in European data privacy law"[26].

The principle of proportionality has been incorporated in Article 5(1) of **modernised Convention 108**[27] which provides: "Data processing shall be **proportionate** in relation to the legitimate purpose pursued and reflect at all stages of the processing a **fair balance** between all interests concerned, whether public or private, and the rights and freedoms at stake" (emphasis supplied).

At the core of the notion of proportionality lies the concept of a **balancing exercise**: the weighing up of the **intensity of the interference** *vs* the **importance** ('legitimacy', using the wording of the case-law) of the objective achieved **in the given context**.

A well-performed test requires the express identification, and structuring into a coherent framework, of the different elements upon which the weighting depends, in order to be complete and precise.

Hence, the **clarity of the measure** restricting the fundamental rights to privacy and/or and data protection is a precondition for the identification of the intensity of the interference. The latter, in its own turn, is needed to verify whether the impact on these fundamental rights is "proportionate to the aim" (i.e. the objective pursued by the legislation under scrutiny).

As stated by the CJEU, it is essential to point out that proportionality is an assessment ***in concreto*** (case by case):

> *"It is for the referring court to take account, in accordance with the principle of* ***proportionality****, of* ***all the circumstances of the case before it****, in particular the duration of the breach of the rules implementing Directive 95/46 and the importance, for the persons concerned, of the protection of the data disclosed"*[28] (emphasis supplied).

[25] See WP29, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 27 February 2014, page 9, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

[26] Lee A. Bygrave, *Data Privacy Law. An International Perspective*, Oxford University Press, 2014, page 147.

[27] Council of Europe, **Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data,** Consolidated text, available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

[28] CJEU, case C-101/01, *Linqvist*, ECLI:EU:C:2003:596, para. 89.

In other words, the proportionality analysis is always **contextual**[29]: as further explained in these Guidelines, this analysis cannot take place without first identifying the context of the measure under scrutiny (for instance, *does the controller share or provide access to the information on the person concerned? with whom and for what purpose?*).

> The operative part of the Guidelines provides guidance in this respect. Similarly to the Commission Impact Assessment methodology with regard to data protection issues, the Proportionality Guidelines essentially aim at **helping the legislator ask the right set of questions**, having regard to the most relevant and recurrent data protection issues. The following checklist in these Guidelines (a four steps-analytical tool) also aims at stimulating 'out of the box' thinking, leading to innovative *ex ante* policy choices and helping in the monitoring and ex post evaluation of the measures.

III. Checklist for assessing proportionality of new legislative measures

1. Overall description of the workflow

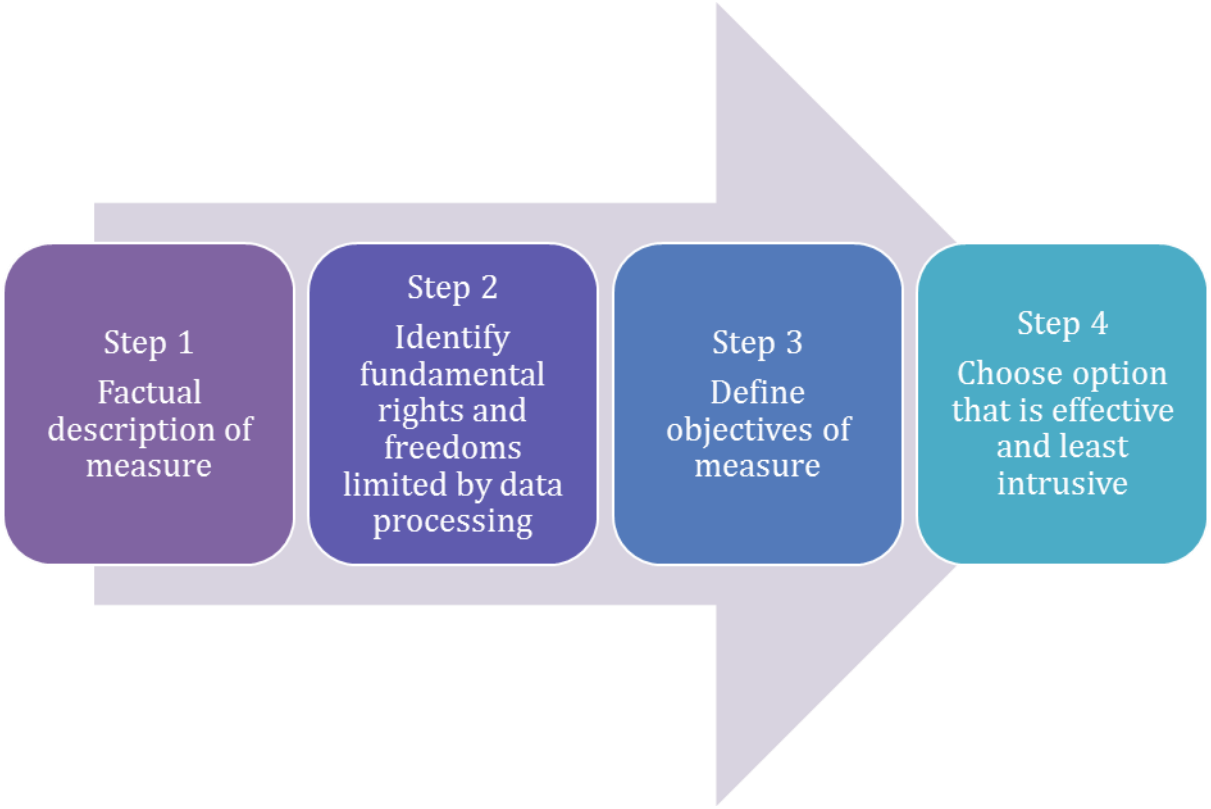
The overall assessment of necessity and proportionality (**synoptic view**) is as follows:

Test 1: As for necessity (necessity test), the steps recommended in the Necessity Toolkit are[30]:

- **Step 1** is preliminary: it requires **a detailed factual description** of the measure proposed and its purpose, prior to any further assessment.
- **Step 2** will help identify whether the proposed measure represents **a limitation** on the rights to the protection of personal data or respect for private life (also called right to privacy), and possibly also on other rights.
- **Step 3** considers the **objective of the measure** against which the necessity of a measure should be assessed.
- **Step 4** provides **guidance on the specific aspects to address** when performing the necessity test, in particular that the measure should be **effective** and the **least intrusive**.

[29] See, as example, ECtHR, *M.K. v. France*, para. 46: "[T]he Court considers that the respondent State has **overstepped its margin of appreciation in this matter**, as the regulations on the retention in the impugned database of the fingerprints of persons suspected of having committed offences but not convicted, **as applied to the applicant in the instant case**, do not strike a fair balance between the competing public and private interests at stake. Consequently, the retention of the data must be seen as a **disproportionate interference** with the applicant's right to respect for his private life and cannot be regarded as necessary in a democratic society" (emphasis supplied).

[30] See at page 9 of the EDPS Necessity Toolkit.



If the assessment of the measure leads to the conclusion that a measure complies with the requirement of necessity (**test 1**), then the measure can be examined under the following steps of the proportionality test (**test 2**).

In other words, under **test 2** we will reconsider the measure assessed as necessary (meaning that this is the least intrusive effective measure available to attain the objective pursued) and assess whether the limitation (interference) that it causes is proportionate to the objective intended to be achieved.

Test 2: As for proportionality (proportionality test), the steps are:

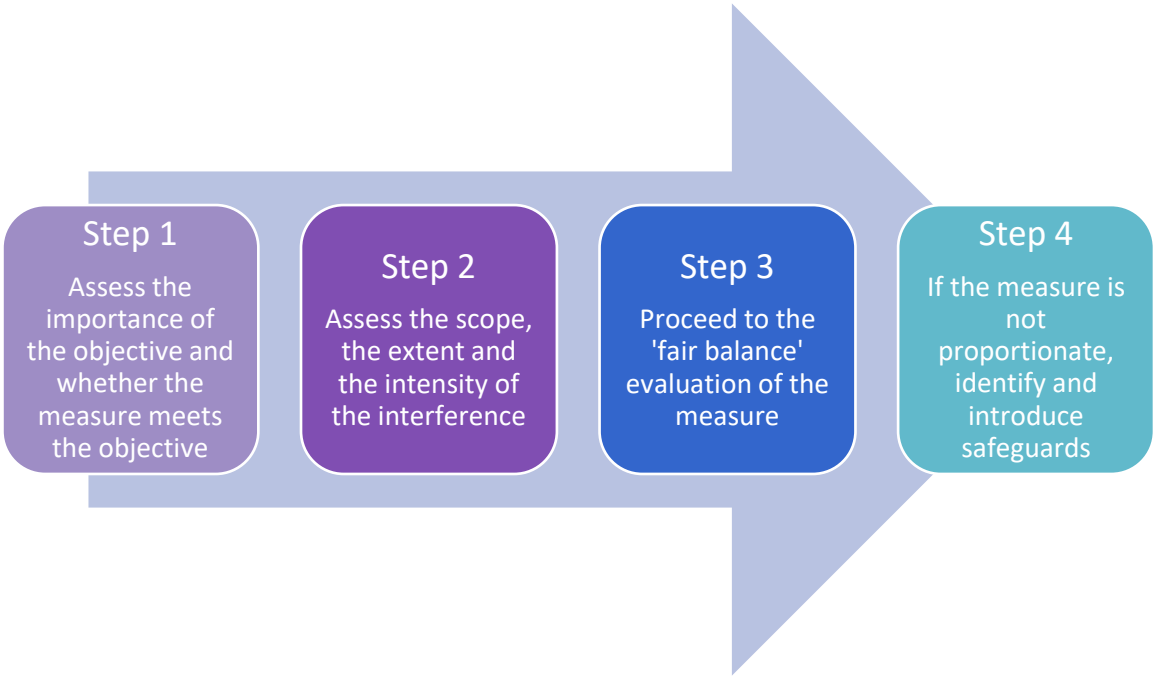
- **Step 1** (or 5 of the overall combined workflow): assess **the importance** ('**legitimacy**') **of the objective** (identified under step 3 of the Necessity Toolkit) and **whether and to what extent** the proposed measure would meet this objective and addresses the issue identified in the problem definition ("**genuinely** meets") [this would be 'the advantage/benefit'].

