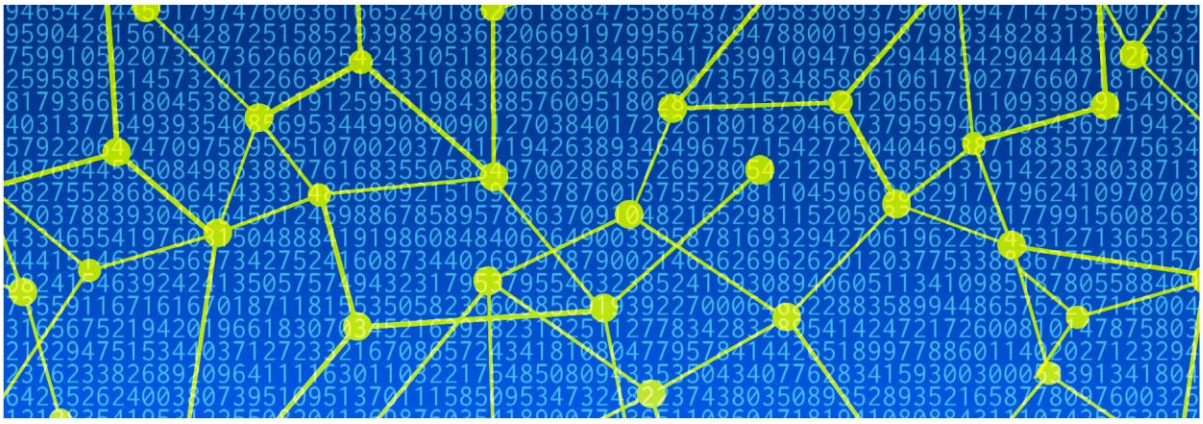


EUROPEAN DATA PROTECTION SUPERVISOR

# Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights

## Background paper

- for consultation -

EDPS

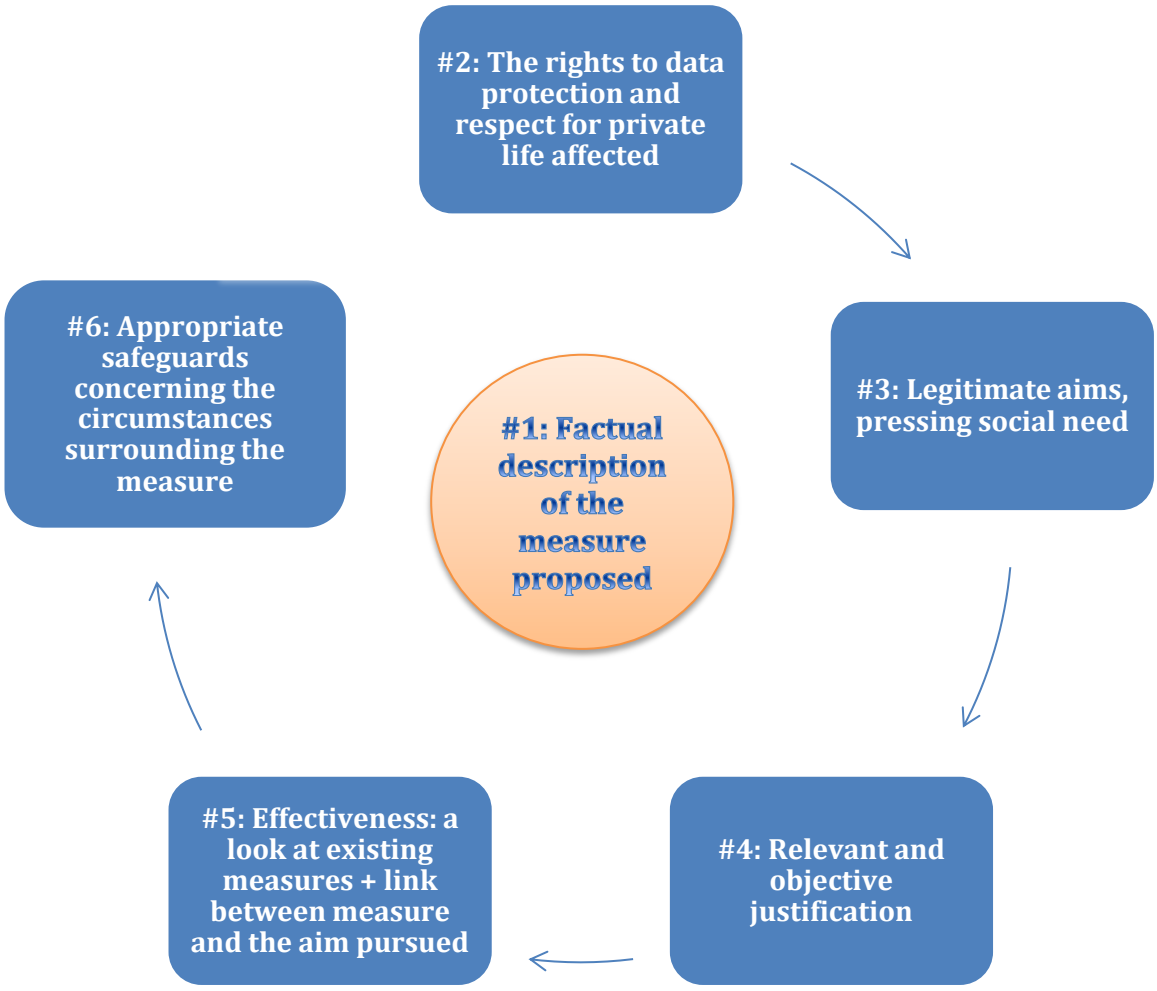
16 June 2016

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

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

*The initiative to issue a "toolkit" based on this background paper and following a stakeholders' consultation relates to the EDPS' mission to advise the EU institutions on the implications for fundamental rights and in particular the rights to privacy and to data protection of specific policies and measures, including legislative measures. It is in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. With the "toolkit" that will result from the consultation the EDPS hopes to equip better EU policymakers and legislators responsible for preparing and scrutinising measures that involve processing of personal data and which are likely to interfere with the rights to privacy and to data protection and with other rights and freedoms laid down in the Charter of Fundamental Rights of the EU.*