- **Step 2** (or 6 of the overall combined workflow): assess **the scope, the extent and the intensity** of the interference (identified under step 2 of the Necessity Toolkit) in terms of **impact** on the fundamental rights to privacy and data protection [this would be 'the disadvantage/cost'].

- **Step 3** (or 7 of the overall combined workflow): proceed to the **fair balance (*advantage/disadvantage*; *benefit/cost*) evaluation** of the measure.

- **Step 4** (or 8 of the overall combined workflow): **take a decision ('go/no go') on the measure**. If the result is 'no go', taking into account all factors which determined the

evaluation as disproportionate, identify and introduce (if possible) safeguards which could make the measure proportionate.



2. Description of the steps of the proportionality test

Step 1: assess the importance ('legitimacy') of the objective and whether and to what extent the proposed measure would meet this objective (effectiveness and efficiency)

A detailed description of the **purpose**(s) of the envisaged measure is not only a **prerequisite** to the proportionality test, but also helps to demonstrate compliance with the first requirement of Article 52(1) of the Charter, *i.e.* the *quality of the law*[31].

[31] As stated in the Opinion of Advocate General Mengozzi, ECLI:EU:C:2016:656, para. 193 on the draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data: "*According to the case-law of the ECtHR, that expression requires, in essence, that the measure in question be* ***accessible*** *and* ***sufficiently foreseeable****, or, in other words, that its terms be sufficiently clear to give an adequate indication as to the circumstances in which and the conditions on which it allows the authorities to resort to measures affecting their rights under the ECHR*" (emphasis supplied).
- In joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, Advocate General Saugmandsgaard Øe further elaborates in his Opinion, ECLI:EU:C:2016:572, paras. 139-140, that: "*According to that body of case-law, the expression 'provided for by law' means that the legal basis must be adequately accessible and foreseeable, that is to say****, formulated with sufficient precision to enable the individual - if need be with appropriate advice - to regulate his conduct****. The legal basis must also provide adequate protection against arbitrary interference and, consequently, must define with sufficient clarity the scope and manner of exercise of the power conferred on the competent authorities (the principle of the supremacy of the law). In my view, the meaning of that expression 'provided for by law' used in Article 52(1) of the Charter needs to be the same as that ascribed to it in connection with the ECHR*.".
In this regard, see also ECtHR, *Catt v The United Kingdom*, 24 January 2019, para. 6 of the concurring opinion of Judge Koskelo joined by Judge Felici, "**the general principles of data protection law**, such as those requiring

In practice, if the law does not **clearly and specifically define the objective**(s) at stake, it is impossible to have an *ex ante* evaluation of the importance of the objective and of the efficacy of the measure at reaching this objective.

It is important to note that both the **measure** and its **objectives** should already have been **identified** under Steps 1 and 3 of the necessity test (test 1). Under this step, we will reconsider these objectives in order to ascertain, still *ex ante* but now *in concreto*, their **importance** and to what extent they will be **effectively fulfilled** by the measure.

Referring to the terminology used by the Commission Impact Assessment, what is being considered here is the effectiveness (*is the measure proposed best placed to achieve the objectives?*) and the efficiency (*cost-effectiveness*) of the measure (the identified policy option) to meet the objective (that is, to **solve the issues identified in the Problem Definition**).

The measures should address **the needs** (i.e. the objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others) **clearly identified in the Problem Analysis**. As stated by the CJEU, the **measure**, to be proportionate, shall "genuinely meet" the **objective**[32]. Also, the objective must mirror the needs singled out in the problem analysis.

When assessing the effectiveness of the measure, the legislator must always first verify the effectiveness of **already existing measures**[33]. In other words, before proposing and adopting new measures, the legislator should consider whether the 'existing measure' is **enforced** in

---

that the data to be processed must be adequate, relevant and not excessive in relation to that purpose, **become diluted, possibly to the extent of practical irrelevance, where the purpose itself is left without any meaningful definition or limitation**." (emphasis supplied).

[32] CJEU, joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970 para.94: "*With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they* ***genuinely meet*** *objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others*" (emphasis supplied).

[33] In the Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf), the WP29 states: "However this assessment is done it should involve an evidence led explanation of why the existing measures are no longer sufficient for meeting that need."

In **Opinion 06/2016 on the Second EU Smart Borders Package**, 21 September 2016 (page 3) (available at:https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf), the EDPS noted that "[n]ecessity and proportionality of this scheme [the Entry Exit System] are to be assessed both globally, **taking into consideration the already existing large-scale IT systems in the EU**, and specifically, in the specific case of these third country nationals legally visiting and entering the EU".

- In **Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS)**, 6 March 2017 (available at: https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_en.pdf), the EDPS clearly stated (page 8): "[A] privacy and data protection impact assessment of ETIAS should **take stock of all EU-level measures taken for migration and security objectives and analyse in-depth their concrete implementation, their effectiveness and their impact on individuals' fundamental rights before creating new systems involving the processing of personal data**. This analysis should also take into account the policy area in which these measures apply and the respective role of the key actors involved.".

- See **EDPS Opinion 5/2015 on the Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime**, (page 15): "The Proposal does not provide for a comprehensive evaluation of the ability of the current existing instruments to reach the purpose of the EU PNR scheme.".

practice, and whether **broadening and/or deepening** this measure would already satisfactorily address the problem identified in the Problem Analysis. Without a systematic assessment of the effectiveness of existing measures pursuing a similar or the same purpose, the proportionality test for a new measure cannot be considered as having been duly performed. In the case of a pre-existing measure, effectiveness has to be considered, during the balancing exercise, not in absolute terms but in terms of **added value** of the measure.

Guidance (how to proceed)

- **Needs** should be sufficiently described in the problem analysis to enable a clear understanding of *what* exactly prompted the initiative for a legislative proposal. The legislator needs to have complete and accurate information on the **problems to be solved** (the **Drivers** of the problem) and about the available options.

- In particular, concerning the problem to be addressed (**Problem Definition**), the legislator should be aware of the **level of urgency of the public interest** (for instance, public security) to be addressed and **clearly refer to it** in the measure (specifying, for example, that the measure is intended to address a temporary high-level threat). This could be brought down to the following question: "Are we in presence of a *pressing social need* for restricting the right (to privacy and/or data protection)?"[34].

- The reference to the **level of threat**, as referred to above, and the monitoring/update on this driver allows the legislator to lift the measure restricting the rights to privacy and protection of personal data once this level decreases. An independent oversight system, to avoid the temporary measure becoming permanent, is also key.

- It is important to verify whether the **concrete purpose**(s) of the measure **mirrors** these needs. This could be brought down to the following question: "Does the envisaged purpose correspond to this need?" [using the Impact Assessment terminology, "*Does the measure, taking into account its impact/consequences, solve the Problem*?"] The affirmative reply to such question would avoid 'legislative function creep' (namely, a measure that does not genuinely address the problem[35] but a different purpose instead).

---

[34] For example, see the ECtHR ruling in *Weber and Saravia v Germany*, para. 112: "In the applicant's view, these wide monitoring powers **did not correspond to a pressing need** on the part of society for such surveillance. There was no longer a threat of an armed attack on the Federal Republic of Germany by a foreign State possessing nuclear weapons, as there had been during the Cold War. Nor was there any other comparable current danger to be averted. In particular, drug trafficking, counterfeiting of money and money laundering or presumed dangers arising from organised crime did not constitute a danger to public safety sufficient to justify such an intensive interference with the telecommunications of individuals. The fact that interception was limited to content of "relevance for the intelligence service" ("*nachrichtendienstliche Relevanz*"), as a result of the decision of the Federal Constitutional Court, was not sufficient to constrain effectively the monitoring powers of the Federal Intelligence Service" (emphasis supplied).
On pressing social need, see the clarification provided by the **WP29 Opinion on the application of necessity and proportionality concepts and data protection within the law enforcement sector**, WP211, 27 February 2014, pages 7 and 8. See also the list of factors to be taken into account, flagged at pages 9-11. The Opinion is available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

[35] See **Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice**, 17 November 2017 (available at:

- Verify that the **purpose (**the **objective)** enshrined in the proposal for legislation is in line with the **public/societal regulatory need** that will be addressed (the harm the society may be exposed to in the absence of the measure, for instance widespread common criminality or specific white collar crimes).