# NECESSITY


#2: The rights to data protection and respect for private life affected
#3: Legitimate aims, pressing social need
#4: Relevant and objective justification
#5: Effectiveness: a look at existing measures + link between measure and the aim pursued
#6: Appropriate safeguards concerning the circumstances surrounding the measure
#1: Factual description of the measure proposed

# TABLE OF CONTENTS

## Contents

## I. Purpose of this document

When designing and implementing new policies, or when adopting any new legislative measure the EU institutions and bodies must respect the Union's core values, which include the protection of fundamental rights[1] as laid down in the Charter of Fundamental Rights of the European Union (hereinafter, the Charter). As the independent advisor to the EU institutions and bodies under Regulation (EC) No. 45/2001 on all matters concerning processing of personal data, the EDPS aims at assisting in the difficult task of ensuring that any limitations on the exercise of the fundamental rights to personal data protection and the respect of private life are compliant with the requirements of EU primary law.

Once adopted, the "toolkit" will provide guidance on the requirement stemming from EU primary law that any interference with or limitation on the exercise of the right to the respect for private life (Article 7 of the Charter, based on Article 8 of the European Convention on Human Rights - ECHR) or the right to personal data protection (Article 8 of the Charter) must be "necessary" (Article 52 of the Charter). It is based on the case law[2] of the Court of Justice of the EU (CJEU), the European Court of Human Rights (ECtHR), previous Opinions of the EDPS and of the Article 29 Working Party. Before issuing the "toolkit", the EDPS is launching a public consultation on the background paper.

"Necessity" is also a recurrent condition in almost all the requirements on the lawfulness of the processing of personal data stemming from EU secondary law[3]. However, necessity of processing operations in EU secondary law and necessity of the limitations on the exercise of fundamental rights refer to different concepts. The former is outside the scope of this background paper.

While the background paper and the toolkit, once adopted, will focus on the assessment of necessity of any limitation on the exercise of the fundamental rights protected by the Charter, the limitations, in addition, must comply with the following set of criteria, as laid down in Article 52(1) of the Charter:

- limitations must be provided for by law,
- they must respect the essence of the right,
- once proved necessary, they must comply with the principle of proportionality, and
- they must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

**The test of necessity should be considered as the first step with which a proposed measure involving processing of personal data must comply.**

Once adopted, the "toolkit" will be useful for any legislative measure and any policy which limits the exercise of fundamental rights, irrespective of their field of application. It is all the more relevant today, when the EU is faced with the difficult task of proposing and adopting measures that address the current security challenges of the EU while complying at the same time with the right to personal data protection and the right to respect for private life[4]. The Paris and Brussels terrorist attacks of 2015 and 2016 triggered an immediate response from EU. Adoption of legislative proposals under debate for some years[5] was accelerated and packages of new proposals[6] were announced. All of these measures – whether already

adopted, currently under debate or merely announced in Communications - have in common that they increasingly use personal data in new, complex ways and interfere in the private sphere of individuals[7]. This raises concerns with regard to respect for fundamental rights.

This paper provides a short background on the role of necessity in the limitation on the exercise of the rights to data protection and respect for private life and proposes a checklist to guide the legislator in assessing necessity, composed of specific questions and supported by concrete examples from case law and practice.

## II. The importance of necessity in limiting the exercise of the rights to data protection and to respect for private life

### 1. The Charter and the ECHR

Following the entry into force of the Lisbon Treaty, the Charter has become the main reference for assessing compliance of EU secondary law with fundamental rights[8]. Settled case-law of the CJEU states that the ECHR "does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law"[9]. In consequence, the CJEU has affirmed in recent case law that an examination of the validity of a provision of secondary EU law "must be undertaken solely in the light of the fundamental rights guaranteed by the Charter"[10].

However, in accordance with Article 6(3) TEU, the CJEU has also recalled that the specific provisions of the ECHR must be taken into account "for the purpose of interpreting" the corresponding provisions of the Charter[11]. In particular, 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". Moreover, the Charter itself requires that in so far as it contains "rights which correspond to rights guaranteed by the [ECHR], the meaning and scope of those rights shall be the same as those laid down by [ECHR]" (Article 52(3) of the Charter).

**Therefore, while the main reference when assessing the necessity of measures that limit the exercise of the rights guaranteed under Articles 7 and 8 of the Charter is Article 52(1) of the Charter and how it is applied by the CJEU, the criteria in Article 8(2) ECHR - and specifically the condition for an interference to be necessary in a democratic society[12], as interpreted in the ECtHR case-law must also be taken into account in the analysis.**

### 2. Relationship between the necessity requirements in the Charter and the ECHR with regard to interference in private life and data protection

The notion of necessity is central to European human rights law in any assessment of the lawfulness and legitimacy of measures which interfere with or limit the exercise of fundamental rights[13]. There are, nevertheless, some differences between the requirements of necessity when limiting the exercise of rights under the Charter, on the one hand, and under the ECHR, on the other hand.