> We recall that, according to the Commission Impact Assessment, the **objectives** must be **SMART**, that is: **specific** (precise and concrete enough); **measurable** (define a desired future state in measurable terms, for instance, decrease in crimes estimated at ..%); **achievable**; **realistic**; and **time-dependent** (related to a fixed date or time period by when the results should be achieved). These requirements, which are common to the better regulation methodology, are particularly important, as the examples will show, in case of legislation restricting or otherwise impacting on the protection of personal data.

- Assess the **importance** of the objective (is it to protect a constitutional value or a fundamental right?[36]).

- Assess the **effectiveness and efficiency** of the measure to fulfil the aforesaid objective.

---

https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf), where the EDPS observed that the Commission "should also clearly set out **for which specific purposes** what categories of personal data would be processed in the context of its future initiatives on interoperability. This will allow a proper debate on interoperability from the fundamental rights perspective." (page 3).
In a similar way, see **EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems**, 16 April 2018, available at: https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf.
"41. The EDPS stresses that "combating irregular migration and ensuring a high level of security" is a very broad description of (otherwise legitimate) purposes (page 12). He notes that Article 20 requires the adoption of a national law that shall further define them. However, he would like to recall that the Court of Justice of the European Union ('CJEU') in its Digital Rights Ireland ruling (para. 61) held that the Directive 2006/24 failed to '*lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences*' by simply referring '*in a general manner to serious crime, as defined by each Member State in its national law.'* The Court also considered that the purpose for the access and use of the data was not '*strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto*'.
42. **The EDPS considers that the purposes of combating irregular migration and contributing to a high level of security in the context of Article 20 are too broad and do not fulfil the requirements of being '*strictly restricted'* and '*precisely defined*' in the Proposals, as required by the Court. He therefore recommends to further define them in the Proposals**. For instance, "irregular migration" could refer to the conditions of entry and stay as set out in Article 6 of Regulation (EU) 2016/399 of the European Parliament and of the Council. As regards security, the EDPS recommends to target the criminal offences that could in particular threaten a high level of security; for instance by referring to the crimes listed in Article 2(2) of Framework Decision 2002/584/JHA if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.".
[36] For the **overview of the rights, freedoms and principles guaranteed by the Charter**, see Annex II, page 28, of the Commission Staff Working Paper, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC (2011) 567 final.

Relevant examples

As an illustration of this **methodology**, in particular we **deconstruct** into the four grey boxes providing examples for each of the four steps the CJEU judgments in the *Tele2* and *Ministerio Fiscal* cases, the Advocate General Opinion and the CJEU Opinion 1/15 in the EU-Canada Passenger Name Record (hereinafter 'PNR') case and the CJEU judgment in the *Bevándorlási és Állampolgársági Hivatal* case.

EXAMPLE 1: Tele2 Sverige AB (CJEU, C-203/15, ECLI:EU:C:2016:970)

The Court **described the objectives** of the measure under scrutiny (briefly, an obligation relating to the retention of traffic and location data) as follows: "*the first sentence of Article 15(1) of Directive 2002/58 provides that the **objectives** pursued by the legislative measures that it covers, which derogate from the principle of confidentiality of communications and related traffic data, must be 'to **safeguard national security - that is, State security - defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system**', or one of the other objectives specified in **Article 13(1)** of Directive 95/46, to which the first sentence of Article 15(1) of Directive 2002/58 refers (...). That **list of objectives is exhaustive**, as is apparent from the second sentence of Article 15(1) of Directive 2002/58, which states that the legislative measures must be justified on 'the grounds laid down' in the first sentence of Article 15(1) of that directive. Accordingly, the Member States **cannot adopt such measures for purposes other than those** listed in that latter provision*" (emphasis supplied).While the **importance** of the objective (protection of public security and the enforcement of criminal law) is evident in this case, the Court also acknowledged that the measure would enhance the possibilities to use modern investigation techniques, and hence "*the **effectiveness** of the fight against serious crime, in particular organised crime and terrorism*" (emphasis supplied).

EXAMPLE 2: Ministerio Fiscal (CJEU, C-207/16, ECLI:EU:C:2018:788)

Having regard to the **importance of the objective**, the Court recognised that **the objective** of the measure is limited to **"*preventing, investigating, detecting and prosecuting criminal offences generally*"** (in this case, the theft of a wallet and a mobile phone) as opposed to a 'serious crime'. Hence, it can be argued that the Court considered the 'magnitude' of importance of the objective as relatively **minor**.

On the **effectiveness of the measure** to pursue the aforesaid objective, the Court remarked that via the measure under scrutiny, "*the police seeks, for the purposes of a criminal investigation, a Court authorisation to **access personal data retained by providers of electronic communications services**, (..) **to identify the owners of SIM cards activated over a period of 12 days with the IMEI code of the stolen mobile telephone**." **"***The data concerned by the request for access at issue in the main proceedings (...) **enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards (activated on the stolen telephone)**. It is therefore evident that the measure would be **effective** in tracing back, if any, the thief or a purchaser of the telephone (in case he or she decided to make use of the telephone, installing on it a SIM card) and thus allowing to identify, directly or indirectly via further and so enabled investigations, the author of the offence*" (emphasis supplied).

EXAMPLE 3: 'EU-Canada PNR' (Advocate General Opinion, ECLI:EU:C:2016:656 and CJEU, Opinion 1/15, ECLI:EU:C:2017:592)

Advocate General Mengozzi, at para. 205 of his Opinion, recognised both the **importance of the objective** and **the effectiveness** of the measure in reaching this objective: "*I do not believe that there are any real obstacles to recognising that the interference constituted by the agreement envisaged **is capable of attaining the objective of public security,** in particular the objective of combating terrorism and serious transnational crime, pursued by that agreement. As the United Kingdom Government and*

the Commission, in particular, have claimed, the transfer of data for analysis and retention provides the Canadian authorities with additional opportunities to identify passengers, hitherto not known and not suspected, who might have connections with other persons and/or passengers involved in a terrorist network or participating in serious transnational criminal activities. ***As illustrated by the statistics*** *communicated by the United Kingdom Government and the Commission concerning the Canadian authorities' past practice, that data constitutes a* ***valuable tool for criminal investigations****, which is also of such a kind as to favour, notably in the light of the police cooperation established by the agreement envisaged, the prevention and detection of a terrorist offence or a serious transnational criminal act within the Union*" (emphasis supplied).

The Court took into account the **already existing measures**, and concluded that the already available data "*are* ***not sufficient*** *to attain with comparable effectiveness the public security objective pursued by the agreement envisaged*" (emphasis supplied).

EXAMPLE 4: ***Bevándorlási és Állampolgársági Hivatal*** **(CJEU, C-473/16, ECLI:EU:C:2018:36)**

In this case, the measure under scrutiny is the collection and processing of a **psychologist's report** on the sexual orientation of a person applying for refugee status pursuant to Directive 2011/95. The Court acknowledged that **the objective** of the measure is "*to allow the search for information enabling his actual need for international protection to be assessed*".

The Court also observed that "***the suitability*** *of an expert's report such as that at issue in the main proceedings may be accepted only if it is based on sufficiently reliable methods and principles in the light of the standards recognised by the international scientific community*" (emphasis supplied).

Still, on **the effectiveness** of the measure in reaching the aforesaid objective, the Court observed: "*such an expert's report* ***cannot be considered essential*** *for the purpose of confirming the statements of an applicant for international protection relating to his sexual orientation in order to adjudicate on an application for international protection based on a fear of persecution on grounds of that orientation*" (emphasis supplied).

In particular, the Court stated that: "*where the Member States apply the principle that it is the duty of the applicant to substantiate his application, the applicant's statements concerning his sexual orientation which are not substantiated by documentary evidence or evidence of another kind* ***do not need confirmation when the conditions set out in that provision are fulfilled: those conditions refer, inter alia, to the consistency and plausibility of those statements*** *and* ***do not make any mention of the preparation or use of an expert's report***" (emphasis supplied).

"*Furthermore, even assuming that an expert's report based on projective personality tests, such as that at issue in the main proceedings,* ***may contribute*** *to identifying with a degree of reliability the sexual orientation of the person concerned, it follows from the statements of the referring court that* ***the conclusions of such an expert's report are only capable of giving an indication*** *of that sexual orientation. Accordingly, those conclusions are, in any event,* ***approximate in nature and are therefore of only limited interest*** *for the purpose of assessing the statements of an applicant for international protection, in particular where, as in the case at issue in the main proceedings, those statements are not contradictory*" (emphasis supplied).

EXAMPLE 5: EDPS Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS)

It is possible that the legislator also refers to **the objective** of the measure as '**risk to be avoided**'. Also in this case, as highlighted by the EDPS, the risks should be defined as far as possible. "Article 1 of the Proposal mentions that ETIAS aims at determining whether the presence of a visa-exempt traveller in the territory of the Member States poses an **irregular migration, security and/or public health risk**. The EDPS notes that the Proposal **defines the public health risk** by referring to specific categories of diseases, but **does not define security and irregular migration risks**" (emphasis supplied).