Article 52(1) of the Charter is a general, comprehensive provision, which sets the same criteria for restrictions of any of the fundamental rights prescribed in the Charter. The

requirement for the limitation to be *necessary* is one of them. In contrast, the ECHR provides different criteria for the restriction of each fundamental right, which have been further developed by the case law of the ECtHR. In particular, the ECHR imposes different standards of necessity, from *absolutely necessary* (the right to life), to *strictly necessary* (the right to a fair trial), to *necessary in a democratic society* (the rights to respect for private life, freedom of expression, freedom of thought etc.), to simply *necessary* (protection of property).

The right to respect for private life (which the ECtHR has interpreted to embrace the processing of personal data) is enshrined in Article 8 of the ECHR. The second paragraph of this article provides that any interference with the exercise of the right to private life must be provided for by law and must be *necessary in a democratic society* for the legitimate aims enumerated therein or for the protection of the rights and freedoms of others. The ECtHR, interpreting this condition, found that "necessity" does not have the flexibility of expressions such as "admissible", "ordinary", "useful", "reasonable", "desirable", but necessity "implies a pressing social need"[14]. In addition, ECtHR suggests that "strictly necessary" is synonymous with "indispensable"[15].

## 3. Relationship between proportionality and necessity under EU law

With regard to the relationship between the concepts of necessity and proportionality, it should be recalled that proportionality 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 treaties"[16]. 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". 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)"[17].

According to 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 (...)". Therefore, before subjecting any such limitation to the principle of proportionality, it must first be ascertained that the limitation is necessary. Even if not always explicit, this sequencing of the lawfulness test for limitations of fundamental rights is reflected in the case law of the CJEU in the field of data protection[18]. Moreover, in the recent *Schrems* ruling where the CJEU found that a legal act of the Union was not compliant with the Charter, the Court did not even go on to assess proportionality after finding that the limitations to the rights in Articles 7 and 8 of the Charter were not strictly necessary[19].

## 4. Limitations on the exercise of the rights to respect for private life and data protection must be *strictly necessary*

The case law of the CJEU and the ECtHR, converge in applying a *strict necessity* test for any limitations on the exercise of the rights to personal data protection and respect for private life: "the right to respect for private life requires that derogations and limitations in relation to the protection of personal data **must apply only in so far as is strictly necessary**"[20]. This confirms the important role that necessity plays in the lawfulness of measures that interfere in the private sphere of individuals.

**EXAMPLE 1:** *Satamedia* (CJEU, Case C-73/07, 16.12.2008)

In a judgment preceding the entry into force of the Treaty of Lisbon and, hence, the binding effect of the Charter, the CJEU already referred to balancing the fundamental right to freedom of expression and the fundamental right to privacy by requiring that "the derogations and limitations in relation to the protection of data provided for in the chapters of the [Directive 95/46] must apply only in so far as is strictly necessary" (paragraph 56). This is the first case where the CJEU applies the strict necessity test to limitations of the rights to respect for private life and the protection of personal data.

In addition, the CJEU has recently affirmed that the strict necessity test applies above all other conditions for lawfulness of EU legislation involving the limitation on the exercise of the fundamental rights guaranteed by Articles 7 and 8 of the Charter.

**EXAMPLE 2:** *Schrems* (CJEU, Case C-362/14; 6.10.2015)

After enumerating a list of specific conditions regarding the minimum safeguards needed for legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter, such as laying down clear and precise rules governing the scope and application of a measure (paragraph 91), the Court affirms that (emphasis supplied) "furthermore, **and above all**, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply **only in so far as is strictly necessary**" (paragraph 92). In Schrems, the CJEU concluded that "**legislation is not limited to what is strictly necessary** where":
1) it authorises, on a generalised basis, **storage of all the personal data of all the persons** whose data has been transferred from the European Union to the United States,
2) **without any differentiation, limitation or exception** being made in the light of the objective pursued and
3) **without an objective criterion** being laid down by which **to determine the limits of the access of the public authorities** to the data, **and of its subsequent use**,
4) **for purposes which are specific, strictly restricted and capable of justifying the interference** which both access to that data and its use entails (paragraph 93).

The ECtHR also applies a test of *strict necessity* when assessing the compliance of interferences to the right to respect for private life, as enshrined in Article 8 of the ECHR.

**EXAMPLE 3:** *Klass and others v. Germany*, (ECHR, 5029/71, 6.09.1978)

In *Klass and others*, the ECtHR, before applying the complex test in Article 8(2) of the ECHR to the measures analysed, first established that "*this paragraph* (i.e. Article 8(2)) *is to be narrowly interpreted*" and that "*powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention* ***only in so far as strictly necessary for safeguarding the democratic institutions***" (paragraph 42). Only in the following paragraphs does the ECHR start to assess the criteria laid down in Article 8(2) of the Convention, starting with the condition that the interference is provided for by law.

**EXAMPLE 4:** *Szabo and Vissy v. Hungary* (ECHR, 37138/14, 12.01.2016)

The ECtHR took into account "the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy" in order to state that "the requirement 'necessary in a democratic society' must be interpreted in this context as requiring strict necessity in two aspects", i.e. for the safeguarding of the democratic institutions in general, and for obtaining of vital intelligence in an individual operation in particular (paragraph 73).

**Having regard to all of the above, following a stakeholders' consultation the EDPS will propose a checklist of criteria for the EU institutions and bodies to follow when assessing the necessity of any proposal that involves interference with the rights guaranteed under Articles 7 and 8 of the Charter. For instance, this analysis could be part of the Impact Assessment accompanying relevant legislative proposals[21].**

### 5. Necessity in data protection law, a facts-based concept

An analysis of the case law of the CJEU and ECtHR also indicates that necessity in data protection law is a facts-based concept, rather than an abstract legal notion – necessity is a consequence of the factual details of a processing operation, considered in the light of the circumstances surrounding the adoption of the measure and the concrete purpose it aims to achieve.