Step 2: assess the (scope, extent and intensity of the) interference in terms of effective impact of the measure on the fundamental rights to privacy and data protection

A detailed assessment of the interference of the envisaged measure with the fundamental rights to privacy and data protection is the other key step of the proportionality test.

It is important to note that **the fundamental rights and freedoms limited** by the measure have already been **identified** under Step 2 of the necessity test (test 1). Under this step, we will reconsider these fundamental rights and freedoms in order to ascertain, still *ex ante*, but *in concreto*, how they would be affected. Indeed, as mentioned in the FRA handbook "Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level-Guidance", "*the measure should not impose a **disproportionate and excessive burden** on the persons affected by the limitation in relation to the objective pursued*"[37].

It is important to note that the impact can be **minor** with regard **to the individual** concerned, but nonetheless **significant or highly significant** collectively/**for society** as a whole (**impact on individuals** *vs* **impact on society as a whole**)[38].

The **costs** of the privacy impacting measure, under this perspective, are represented by the **externalities** of the lack of data protection (the 'data pollution'). Hypothetical examples of such externalities are: harm to the electoral and political process (misuse of data for political manipulation) [39]; unlawful profiling and discrimination causing distrust towards public authorities; 'chilling effect' on freedom of expression of an all-encompassing surveillance

[37] FRA Handbook referred to above, p. 76. See also CJEU, case C-258/14, *Eugenia Florescu and others v. Casa Județeană de Pensii Sibiu and others*, ECLI:EU:C:2017:448, para. 58.

[38] See Omri Ben-Shahar, *Data Pollution*, University of Chicago, June 2018, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191231 See page 3: "The privacy paradigm is founded on the premise that the injury from the personal data enterprise is private in nature -to the "core self"- although by sheer aggregation (or by more nuanced channels) these deeply private injuries have a derivative social impact" and page 4: "[V]ast literature has combed through every aspect of the private harms from data collection, the potential privacy injuries to the people whose data is collected. The **externality problem**, however, has been entirely neglected: how the participation of people in data-harvesting services affects **others, and the entire public**.".

[39] See EDPS Opinion on Online Manipulation, referred to under footnote 42.
ICO, "*Democracy disrupted? Personal information and political influence*", 11 July 2018, available at: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf.
Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *Action Plan against Disinformation* (JOIN(2018) 36 final), available at:
https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
Communication from the commission to the European parliament, the Council, the European economic and social committee and the Committee of the regions on "Securing free and fair European elections", available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-free-fair-elections-communication-637_en.pdf.

measure[40] or other negative effects on the freedom of the individuals stemming from a pervasive and systemically implemented profiling and scoring system[41].

Even though difficult to quantify in practice[42], these externalities shall be taken into account by the legislator in its evaluation of the 'privacy cost' of the measure.

In case of a proposed surveillance measure, it is important to evaluate **the level of intrusiveness** of the method of surveillance. For this evaluation, the **dimensions of surveillance** need to be assessed. Relevant case law of the ECtHR and of the CJEU has identified dimensions of surveillance, starting with the 'senses-dimension' (for instance, audio, video-recording)[43], to the possibilities for analysing, merging and communicating the information. The **level of intrusiveness** into the private life of the targeted individuals, as well as the potential intrusion into the private life of **third parties**, must be carefully assessed by the authorities that decide upon the measure.

The impact under this step also relates to the potential **harmful effect** of the measure on a **wider basis than that of protecting privacy**, hence including the risks for other fundamental rights. This is in line with the approach taken by the GDPR that refers explicitly and on multiple occasions to the 'risks for the rights and freedoms of natural persons', thus highlighting the fact that an harmful effect to the right to privacy is often **inextricably linked** to harm to **other fundamental rights**, such as the rights to **freedom of expression, free movement, freedom**

[40] In his Opinion, ECLI:EU:C:2013:845, in *Digital Rights*, Advocate General Cruz Villalón referred to this chilling effect: "*[I]t must not be overlooked that the vague feeling of surveillance which implementation of Directive 2006/24 may cause is capable of having a decisive influence on the exercise by European citizens of their freedom of expression and information and that an interference with the right guaranteed by Article 11 of the Charter therefore could well also be found to exist*" (para 52); "*The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period*" (para. 72).
The CJEU, confirming the Advocate General's approach, stated, at para. 37 of the judgment, that *"(...) the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.*".

[41] See, for hypothetical examples, H.J. Pandit, D. Lewis, *Ease and Ethics of User Profiling in Black Mirror*, 2018, available at: https://dl.acm.org/citation.cfm?id=3191614 See, as impact assessment model, the "Ethics Canvas", page 1582.

[42] See at page 31 of *Data Pollution* referred to in footnote 38: "Data externalities are often qualitative and conjectural. What is the cost figure attached to distorted Presidential elections? To discriminatory racial profiling?".

[43] In case *Uzun v Germany*, the ECtHR considered the use of a GPS device for location tracking as a less intrusive measure than the interception of personal communications.
- On **video surveillance** (CCTV), see **EDPS Video-Surveillance Guidelines**, 17 March 2010, available at: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf.

of association[44], and to general principles of EU law such as the **principle of 'non-discrimination'**[45]. In this sense, these Guidelines take a 'fundamental rights approach'.

Guidance (how to proceed)

The impact should be sufficiently described to enable a clear understanding of **the scope, extent and intrusiveness level of the interference** on the fundamental rights to privacy and to the protection of personal data. It is particularly important to precisely identify:

- **the impact[46],** taking into account:

[44] The EDPS has been advocating a broader approach to data protection that takes these interfaces into account. See, in particular, **EDPS Opinion 3/2018 on online manipulation and personal data**, page 13: "Privacy and personal data protection are placed among the 'freedoms' of the EU, which include **freedom of thought, conscience and religion**, **freedom of expression and information**, and **freedom of assembly and association** (Articles 10, 11 and 12). These **are also clearly at stake** due to the ability of the major platform intermediaries either to facilitate or to impede information dissemination. For instance, content which is not indexed or ranked highly by an Internet search engine is less likely to reach a large audience or to be seen at all. Alternatively, a search algorithm might also be biased towards certain types of content or content providers, thereby risking affecting related values such as media pluralism and diversity" and page 5: "EU law on data protection and confidentiality of electronic communications apply to data collection, profiling and micro-targeting, and **if correctly enforced should help minimise harm** from attempts to manipulate individuals and groups." The Opinion is available at:
https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

[45] For instance, the Meijers Committee, in its "Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), 12 December 2017, COM (2017) 794", 19 February 2018, noted the intersection between **limitation of privacy** (collection and processing of personal data relating to a group/category of persons) **and breach of the non-discrimination principle**. See at page 3 of the Comments: "[T]he explicit objective of the proposal of facilitating identity checks of third country nationals by police organisation within the EU territory, to see whether information on this person is stored in one or more of the EU databases, will enhance the possibility of third-country nationals (or those considered to be third-country nationals) being stopped for identity checks. In this context, the Meijers Committee recalls the *Huber v. Germany* case, in which the CJEU dealt with the **differential treatment between nationals and EU citizens living in Germany** with regard to the **central storage and multiple use of personal data in an aliens administration, including the use for law enforcement purposes** (CJEU *Huber v. Germany*, C-524/06, 16 December 2008, para 78-79).".

[46] The impact analysis referred to in these Guidelines takes into account the contextual **data protection harm and risk of harm potentially -stemming from the legislative measure target of evaluation- for individuals concerned and for society as a whole**. It is therefore different (broader) from the notion of "**risks of varying likelihood and severity for the rights and freedoms of natural persons**", referred to under Article 24 of the GDPR.
Another difference with the **data protection impact assessment** (DPIA) pursuant to Article 35 of the GDPR is that in these Guidelines we refer to the 'more abstract level' assessment of the proportionality of *the legislative measure* (rather than of a *type of processing* envisaged by a controller). Accordingly, the proportionality could be considered as a '*DPIA on the law*' (to be performed in the context of the advisory function on legislative measures impacting on the right to privacy and to the protection of personal data).
Nonetheless, it can be useful to remark that **many of the factors which are relevant to perform the DPIA are also relevant for the evaluation of the privacy costs of a legislative measure.**
See, in this regard, the **WP29, now EDPB, 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**, WP248, as last revised and adopted on 4 October 2017, available at:
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
The following nine factors (to establish high risks) are pointed out at pages 9-11: (i) **Evaluation or scoring**, including profiling and predicting; (ii) **Automated-decision making** with legal or similar significant effect; (iii) **Systematic monitoring**; (iv) **Sensitive data** or data of a highly personal nature; (v) Data processed on a **large scale**; (vi) **Matching or combining** datasets; (vii) Data concerning **vulnerable data subjects**; (viii) Innovative use or applying **new technological or organisational solutions,** like combining use of finger print and face

- *the **scope*** of the measure: is it sufficiently limited? *number of people* affected; whether it raises '***collateral** intrusions'*, that is interference with the privacy of persons other than the subjects of the measure[47];