For instance, the ECtHR made it clear that the necessity in a democratic society of a measure depends on all the circumstances of the measure.

**EXAMPLE 5:** *Zacharov v. Russia* (ECHR, 47143/06, 4.12.2015)

The Court declared that when assessing whether an interference with the right to private life is necessary in a democratic society, it must be satisfied that there are **adequate** and **effective** guarantees against abuse, "in view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it (our emphasis - n.)" (paragraph 232). It further added that "**the assessment depends on all the circumstances of the case**, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (emphasis supplied)" (paragraph 232).

## III. Checklist for assessing necessity of new legislative measures

The checklist is likely to consist of six steps. Since necessity is a direct consequence of the factual reality of a given measure, the first step (**Step #1**) is preliminary and it implies a detailed factual description of the measure proposed and its purpose, in the absence of any substantive assessment.

The following five steps imply an assessment of the details resulting from the first step. Each step, to be addressed consecutively, corresponds to a set of questions which will facilitate the assessment.

- **Step #2** will help identify if the proposed measure represents an interference with fundamental rights - in particular the rights to data protection or respect for private life, but possibly also with other rights, like effective judicial redress, freedom of expression or non-discrimination. The condition of necessity is only triggered if there is interference with any of the fundamental rights. Otherwise, no further analysis is needed;
- **Step #3** assesses several conditions linked to the objective of the measure;
- **Step #4** provides guidance with regard to the objective evidence needed to propose the measure;
- **Step #5** assesses the effectiveness of the measure;
- **Step #6** facilitates the analysis of whether the specific obligations and rights created by the measure comply with strict necessity requirements as developed by the CJEU.

**If the assessment of any of the elements detailed in Steps #2 to #6 leads to the conclusion that a measure does not comply with the requirement of necessity, then the measure should either not be proposed, or it should be modified so as to comply with these requirements.**

## #1: Factual description of the measure proposed

**Guidance**

- ✓ The measure needs to be described so as to enable a clear understanding of what exactly is being proposed.
- ✓ This description will enable identification of the rights and freedoms affected and will help assess the seriousness of the interference. At the same time, it will facilitate the application of conditions already established by the CJEU in particular cases, to assess whether the measure is necessary.
- ✓ It is important to precisely identify what the proposed measure entails in terms of personal data processing and what the objective of the measure is.

**Ask yourself:**

What is the purpose of the measure?

Why is this specific measure needed?

Describe the measure.

- Does it imply use of personal information?
- If yes, what kind of personal information? Information related to whom?
- How is the personal information used?
- Are there authorities involved? Are there private parties involved?

## #2: Fundamental rights and freedoms affected

**Guidance:**

- ✓ If the proposed measure involves the use of personal data, it must respect the right to personal data protection (see Section 4) and it may interfere with the right to respect for private life[22].
- ✓ In this respect, the settled case law of the CJEU states that "**to establish the existence of an interference** with the fundamental right to respect for private life, **it does not matter whether the information is sensitive or whether the persons concerned have been inconvenienced in any way**"[23], whereas the ECtHR, for instance, repeatedly held that the storing by a public authority of data relating to the private life of an individual amounts to an interference with the right to respect for his private life[24] and that the use made of them has no bearing on that finding[25].
- ✓ If the measure involves access of the competent national authorities to the data processed, such access constitutes a further interference with the fundamental right to respect for private life[26].
- ✓ **Other rights and freedoms may be affected** by the proposed measure, independent of the use of personal data, which triggers subsequent analysis. For instance, the right to effective judicial redress may be affected[27], or the right to non-discrimination[28], or the right to freedom of expression[29].
- ✓ The **nature of the rights** affected, together with **the nature and seriousness of the interference** with those rights, the **area concerned** and **the object pursued** by the interference - which can be assessed based on the factual details of the measure, may lead to **a reduced discretion of the EU legislature to adopt a measure**[30] (for the assessment of the object pursued).
- ✓ If the proposed measure uses sensitive data, a higher threshold should be used in the assessment of necessity. For instance, biometric data are peculiar in nature, being unequivocally linked to the individual, whose body is made "readable"[31].

**Ask yourself:**

**Does the measure proposed involve in any way the use of personal information?**

- If yes, how is it used (e.g. collected, stored, transferred etc.)?
- Who has access to it?

**Which are the fundamental rights and freedoms affected?**

- Is there a "difference of treatment" created between individuals which could lead to discrimination?
- Are there any consequences for the possibility of individuals to seek judicial remedies?
- Are there any consequences on freedom of speech, freedom of thought, freedom to receive information?

**How are the fundamental rights and freedoms affected?**

- How many persons are affected?
- What are the consequences of the processing of the personal information?

**To do:**

- ✓ If neither of the fundamental rights to data protection and to respect for private life are affected, the following analysis is not necessary.
- ✓ If one or more fundamental rights are affected, the mere fact that a measure limits the exercise of fundamental rights does not as such mean that the measure should not be proposed. It means, however, that the measure must comply with the conditions for it to be lawful, as laid down in Article 52(1) of the Charter. **The following steps to assess necessity are particularly relevant for measures limiting the rights to data protection and respect for private life.** They may also be used to assess necessity in the other areas mentioned above, where relevant.