- *the **extent**: how is the right restricted? amount of information* collected; for *how long; whether the measure under scrutiny requires the collection and processing of special categories of data*[48];

- *the **level of intrusiveness***, taking into account: *the nature of the activity* subjected to the measure (whether it affects activities covered by duty of confidentiality or not, lawyer-client relationship; medical activity); *the context*; whether it amounts to ***profiling*** of the individuals concerned or not[49]; whether

---

recognition for improved physical access control, *etc*.; (ix) When the processing in itself "**prevents data subjects from exercising a right or using a service or a contract**.".
Annex I to the Guidelines provides for examples of **sector-specific** frameworks, for example "**Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems**", available at: http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.
See in particular at pages 27-31 on the **Identification, Quantification (severity and likelihood) and Assessment** of the 'risk'.
- Lastly, see the **draft list of the competent supervisory authority**(ies) **regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR),** available at: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

[47] See *Big Brother Watch and others v United Kingdom*, ECtHR, 13 September 2018, para. 2.43: "2.43. **Collateral intrusion** is the obtaining of any information relating to individuals other than the subject(s) of the investigation. Consideration of collateral intrusion forms part of the proportionality considerations, and becomes increasingly relevant when applying for traffic data or service use data. Applications should include details of **what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion**. When there are **no meaningful collateral intrusion risks**, such as when applying for subscriber details of the person under investigation, **the absence of collateral intrusion should be noted**" (emphasis supplied).

[48] See CJEU, joined cases C-465/00, C-138/01, and C-139/01, *Rechnungshof*, ECLI:EU:C:2003:294 para. 52: "*The Austrian Government notes in particular that, when reviewing proportionality, **the extent** to which the data affect private life must be taken into account. Data relating to **personal intimacy, health, family life or sexuality** must therefore be protected more strongly than data relating to income and taxes, which, while also personal, concern personal identity to a lesser extent and are thereby less sensitive*" (emphasis supplied).
- On the processing of **health data**, see **EDPS Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS)**, at page 13: "The EDPS doubts that the processing of this particularly sensitive category of data on such a large-scale and for this period of time would meet the conditions laid down in Article 52(1) of the Charter and accordingly be considered as necessary and proportionate. The EDPS questions the relevance of collecting and processing health data as envisaged in the Proposal due to the lack of their reliability and the necessity to process such data due to the limited link between health risks and visa-exempt travellers.".
- Specific attention has been devoted recently to the risks of Artificial Intelligence applied to Facial (and 'affect') recognition. See *AI Now Report 2018*, December 2018, available at: https://ainowinstitute.org/AI_Now_2018_Report.pdf.
- On **biometric data**, see **WP 29 Opinion 3/2012 on developments in biometric technologies**, pages 30-31, on the specific risks posed by biometric data; and **WP 29 Opinion 02/2012 on facial recognition in online and mobile services**, Section 5, Specific risks and recommendations.

[49] In this context, we refer to the term "profiling" in the broad sense, as 'establishing a profile of the individual', as referred to in the *Tele2* case, and not necessarily to the definition under Article 4(4) of the GDPR: "'*profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

the processing entails the use of (partially or fully) ***automated*** decision making system with a 'margin of error'[50];

- whether it concerns ***vulnerable*** *persons* or not[51];
- whether it **also affects *other fundamental* rights** (there could be 'inextricably linked' fundamental right[52], for instance the right to protection of privacy and the right to freedom of expression, as in the *Digital Rights* and *Tele2* CJEU cases).

In cases where some (or part of the) impacts cannot be ascertained beforehand, it might be helpful applying the so-called **precautionary principle**[53]. As an example of the applicability

[50] See, having regard to the automation of decisions, Opinion 1/15, ECLI:EU:C:2017:592, of the CJEU regarding the proposed EU-Canada PNR data sharing agreement. The Court's Opinion highlighted that the Canadian system for risk assessments of EU travellers operated in a systematic and automated manner, and **with a "significant" margin of error** exposing a large number of individuals who posed no risk to ongoing scrutiny by CBSA and other agencies. The Opinion emphasised that algorithmic systems and risk assessment technology must be "applied in a **non-discriminatory** manner and that final decisions "are based 'solely and decisively' on individualized **human-based** assessment"). Also in this case it may be noted that the right to privacy and to the protection of personal data may link to other fundamental rights and principles (here, non-discrimination).
- More specifically, on the **impact of automated decision making used by State/public authorities**, see Australian Government, *Automated Assistance in Administrative Decision Making, Better Practice Guide*, February 2007 (even if not updated, contains a relevant set of questions), available at: https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf.

[51] ECtHR, *S. and Marper*, para 124: "The Court further considers that the retention of the un-convicted persons' data may be **especially harmful** in the case of **minors** such as the first applicant, given their special situation and the importance of their development and integration in society.".
- See, as an example on special attention needed in case of processing of personal data relating to minors, the **EDPS response to the Commission public consultation on lowering the fingerprinting age for children in the visa procedure from 12 years to 6 years**, 9 November 2017, page 2: "The EDPS recommends that the necessity and proportionality of collecting **fingerprint data of children** as from a younger age should be the focus of an **additional prior reflection and evaluation**, as **part of the impact assessment** that is carried out to accompany the future Commission proposal to revise the VIS Regulation.". The EDPS response is available at: https://edps.europa.eu/sites/edp/files/publication/17-11-09_formal_comments_2017-0809_en.pdf.

[52] See Christopher Docksey, *Four fundamental rights: finding the balance*, International Data Privacy Law, 2016, Vol. 6, No. 3, page 203: "[I]n some context, such as mass surveillance and independent regulation, the rights of privacy and data protection and freedom of expression function in a wholly complementary fashion, each reinforcing the other.".

[53] As early as the 1970s, Hans Jonas was the precursor of the precautionary principle. On 2 February 2000, the **European Commission** stated in its **Communication on the Precautionary Principle** (COM(2000)1 final): "Although the precautionary principle is not explicitly mentioned in the Treaty except in the **environmental** field, its scope is **far wider** and covers those specific circumstances **where scientific evidence is insufficient, inconclusive or uncertain** and there are indications through preliminary objective scientific evaluation that there are **reasonable grounds for concern** that the potentially dangerous effects on the environment, human, animal or plant health may be inconsistent with the chosen level of protection." The Communication is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0001&from=EN.
We consider that this principle, consistently with the metaphor of loss of privacy as 'data pollution', is also applicable to the risks to privacy and to the protection of personal data.
- "When a consensus is lacking regarding the development of new technologies interfering with private life, the ECtHR expects a member state 'claiming a pioneer role' to bear 'special responsibility for striking the right balance'", P. Popelier and C. Van De Heyning, *Procedural Rationality: Giving Teeth to the Proportionality Analysis*, European Constitutional Law Review, 9, 2013, page 243, referring to case *S and Marper v United Kingdom*, ECtHR.
- In his **Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems**, the EDPS took into account the unpredictable risks and hence called for a wider, evidence-based, debate (on interoperability), *"(...) interoperability is not primarily a technical choice, it is first and foremost a political choice to be made, with **significant legal and societal implications in***

of this principle, it might be suggested to the legislator, according to all relevant circumstances of the case, to adopt an 'incremental approach', opting for the use of an already *experimented and verified* IT tool rather than an IT tool whose effectiveness (false negatives, false positives) has not yet been fully tested.

Relevant examples

EXAMPLE 1: *Tele2 Sverige AB* (CJEU, C-203/15 and C-698/15, ECLI:EU:C:2016:970)

The Court evaluated the **interference** as **serious**, especially in light of the fact that the measures implied establishing a profile of the person concerned.

The Court observed that: "*legislation provides for a **general and indiscriminate retention** of **all traffic and location data** of **all subscribers and registered users** relating to **all means of electronic communication**, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions. As stated in the order for reference, the **categories of data** covered by that legislation correspond, in essence, to the data whose retention was required by Directive 2006/24*.".

"*The **data** which providers of electronic communications services must therefore retain **makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment**. That data includes, inter alia, the **name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services**. That data **makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place**. Further, that data makes it possible to know **how often the subscriber or registered user communicated with certain persons in a given period** (see, by analogy, with respect to Directive 2006/24, the Digital Rights judgment, para. 26).*".

"*That **data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them** (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, para. 27). In particular, that data provides the means (...) of **establishing a profile of the individuals concerned**, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications*.".

"*The **interference entailed by such legislation** in the fundamental rights enshrined in Articles 7 and 8 of the Charter is **very far-reaching** and must be considered to be **particularly serious**. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned **to feel that their private lives are the subject of constant surveillance** (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, para. 37).".*

*On the impact of the measure on **other fundamental rights**, linked to the rights to privacy and to the protection of personal data, the Court noted that: "the retention of traffic and location data could (...)*

the years to come**. Against the backdrop of the clear trend to mix distinct EU law and policy objectives (i.e. border checks, asylum and immigration, police cooperation and now also judicial cooperation in criminal matters), as well as granting law enforcement routine access to non-law enforcement databases, the decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a 'point of no return'. For these reasons, the EDPS calls for a **wider debate on the future of the EU information exchange, their governance and the ways to safeguard fundamental rights in this context." (para.25).

have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their ***freedom of expression****, guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, para. 28)*" (emphasis supplied).