**Relevant examples:**

**EXAMPLE 6:** *Schrems* (CJEU, Case C-362/14; 6.10.2015)

In *Schrems*, the CJEU found that the same legislation which affected the essence of the right to respect for private life also touched upon the essence of the right to an effective judicial remedy. "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" (paragraph 95).

**EXAMPLE 7:** *Huber* (CJEU, Case C-362/14; 6.10.2015)

The Court assessed the lawfulness of a database set up by the German authorities, which included personal data on third country nationals and other EU citizens that did not hold the German citizenship. One of the findings of the Court was that **the right to non-discrimination** between EU nationals "must be interpreted as meaning that it precludes the putting in place by a Member State, for the purpose of fighting crime, of a system for processing personal data specific to Union citizens who are not nationals of that Member State" (paragraph 81). To reach this conclusion, the Court took into account that the fight against crime "necessarily involves the prosecution of crimes and offences committed, irrespective of the nationality of their perpetrators" (paragraph 78). "It follows that, as regards a Member State, the situation of its nationals cannot, as regards the objective of fighting crime, be different from that of Union citizens who are not nationals of that Member State and who are resident in its territory" (paragraph 79).

**EXAMPLE 8:** *EDPS Opinion 3/2016 Opinion on the exchange of information on third country nationals as regards the European Criminal Records Information System (ECRIS), 13.4.2016*

The legislative proposal aimed to create a special system for exchanging information between the Member States on convictions of third country nationals, which would also contain data on EU nationals that have the nationality of a third country. They would, therefore, be treated differently than the EU nationals that do not possess the nationality of a third country. The EDPS found that "t*he difference of treatment contained in the proposal does not seem to be necessary to achieve the objective pursued, considering that for EU nationals the existing procedures of ECRIS can be applied*

*in order for authorities to share information*" and that "*this difference of treatment may result in discrimination, which would breach Article 21(1) of the EU Charter*" (paragraph 33).

## #3: Objectives

**Guidance:**

- ✓ The **purpose** of the measure **must genuinely meet an objective of general interest recognised by the Union** (see Example 10) **or the need to protect the rights and freedoms of others.**
- ✓ An interference will be considered by the ECtHR "necessary in a democratic society" for a legitimate aim "if it answers a pressing social need, (and, in particular, if it is proportionate to the legitimate aim pursued) and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'"[32](for the assessment of the reasons adduced, see #4 below).
- ✓ The **problem** to be addressed must be "pressing", which means that it must be real, present or imminent, critical for the functioning of the society.

**Ask yourself:**

What is the problem to be addressed?

Is the problem pressing, critical for the functioning of the society?

What is the purpose of the measure?

- Is the purpose clear and precise?

**To do:**

- ✓ If the problem to be addressed is not pressing, or the purpose of the measure is not precise, then the measure is not necessary and it should not be proposed.

**Relevant examples:**

**EXAMPLE 9**: *Leander v. Sweden*, (ECHR, 9248/81, 26.03.1987)

When assessing the "pressing social need" criterion, the ECHR found that "*there can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power, firstly, to collect and store in registers not accessible to the public information on persons and, secondly, to use this information when assessing the suitability of candidates for employment in posts of importance for national security*" (paragraph 59). Therefore, the Court accepted that "the margin of appreciation available to the respondent State in assessing the pressing social need in the present case, and in particular in choosing the means for achieving the legitimate aim of protecting national security, was a wide one" (paragraph 59).

**EXAMPLE 10:** *Digital Rights Ireland* (CJEU, Joined Cases C-293/12 and C-594/12, 8.04.2014)

When assessing the lawfulness of the Data Retention Directive (Directive 2006/24), the CJEU took into account the conclusions of the Justice of Home Affairs Council of 19 December 2002 that data related to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime, because of the significant growth in the possibilities afforded by electronic communications (paragraph 43). The CJEU also acknowledged that in its case law it found that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest. The same is true of the fight against serious crime in order to ensure public security (paragraph 42). Therefore the Court held that "*the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24 genuinely satisfies an objective of general interest*" (paragraph 44).

**EXAMPLE 11:** *Schecke* (CJEU, Joined Cases C-92/09 and C-93/09, 9.11.2010)

The CJEU found that publication of the names of the beneficiaries of aid from the European Agricultural funds and of the amounts which they receive from those Funds, as it is intended to enhance transparency regarding the use of European funds and improve sounds financial management of these funds, in particular by reinforcing public control of the money used, pursue an objective of general interest recognized by the EU (paragraphs 67 to 71).

## #4: Justification

**Guidance:**

- ✓ The **reasons** why action is needed must be detailed by the legislator.
- ✓ The **objective evidence** must be convincingly supported by documents and available statistics and they must constitute valid references.
- ✓ The documentation must be relevant, accurate and sufficient.

**Ask yourself**:

Why is this measure being proposed?

What is the objective evidence justifying the need for the measure?

- Which are the documents and statistics available?

Is the evidence relevant and sufficient?

**To do**:

- ✓ If there is no objective evidence justifying the need for the proposed measure, or if the existing evidence is not relevant or sufficient, the measure should not be proposed.

**Relevant examples**:

**EXAMPLE 12:** *S. and Marper v. UK* (ECtHR, 30562/04 and 30566/04, 4.12.2008)

The ECHR criticised the UK because their **evidence** supporting a DNA and fingerprint database did not "*reveal the extent to which the measure resulted in convictions of the persons concerned or the number of convictions that were contingent on the retention of the samples of unconvicted persons; demonstrate that the high number of successful matches ... was only made possible through ... retention of ... records of all such persons*" (paragraph 116).

**EXAMPLE 13:** *EDPS Opinion on the Proposal for a Directive of the EP and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime,* Brussels, 25.03.2011.