The Court also considered the impact of the measure '*ratione personae'*, namely the requirement imposed by the legislation to retain and make accessible (also) data relating to **members of professions that handles privileged or otherwise confidential information**: "*particular attention must (...) be paid to necessity and proportionality where the communications data sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information*" (emphasis supplied).

EXAMPLE 2: *Ministerio Fiscal* (CJEU, C-207/16, ECLI:EU:C:2018:788)

The Court held that: "*It should (...)* ***be determined whether****, in the present case, in the light of the facts of the case,* ***the interference with fundamental rights enshrined in Articles 7 and 8 of the Charter*** *that police access to the data in question in the main proceedings would entail* ***must be regarded as 'serious'***.".

"*In that regard,* ***the sole purpose of the request*** *at issue in the main proceedings, by which the police seeks, for the purposes of a criminal investigation, a court authorisation to access personal data retained by providers of electronic communications services, is to identify the owners of SIM cards activated over a period of 12 days with the IMEI code of the stolen mobile telephone. (...) that request seeks access to* ***only*** *the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses. By contrast,* ***those data do not concern*** *(...)* ***the communications carried out with the stolen mobile telephone or its location***.".

"*It is therefore apparent that the data concerned by the request for access at issue in the main proceedings only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data,* ***those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned***" (emphasis supplied).

On the basis of all of the above, the Court found that the **interference** is **not a serious one**. We can observe that a key factor that drove the assessment by the Court as 'not serious' of the interference (reasoning in this regard *a contrario* from *Tele2*) is **the absence of the establishment of a profile of the individual concerned**.

EXAMPLE 3: Opinion 1/15 *PNR Canada* (CJEU, ECLI:EU:C:2017:592)

The **interference** in the PNR Canada case was assessed by the Court in particular with reference to the extent, the level of intrusiveness and the scope *ratione personae*. The latter was considered a problem in the agreement (together with other aspects). The Court held that "*although the interference constituted by the agreement envisaged is* ***less extensive*** *than that provided for in* Directive 2006/24, and is also **less intrusive** into the daily life of everyone, its **undifferentiated and generalised nature** raises questions" (emphasis supplied).

The other problematic aspects criticised by the Court relate to: (i) the identification of the competent authority responsible for processing the data; (ii) the automated processing (lack of safeguards identified at paras. 258-260); (iii) the conditions for access to retained data by law enforcement authorities; (iv) the data retention period; (v) the disclosure and transfer of data; (vi) oversight by an independent authority. The above problems have been pointed out by the CJEU *also* in cases *Digital Rights* and *Tele2*.

EXAMPLE 4: *Bevándorlási és Állampolgársági Hivatal* (CJEU, C-473/16, ECLI:EU:C:2018:36)

On **the interference** of the measure at stake, the Court observed: "*the **interference** with the private life of the applicant for international protection arising from the preparation and use of an expert's report, such as that at issue in the main proceedings, is, in view of its nature and subject matter, **particularly serious***.".

"*Such an expert's report is based in particular on the fact that the person concerned **undergoes a series of psychological tests** intended to establish an essential element of his identity that concerns his personal sphere in that it relates to **intimate aspects of his life** (...)*.".

"*It is also necessary to take account, in order to assess the **seriousness of the interference** arising from the preparation and use of a psychologist's expert report, such as that at issue in the main proceedings, of Principle 18 of the Yogyakarta principles on the application of International Human Rights Law in relation to Sexual Orientation and Gender Identity, to which the French and Netherlands Governments have referred, which states, inter alia, that no person may be forced to undergo any form of psychological test on account of his sexual orientation or gender identity*.".

"*When those elements are looked at together, it is apparent that **the seriousness of the interference** with private life entailed by the preparation and use of an expert's report, such as that at issue in the main proceedings, exceeds that entailed by an assessment of the statements of the applicant for international protection relating to a fear of persecution on grounds of his sexual orientation or recourse to a psychologist's expert report having a purpose other than that of establishing the applicant's sexual orientation*" (emphasis supplied).

EXAMPLE 5: EDPS Opinion 06/2016 on the Second EU Smart Borders Package[54]

"The EDPS would first like to stress that from the point of view of Articles 7 and 8 of the Charter **the processing of personal data under the proposed EES will entail is significant and intrusive,** taking into consideration the **number of persons affected** by this scheme, the **type of information** processed, **the means used** to process such information and the different purposes pursued, as explained below.".

EXAMPLE 6: EDPS Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS)

"The Proposal provides for the assessment of all visa-exempt third country nationals' applications against ETIAS screening rules, while only a limited number of them may in reality pose certain types of risks and be denied a travel authorisation. These automated and non-transparent operations on personal data entail as such a **serious interference** with the fundamental rights of an **unlimited number of applicants**, who would be **subject to profiling**; it should be balanced against the expected outcome of such a tool.

Furthermore, depending on the **method used** to develop the specific risk indicators, which could be construed in a very broad manner, **the number of people denied automated authorisation due to a hit based on the screening rules may be relatively high**, even though these persons do not actually present a risk.".

Step 3: proceed to the fair balance evaluation of the measure

When (and only then) the legislator has gathered **all required information** and performed the assessment of the importance and effectiveness and efficiency of the measure and of its

[54] Available at: https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf.

interference on privacy and on the protection of personal data, it should proceed to examining the fair balance of these two aspects.

In the presence of **information asymmetry**, for instance in the presence of known benefits but unknown costs, or *vice-versa*, it will be difficult, if not impossible, to establish whether the measure is proportionate, weighing up all the factors.

In practice, the proportionality principle requires establishing a **balance** between the extent and nature of the interference and the reasons for interfering (the needs), as translated into objectives effectively pursued by the measure. The CJEU underlined that *"[w]here several rights and fundamental freedoms protected by the European Union legal order are at issue, the assessment of the possible disproportionate nature of a provision of European Union law must be carried out with a view to* ***reconciling the requirements*** *of the protection of those different rights and freedoms and a* ***fair balance*** *between them*"[55].

In other words, the principle serves as an instrument for balancing conflicting interests according to a rational standard in cases where precedence is not given *a priori* to any of them[56].

In effect, there is a possible method for reviewing whether or not an EU legal act may be considered compatible with Articles 7 and 8 of the Charter and with the principle of proportionality under Article 52(1) of the Charter. Such method would stem in particular from the judgments of the CJEU referred to in these Guidelines, notably but not exclusively in the specific field of 'general programmes of surveillance'[57].

Guidance (how to proceed)

- First, *prior* to the balance exercise, verify if there is a situation of **information asymmetry**: *has all relevant information been collected and assessment performed on both the 'benefits' and the 'costs' of the measure?*
- Then, **compare** the constraints on privacy and data protection and the benefits (the **balancing** exercise): *are the measures envisaged to fulfil the objective a proportionate response to the need at the basis of a proposal for legislation, given the limitations to the data protection and privacy rights?*

---

[55] CJEU cases, C-283/11, *Sky Österreich GmbH v. Österreichischer Rundfunk* [GC], ECLI:EU:C:2013:28, para. 60; C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI: EU:C:2008:54, paras 65 and 66 and C-544/10, *Deutsches Weintor*, ECLI:EU:C:2012:526, para. 47; ECtHR judgment, *Big Brother Watch and others v United Kingdom*, 13 September 2018, "2.42. An examination of the proportionality of the application should particularly include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.".

[56] Specifically, see CJEU case C-28/08, *Bavarian Lager*, para. 56: "*Regulations Nos 45/2001 and 1049/2001 were adopted on dates very close to each other. They do not contain any provisions granting one regulation primacy over the other*.".

[57] In Opinion **4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems**, at page 12, the EDPS clarified that "the new data processing operations **aiming at correctly identifying the persons** constitute an **interference with their fundamental rights as protected by Articles 7 and 8 of the Charter**. Consequently, they must pass the necessity and proportionality tests (Article 52(1) of the Charter).".

- See also *S and Marper v United Kingdom*, ECtHR, para. 67: "The **mere storing of data relating to the private life of an individual** amounts to an interference within the meaning of Article 8 (...). The subsequent use of the stored information has no bearing on that finding (...). However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.".

- After performing the balancing exercise, ensure that adequate **evidence** is produced and, as the case may be, published, establishing that the **analysis has been done** (*Report on the Proportionality Test*, that is, a synthetic analysis of the **outcome** of the assessment performed).
- **Keep (register and store) all relevant documentation** obtained or produced while performing the **balancing** exercise and drafting the *Report on the Proportionality Test*. Such documentation should be relevant and sufficient to provide justification (or to identify the critical issues) for the measure under scrutiny (target of evaluation), and referred to in an annex to the Report[58].

Relevant examples

EXAMPLE 1: *Tele2 Sverige AB* (CJEU, C-203/15 and C-698/15, ECLI:EU:C:2016:970)

In *Tele2*, the Court held that: "*Given the **seriousness** of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, **only the objective of fighting serious crime** is capable of justifying such a measure (...)*" (emphasis supplied).