The EDPS noted that the Impact Assessment of the proposed directive included extensive explanations and statistics to justify the Proposal, but that these elements were not convincing. As an illustration, the description of the threat of terrorism and serious crime in the impact assessment and in the explanatory memorandum of the Proposal cited the number of 14.000 criminal offences per 100.000 population in the Member States in 2007. While this number was impressive, it related to undifferentiated types of crimes and cannot be of any support to justify a Proposal aiming and combating only a limited type of serious, transnational crimes and terrorism. As another example, citing a report on drug "problems" without linking the statistics to the type of drug trafficking concerned by the Proposal did not constitute, in the view of the EDPS, a valid reference (paragraph 11). The EDPS concluded that the background documentation was not relevant and accurate so as to demonstrate the necessity of the instrument (paragraph 12).

## #5: Effectiveness

**Guidance:**

- ✓ In order for a measure to be necessary to meet the identified need, it must be **essential** to meet that need rather than being the most convenient or cost effective[33].
- ✓ There must be **a link between the limitation or interference and its intended protective function** for one of the legitimate aims identified, which means that the objective pursued must be achieved as a direct consequence of the limitation.
- ✓ It should also be assessed whether the resulting loss of privacy is proportionate to any anticipated benefit. "If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate"[34] (see also Example 16).
- ✓ There must be **a link between the information used** by the measure and the **objective pursued**[35].
- ✓ In addition, not everything that "might prove to be useful" for a certain purpose is "desirable or can be considered as a necessary measure in a democratic society"[36].

**Ask yourself:**

Is the measure essential for satisfying the need to be addressed?

Are there existing measures that could achieve the same purpose if they were effectively applied and enforced?

Do the benefits of the measure outweigh the detrimental effects?

**To do:**

- ✓ If the measure is not essential to satisfy the need to be adressed, or if existing measures are already in place that can achieve the same purpose if they were effectively applied, or if the benefits of the measure do not outweigh the detrimental effects, then the measure is not necessary.

**EXAMPLE 14:** *Österreichischer Rundfunk and Others* (CJEU, Cases C-465/00, C-138/01 and C-139/01, 20.05.2003)

When assessing whether the publication of names together with income of employees of different public bodies that were subject to control by the Court of Auditors was compliant with the right to private life, the CJEU took into account that "the interest of the Republic of Austria in ensuring the best use of public funds, and in particular keeping salaries within reasonable limits, must be balanced against the seriousness of the interference with the right of the persons concerned to respect for their private life" (paragraph 84). The Court observed that the information at issue is not only communicated to the supervisory body (Court of Auditors) and to the competent parliamentary bodies, but is also made widely available to the public (paragraph 87). The CJEU invited the national courts to examine whether the objective pursued by such a wide publication "could not have been attained **equally effectively** by transmitting the information as to names to the monitoring bodies alone" (paragraph 88).

**EXAMPLE 15:** *The EDPS Video-surveillance guidelines*, Brussels, 17.03.2010

In guidance issued to the EU institutions to assess whether video-surveillance measures are necessary, the EDPS highlighted that "systems should not be installed if they are not effective in achieving their purposes, for example, if they merely provide the illusion of greater security" (paragraph 5.4). "Vide-surveillance should not be used if adequate alternatives are available. An alternative can be considered adequate unless it is not feasible or significantly less effective than video-surveillance or would involve disproportionate costs. Mere availability of the technology at a relatively low cost is not sufficient to justify the use of video-technology. One should refrain from simply making the choice which appears to be the least expensive, easiest and quickest decision, but which fails to take into

account the impact on the impact on the data subject's legitimate interests and the effect on their fundamental rights" (paragraph 5.5).

**EXAMPLE 16:** *EDPS letter on "Prior checking notification concerning "Processing of leave and flexitime"*, 13.10.2014

In the context of a Prior Check notification pursuant to Article 27 of Regulation 45/2001 of a measure that was proposing the use of fingerprints for monitoring of working time, the EDPS highlighted that such a processing operation is not necessary. "The EDPS warns that the use of fingerprints-based systems for the monitoring of working time of staff members is **not** considered as **necessary**, and therefore, **not legitimate** pursuant to the aforesaid Article 5 (n. - of Regulation 45/2001). The requirement of the processing of personal data being necessary in relation to the purpose obliges the controller to **assess whether the purpose of the processing could be achieved with less intrusive means**. Indeed, **instead of opting** for a system using biometric data, other systems should have been considered by [the Union body] in this context, such as: signing in, using attendance sheets, or using clocking in systems via magnetic badges (emphasis added)" (Section 5).

**EXAMPLE 17:** *Article 29 Working Party Opinion 7/2010 on European Commission's Communication on the Global approach to transfers of Passenger Name Records (PNR) data to third countries, 12.11.2010*

When assessing the necessity of transfers of PNR data to third countries, the Article 29 Working Party advised the Commission to "evaluate whether the request for passenger data from third countries could be satisfied through these (n. - already existing) systems and mechanisms, before entering into new agreements". The Working Party also highlighted that "alternative options must be carefully considered before establishing such a system, in view of the intrusive character of decisions taken, at least for a large part, in an automated way on the basis of standard patterns, and in light of the difficulties for individuals to object to such decisions" (page 4).

**EXAMPLE 18:** *Article 29 Working Party Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services, WP 99, 09.11.2004*

When assessing one of the first drafts that proposed data retention measures for telecommunications traffic data, the Article 29 Working Party found that "the framework decision has not provided any persuasive arguments that retention of traffic data to such a large-scale extent **is the only feasible option** for combating crime or protecting national security. The requirement for operators to retain traffic data which they don't need for their own purposes would constitute a derogation without precedent to the finality/purpose principle" (page 4).