The Court had clear in mind, on one side, the importance and effectiveness of the measure; on the other side, the **scope** (not restricted to data pertaining to a particular time period and/or geographical area and/or to persons likely to be involved in serious crime) and the **level/intensity** (including **profiling**) of the interference.

[58] In his Opinion, ECLI:EU:C:2013:845, in joined cases C-293/12 and C-594/12, *Digital Rights*, the Advocate General pointed out the **lack of relevant and sufficient reasons** on the **two years data retention period** prescribed by the directive as a key factor for rejecting the proportionality of the two years data retention period (as opposed to the, justified, less than one year retention time). See paras. 148-149: "*[I]t may be considered that a retention period for personal data 'which is measured in months' is to be clearly distinguished from a period 'which is measured in years'. The first period would correspond to that falling within what is perceived as present life and the second to that falling within life perceived as memory. The interference with the right to privacy is, from that perspective, different in each case and the necessity of both types of interference must be capable of being justified. Although the necessity of the interference in the dimension of present time seems to be sufficiently justified, I have found **no justification for an interference extending to historical time**. Expressed more directly, and without denying that there are criminal activities which are prepared well in advance, I have not found, in the various views defending the proportionality of Article 6 of Directive 2006/24, any sufficient justification for not limiting the data retention period to be established by the Member States to less than one year*.".
- See also joined cases *Volker und Markus Schecke and Hartmut Eifert*, **C-92/09 and C-93/09**, ECLI:EU:C:2010:662, para. 81: "***There is nothing to show** that, when adopting Article 44a of Regulation No 1290/2005 and Regulation No 259/2008, the Council and the Commission took into consideration methods of publishing information on the beneficiaries concerned which would be consistent with the objective of such publication while at the same time causing less interference with those beneficiaries' right to respect for their private life in general and to protection of their personal data in particular (...)*." (emphasis supplied).
- In **Opinion 7/2018** on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents, 10 August 2018 (available at: https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en_0.pdf) in page 3 the EDPS "*observes that the Impact Assessment accompanying the Proposal **does not appear to support the policy option chosen** by the Commission, i.e. the mandatory inclusion of both facial images and (two) fingerprints in ID cards (and residence documents). (...) Therefore, the EDPS recommends to reassess the necessity and the proportionality of the processing of biometric data (facial image in combination with fingerprints) in this context*.".
- Similarly, in **Opinion 7/2017 on the new legal basis of the Schengen Information System**, 2 May 2017 (available at: https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdf), the EDPS, in page 3, considered "(...) *that the introduction of new categories of data, including new biometric identifiers, raises the question of the necessity and proportionality of proposed changes and for this reason the Proposals should be complemented with the impact assessment on the right of privacy and the right to data protection enshrined in the Charter of Fundamental Rights of the EU*.".

Having weighed up the one against the other, the Court held that: "*The effectiveness of the fight against serious crime* ***cannot in itself justify*** *that national legislation providing for the* ***general and indiscriminate retention*** *of all traffic and location data should be considered to be necessary for the purposes of that fight."* The measure *"therefore* ***exceeds the limits of what is strictly necessary*** *and cannot be considered to be justified, within a democratic society*" (emphasis supplied).

EXAMPLE 2: *Ministerio Fiscal* (CJEU, C-207/16, ECLI:EU:C:2018:788)

In *Ministerio Fiscal,* the Court held that the measure under scrutiny is **proportionate** (successfully passes the proportionality test, and is therefore lawful under both the necessity and the proportionality principles).

A key factor for this assessment is the fact that the interference had been considered as 'not serious', and therefore could not outweigh the ('equally' not serious/high) importance of the objective as effectively fulfilled by the measure.

Referring to the words of the Court: *"[W]hen* ***the interference*** *that (the measure) entails is* ***not serious****, (the measure) is capable of being* ***justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally***." On the contrary, "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'"** (emphasis supplied).

EXAMPLE 3: Opinion 1/15 *PNR Canada* (CJEU, ECLI:EU:C:2017:592)

The measure under scrutiny in this case is such as to present **information asymmetry** between the expected benefits and the impact on the fundamental right to privacy and to the protection of personal data. This is due in particular to the fact that **the categories of personal data** to be processed are not **clearly and precisely** worded; the rules applicable to the automated pre-screening of passengers are also **not specified** by the measure.

Indeed, such lack of specifications not only makes the comparability exercise impossible, but also brings the Court to the point of directly declaring the agreement, in its current version, **not** compatible with Articles 7 and 8 and Article 52(1) of the Charter.

EXAMPLE 4: *Bevándorlási és Állampolgársági Hivatal* (CJEU, C-473/16, ECLI:EU:C:2018:36)

In this case, the Court, having regard to all elements on the importance and effectiveness of the measure and on its interference (on a single specified person, in this case), concluded that: "*Article 4 of Directive 2011/95, read in the light of Article 7 of the Charter, must be interpreted as* ***precluding the preparation and use, in order to assess the veracity of a claim made by an applicant for international protection concerning his sexual orientation, of a psychologist's expert report****, such as that at issue in the main proceedings, the purpose of which is, on the basis of projective personality tests, to provide an indication of the sexual orientation of that applicant*" (emphasis supplied).

In other words, the Court found the measure under scrutiny **not proportionate**, due to the extremely serious interference of the measure, but also due to the lack of effectiveness in reaching the objective pursued.

EXAMPLE 5: *Scarlet Extended* (CJEU, C-70/10, ECLI:EU:C:2011:771)

This case is interesting because it shows that the **right to the protection of personal data** may play the role of a *concurring right*, that is not the one mainly affected by the measure, but which nonetheless, **together** with other rights (freedom to conduct business; freedom to receive or impart information), can tilt the balance in favour of the non-proportionality of the measure (pursuing the objective of better protecting intellectual property rights).

We report the most relevant excerpts of this ruling: "*the injunction to install the contested **filtering system** is to be regarded as not respecting the requirement that a **fair balance** be struck between, on the one hand, the **protection of the intellectual-property right** enjoyed by copyright holders, and, on the other hand, that of the **freedom to conduct business** enjoyed by operators such as ISPs.*

*Moreover, the effects of that injunction would not be limited to the ISP concerned, as the contested filtering system may **also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data** and their **freedom to receive or impart information**, which are rights safeguarded by Articles 8 and 11 of the Charter respectively. (...)*

*Consequently, it must be held that, in adopting the injunction requiring the ISP to install the contested filtering system, the national court concerned would **not be respecting the requirement that a fair balance** be struck between the **right to intellectual property**, on the one hand, and the **freedom to conduct business**, the **right to protection of personal data** and the **freedom to receive or impart information**, on the other*" (emphasis supplied).

EXAMPLE 6: EDPS Opinion 1/2017 on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC. Access to beneficial ownership information and data protection implications

In this Opinion, as well as in the Proposal, the objective is referred to as 'risk to be avoided' (in this case, the risk of money laundering and terrorism-financing). As a rule, the collection and processing of personal data, to be proportionate to the aim, should be 'adjusted to' (take into account) the risk (for instance, to the 'economic public order') posed by the persons concerned. This would allow the **optimisation** of the interference on the right to privacy and to the protection of personal data.

The EDPS Opinion on the Proposal amending the anti-money laundering directive noted that, contrary to the aforesaid approach: "the Proposal (...) removes existing safeguards that would have granted a certain **degree of proportionality**. For example, in setting the conditions for access to information on financial transactions by FIUs, the Proposal provides that, for the future, FIUs' [Financial Intelligence Units] need to obtain additional information may **no longer and not only be triggered by suspicious transactions** (as is the case now [so-called 'risk based approach' to anti-money laundering]), but also by FIUs' own analysis and intelligence, **even without a prior reporting of suspicious transactions**. The role of FIUs, therefore, is shifting from being "*investigation based*" to being "*intelligence based*". The latter approach is more similar to data mining than to a targeted investigation, with obvious consequences in terms of personal data protection.".

EXAMPLE 7: EDPS Video-Surveillance Guidelines

The same approach, consisting in finding out **the optimisation of the interference on the right to privacy and to the protection of personal data with the aim pursued by the measure** (for instance, security of premises), is applied in the EDPS Guidelines on Video-Surveillance: "Using a pragmatic approach based on the twin principles of selectivity and **proportionality,** video-surveillance systems can meet security needs while also respecting our privacy. Cameras can and should be used intelligently and should **only target specifically identified security problems** thus minimising gathering irrelevant footage. This not only minimises intrusions into privacy but also helps ensure a **more targeted, and ultimately, more efficient**, use of video-surveillance." Specific indications are provided in the Guidelines (among others, on: camera locations and viewing angles; number of cameras; times of monitoring; resolution and image quality; special categories of data; areas under heightened expectations of privacy; high-tech and/or intelligent video-surveillance; interconnection of video-surveillance systems).

EXAMPLE 8: EDPS Opinion 5/2015 on the Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

"The essential prerequisite for a PNR scheme -*i.e.* compliance with necessity and **proportionality** principles- is still **not met in the Proposal**. The Proposal (...) does not set forth any detailed analysis of the extent to which less intrusive measures could achieve the purpose of the EU PNR scheme. Finally, the non-targeted and bulk collection and processing of data of the PNR scheme amount to a measure of general surveillance. In the view of the EDPS, the only purpose which would be compliant with the requirements of transparency and proportionality, would be the use of PNR data on a case-by-case basis but only in case of a serious and concrete threat established by more specific indicators. Since there is **no information available to the effect that the necessity and proportionality of the measures proposed have been adequately demonstrated**, the EDPS considers that the Proposal, **even modified, still does not meet** the standards of Articles 7, 8 and 52 of the Charter of Fundamental Rights of the Union, Article 16 of the TFEU and Article 8 of the ECHR. The EDPS would encourage the legislators to further explore the feasibility against current threats of **more selective and less intrusive surveillance measures based on more specific initiatives focusing, where appropriate, on targeted categories of flights, passengers or countries**.".

Step 4: analyse conclusions on the proportionality of the proposed measure. *If* the conclusion is 'not proportionate', identify and introduce safeguards which could make the measure proportionate.

If the balancing exercise as described under Step 3 leads to the conclusion that a proposed measure does **not** comply with the requirement of proportionality, then either the measure should **not be proposed**, or it should be **modified** so as to comply with these requirements.

Guidance (how to proceed)

- Synthetically analyse the **outcome** of the assessment performed under step 3 as described in the *Report on the Proportionality test*, highlighting in particular **the factors** that gave rise to the conclusion of 'non-proportionality' ('negative proportionality test');
- **Rework** the proposal, drafting if possible one or more **corrective options** addressing the critical issues (**define** more narrowly the purpose, the categories and the amount of personal data to be processed[59], and thus reduce the level of interference of the measure with privacy and data protection);
- Envisage and introduce **safeguards** reducing the impact of the proposal on the fundamental rights at stake (*for example*, introduce the need for human verification in case of legislation providing for fully automated measures)[60].

[59] As example, see **formal comments of the EDPS on the Proposal for a Directive of the European Parliament and of the Council on credit servicers, credit purchasers and the recovery of collateral**, recommending to better define the categories and amount of documents (containing personal data) to be processed pursuant to the Proposal, at page 3. The formal comments are available at: https://edps.europa.eu/sites/edp/files/publication/19-01-24_comments_proposal_directive_european_parliament_en.pdf.

[60] As example of **safeguards**, see **EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems**, page 16: "[t]he different instruments also require the **verification by an independent authority** that the above conditions are met prior to the access. In case of the ETIAS, the EES, and the Eurodac system, the law enforcement authorities are also required to **first consult other relevant systems** (e.g. national databases, Europol data, Prüm, the VIS).".
- See also the FRA Opinion on "Interoperability and fundamental rights implications", 11 April 2018, with regard to the need of differential treatment (safeguards) for vulnerable persons, remarks (page 33): "Replacing the cascade system with a streamlined mechanism, such as the proposed hit/no hit check against the Common Identity

- Provide for **re-evaluation** and **sunset clauses**: most probably the situation to be addressed is characterised by a very dynamic environment, from both the technological and societal viewpoint. This uncertainty may have contributed to the assessment of the measure as non-proportionate for 'prudential reasons' (precautionary principle), due to uncertainties on the effective impact of the measure (for example, due to the envisaged technological tools). In this case, in addition to further safeguards, it is advisable to provide for strict **re-evaluation** (regular checks/evaluation of the impact *post factum*, also aiming at addressing unexpected effects) and **sunset clauses** ('unless conformed or revised, the measure is *no longer applicable as from'*). **Specific oversight** mechanism/bodies might also be considered[61].
- **Re-run** the assessment of necessity and proportionality (both tests, since the introduced modification may trigger the need to perform again each step of test 1 and 2).

Relevant examples

EXAMPLE 1: *Tele2 Sverige AB* (CJEU, C-203/15 and C-698/15, ECLI:EU:C:2016:970)

The **outcome** of the assessment of proportionality (referred to as 'strict necessity') in *Tele2* is **negative**. The Court points out to the **factors** that determined its negative assessment: in particular, such factors relate to the (lack of) relationship between the data which must be retained and the threat to public security, countering which is the objective of the measure (see para. 106 of the judgment).

A contrario, the Court also expressly laid down the features of the proportionate measure. In particular, the measure "*must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions*

Repository means that data of all persons are considered equally sensitive and that data of persons in a **vulnerable situation** (such as that of persons seeking international protection) would not require **enhanced safeguards**.".
- Concerning safeguards (human verification, meaningful explanations, reporting) in the context of a possible use of automated measures, see **EDPS formal comments on the Commission proposal on the prevention of dissemination of online terrorist material**, at page 8: "Article 8(1), under the "transparency obligations", provides that HSPs should set out in their terms and conditions their policy on the prevention of terrorism content, "including, **where appropriate**, a meaningful explanation of the functioning of proactive measures including the use of automated tools" (emphasis added). Moreover, Article 9(1) provides that HSPs using automated tools shall introduce effective and appropriate safeguards to ensure that decisions taken in particular to remove or disable content are accurate and well-founded. Article 9(2) specifies that such safeguards shall consist of "human oversight and verifications **where appropriate** and, in any event, where a detailed assessment of the relevant context is required [...]" (emphasis added). Having regard to these safeguards, the EDPS recommends replacing in Article 8(1) and 9(2) the wording "where appropriate" with "in any case", or, alternatively, deleting the wording "where appropriate". The EDPS also notes that, pursuant to Article 6(2), HSPs should submit a report on the proactive measures taken, including the ones based on automated tools, to the authority competent to oversee the implementation of proactive measures under Article 17(1)(c). The EDPS recommends specifying in the Proposal, under Recital 18, that HSPs should provide the competent authorities with all necessary information about the automated tools used to allow a thorough public oversight on the effectiveness of the tools and to ensure that they do not produce discriminatory, untargeted, unspecific or unjustified results." The formal comments are available at:
https://edps.europa.eu/data-protection/our-work/publications/comments/formal-comments-edps-preventing-dissemination_en.

[61] See **WP29 Working document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees),** WP237 of 13 April 2016, Section 6, "Guarantee C - **An independent oversight mechanism should exist**", pages 9-10. The document is available at:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary. Second, (...) the retention of data must (...) meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to ***identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences****, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a* ***geographical criterion*** *where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences*" (emphasis supplied).

Other **conditions** for the proportionality of the measure, and concerning access by the law enforcement authorities to the retained data, are laid down in paras. 120-122, namely the prior review by a Court or by an independent administrative body; the notification, as soon as this is not liable to jeopardise investigations, to the person affected; the provision for the data to be retained in the European Union; the provision for the irreversible destruction of the data at the end of the retention period. These other conditions can in reality be consider as **safeguards**, which, together with the definition of the scope of the measure, can make the measure proportionate.

The judgment also refers to the "*review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (see, to that effect, the Digital Rights judgment, paragraph 68, and the judgment of 6 October 2015, Schrems, C-362/14, paragraphs 41 and 58)*" (emphasis supplied). This last requirement pertains to the condition of the **respect of the essence of the fundamental right** and falls under **test 1 (Necessity test)**.

So far, the legislator **did *not* put forward a new proposal** for a data retention Directive. If it decides to do so, it should go through both tests 1 and 2, namely the Necessity and the Proportionality tests.

EXAMPLE 2: *Ministerio Fiscal* (CJEU, C-207/16, ECLI:EU:C:2018:788)

In *Ministerio Fiscal*, the measure was considered by the Court **proportionate** to the aim. No remark was made by the Court concerning critical issues to be addressed by the legislator. Hence, there is no need to rework the measure (redefine the purpose, the scope, the level of interference; provide for more or different safeguards) and/or to **re-run** the assessment of necessity and proportionality.

EXAMPLE 3: Opinion 1/15 *PNR Canada* (CJEU, ECLI:EU:C:2017:592)

The Court considered the measure **not** compatible with Articles 7 and 8 and Article 52(1) of the Charter. The factors giving rise to such final evaluation basically concerned: a) the lack of clarity and specification of the measure (and hence to the impossibility of measuring the impact); b) the lack of safeguards (e.g., control by an independent authority).

At the same time, the Court **detailed the conditions** (preceded by the wording '*provided that'*, '*in so far as*') that would make the measure proportionate. Hence, on the one side, the discretion of the legislator in this case is quite reduced, since it will have to follow the punctual instructions provided by

the Court. At the same time, the work of the legislator is clearly facilitated since, following the Court's advice when redrafting the measure, it should be safe from the risk of another declaration of incompatibility by the Court.

EXAMPLE 4: *Bevándorlási és Állampolgársági Hivatal* (CJEU, C-473/16, ECLI:EU:C:2018:36)

The Court considered that Article 7 of the Charter must be interpreted as **precluding** the preparation and use, in order to assess the veracity of a claim made by an applicant for international protection concerning his sexual orientation, of a psychologist's expert report, such as that at issue in the main proceedings, the purpose of which is, on the basis of projective personality tests, to provide an indication of the sexual orientation of that applicant.

In this case, it seems difficult, given in particular the **very high intensity** of the interference, to foresee **safeguards** that could make proportionate the recourse to the measure under scrutiny.