**EXAMPLE 19:** *S. and Marper v. UK*, (ECHR, 30562/04 and 30566/04, 4.12.2008)

When assessing whether the UK database retaining DNA data of former crime suspects that were found innocent was necessary in a democratic society, the ECtHR considered the issue "with due regard to ... the law and practice of other Contracting States" (paragraph 107). Further, ECtHR stated that it cannot "disregard the fact that, notwithstanding the advantages provided by comprehensive

extension of the DNA database, other Contracting States have chosen to set limits on the retention and use of such data with a view to achieving a proper balance with the competing interests of preserving respect for private life" (paragraph 112). Moreover, the Court looked at the practice in Scotland, which it found to be of "particular significance" because Scotland is a part of the UK, highlighting how the Scottish Parliament adopted less intrusive measures to keep DNA samples for law enforcement purposes (paragraph 109).

**EXAMPLE 20:** *EDPS Opinion 3/2016 Opinion on the exchange of information on third country nationals as regards the European Criminal Records Information System (ECRIS), 13.04.2016*

The legislative proposal under scrutiny enshrined an obligation for Member States to include biometric data (fingerprints) of all convicted third country nationals in ECRIS, arguing that this was necessary for identification purposes. The EDPS took into account the fact that there are Member States whose central authorities do not store fingerprints in their national criminal record registers and are not connected to the national automated fingerprint identification system, as well as the fact that some Member States raised constitutional concerns regarding the obligation to store fingerprints of all convicted third country nationals, irrespective of the type of offence or crime committed (paragraph 14). "*It cannot, therefore, be considered that there is no other way to ensure identification of the persons then to use fingerprints and the necessity of the compulsory use of fingerprints for TCN in ECRIS is therefore yet to be demonstrated"* (paragraph 15).

## #6: The circumstances surrounding the measure

**Guidance:**

- ✓ The measure in question must be "**based on clear and precise rules**" governing its scope and application and impose minimum safeguards for the persons to have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data[37].
- ✓ The seriousness of the interference depends on the type of information to be used, the number of the persons affected, the means used to process information (see Example 21).
- ✓ The measure must **differentiate**, **limit** and **make subject to exceptions** the persons whose information is used in the light of the objective pursued[38] (see also Example 2).
- ✓ If the measure implies access by authorities to the data, the measure must (i) lay down **objective criteria** to determine the limits of the access[39], (ii) establish **substantive and procedural conditions** relating to the access of the competent national authorities to the data and to their subsequent use[40], (iii) lay down an objective criterion by which **the number of persons authorised to access** and subsequently use the data retained **is limited** to what is strictly necessary in the light of the objective pursued[41].
- ✓ In addition, if the objective pursued is within the framework of procedures of prevention, detection or criminal prosecutions, **access** by the competent national authorities to the data retained **must be made dependent on a prior review carried out by a court or by an independent administrative body** whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities[42].

- ✓ When establishing **a retention period** for the data, the measure should make **a distinction between categories of data** based on their **possible usefulness** for the purposes pursued[43] and must use objective criteria for the determination of the length of the retention period[44].
- ✓ In the specific case of public authorities processing personal data, the strict necessity test also requires "in practice" that "there must be adequate and effective guarantees against abuse"[45].

**Ask yourself:**

**What is the proposed measure?**

- Is the proposed measure clear enough?

**What practical obligations are created and for whom?**

**Who will be affected by the measure?**

**What kind of information is going to be used and how?**

- Is the information used relevant to achieve the purpose of the measure?
- Does the information belong to a special category of data?

**Are there any differentiations or exceptions being made with regard to the individuals affected, the means used to process data and the information being used?**

**Who has access to the information?**

- Under what conditions is access granted?

**For how long is the information going to be used?**

- What is the retention period and how is it justified?

**To do:**

- ✓ If the assessment shows that **any of the specific conditions** developed by the CJEU to assess necessity of the content of a measure are not complied with, then the measure should not be proposed or should be amended in order to comply with the conditions.

**Relevant example:**

**EXAMPLE 21:** *Digital Rights Ireland* (CJEU, Joined Cases C-293/12 and C-594/12, 8.04.2014)

When the CJEU assessed whether the interference caused by the Data Retention Directive (Directive 2006/24) is limited to what is strictly necessary, it took into account that "the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives" and "the directive covers all subscribers and registered users" (paragraph 56). The CJEU concluded that it "*entails an interference with the fundamental rights of practically the entire European population*" (paragraph 56).

## ANNEX

### Relevant case-law for assessing necessity

***CJEU***

1. Joined Cases C-465/00, C-138/01 and C-139/01, Rechnungshof et al v. Österreichischer Rundfunk, 20.05.2003 (Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Protection of private life - Disclosure of data on the income of employees of bodies subject to control by the Rechnungshof).

2. Case C-524/06 Heinz Huber v. Bundesrepublik Deutschland, 16.12.2008 (Protection of personal data – European citizenship – Principle of non-discrimination on grounds of nationality – Directive 95/46/EC – Concept of necessity – General processing of personal data relating to citizens of the Union who are nationals of another Member State – Central register of foreign nationals).

3. Case C-73/07 Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy, 16.12.2008 (Directive 95/46/EC – Scope – Processing and flow of tax data of a personal nature – Protection of natural persons – Freedom of expression).

4. Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) v. Land Hessen, 9.11.2010 (Protection of natural persons with regard to the processing of personal data – Publication of information on beneficiaries of agricultural aid – Validity of the provisions of European Union law providing for that publication and laying down detailed rules for such publication – Charter of Fundamental Rights of the European Union – Articles 7 and 8 – Directive 95/46/EC – Interpretation of Articles 18 and 20).

5. Case C-291/12 Michael Schwarz v. Stadt Bochum, 17.10.2013 (Reference for a preliminary ruling – Area of freedom, security and justice – Biometric passport – Fingerprints – Regulation (EC) No 2252/2004 – Article 1(2) – Validity – Legal basis – Procedure for adopting – Articles 7 and 8 of the Charter of Fundamental Rights of the European Union – Right to respect for private life – Right to the protection of personal data – Proportionality).

6. Case C-201/14 Smaranda Bara and Others v. Preşedintele Casei Naţionale de Asigurări de Sănătate, 1.10.2015 (Reference for a preliminary ruling — Directive 95/46/EC — Processing of personal data — Articles 10 and 11 — Data subjects' information — Article 13 — Exceptions and limitations — Transfer by a public administrative body of a Member State of personal tax data for processing by another public administrative body).

7. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd (C-293/12) v. Minister for Communications, Marine and Natural Resources et al, and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others, 8.04.2014 (Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union).

8. Case C-362/14 Maximillian Schrems v. Data Protection Commissioner, 6.10.2015 (Reference for a preliminary ruling — Personal data — Protection of individuals with regard

to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities).

9. C-601/15 PPU J. N. v. Staatssecretaris voor Veiligheid en Justitie, 15.02.2016 (Reference for a preliminary ruling — Urgent preliminary ruling procedure — Standards for the reception of applicants for international protection — Directive 2008/115/EC — Lawful residence — Directive 2013/32/EU — Article 9 — Right to remain in a Member State — Directive 2013/33/EU — Point (e) of the first subparagraph of Article 8(3) — Detention — Protection of national security or public order — Validity — Charter of Fundamental Rights of the European Union — Articles 6 and 52 — Limitation — Proportionality).

***ECtHR***

1. Case of Handyside v. the United Kingdom, Application no. 5493/72, 7.12.1976.

2. Case of Klass and others v. Germany, Application no. 5029/71, 6.09.1978.

3. Case of Leander v. Sweden, Application no. 9248/81, 26.03.1987.

4. Case of Chapman v. UK, Application no. 27238/95, 18.01.2001.

5. Case of Weber and Saravia v. Germany, Application no. 54934/00, 29.06.2006.

6. Case of S. and Marper v. UK, Applications nos. 30562/04 and 30566/04, 4.12.2008.

7. Case of Cvasnica v. Slovakia, Application no. 72094/01, 9.06.2009.

8. Case of Kennedy v. UK, Application no. 26839/05, 18.05.2010.

9. Case of Soltysyak v. Russia, Application no. 4663/05, 10.02.2011.

10. Case of Roman Zacharov v. Russia, Application no. 47143/06, 4.12.2015.

11. Case of Szabó and Vissy v. Hungary, Application no. 37138/14, 12.01.2016.

## NOTES

[1] Article 2 of the Treaty on the European Union (TEU) states that "*The Union is based 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 recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg on 12 December 2007, which shall have the same legal value as the Treaties, and 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".

[2] For an overview of the relevant case law of the CJEU and ECtHR, see "Handbook on European data protection Law", published by the EU Fundamental Rights Agency in June 2014. See also "Factsheet - Personal data protection", issued in April 2016 by the ECtHR through the Press Unit, available here: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[3] See Article 7 of Directive 95/46, Article 5 of Regulation 45/2001, Article 6(1) of Regulation 2016/679 and Article 8(1) of Directive 2016/680.

[4] Focusing on the assessment of necessity of measures interfering specifically with the rights to personal data protection and respect for private life, the background paper should be read in connection with other existing guidance in the area of fundamental rights, such as the Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments (Commission Staff Working Paper, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, Brussels, 6.5.2011, SEC(2011) 567 final.) and the Better Regulation Guidelines (Commission Staff Working Document "Better Regulation Guidelines", Strasbourg, 19.05.2015, SWD(2015) 111 final). The background paper and the resulting "toolkit", once adopted, should also be seen as complementary to the Charterpedia, an online tool developed by the Fundamental Rights Agency, which provides information about the encompassing fundamental rights framework of the EU and includes the full text and legal explanations of the Charter articles, related EU and national case law, and related FRA publications, provided on an article-by-article basis.

[5] See, for instance, Directive (EU) 2016/681 of the European Parliament and of the Council of 27.04.2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *OJ L 119, 04.05.2016, p. 132–149*; Proposal for a Directive as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), COM(2016) 7 final, Strasbourg, 12.1.2016.

[6] See Communication from the Commission to the European Parliament and the Council "Stronger and Smarter Information Systems for Borders and Security", COM(2016) 205 final, Brussels, 06.04.2016.

[7] See Opinion 5/2015 of the EDPS on the EU-PNR Directive, 24.09.2015 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-24_PNR_EN.pdf; Opinion 3/2016 of the EDPS on the ECRIS Proposal for the exchange of information on third country nationals, 13.04.2016, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-04-13_ECRIS_EN.pdf; Opinion 02/2016 of the EDPS on the proposed European Border and Coast Guard Regulation, 18.03.2016, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-03-18_EBCG_EN.pdf.

[8] The recent landmark cases of the CJEU in data protection, particularly *Digital Rights Ireland* and *Schrems* illustrate this.

[9] CJEU, judgments in *Åkerberg Fransson*, C-617/10, paragraph 44, *Inuit Tapiriit Kanatami and Others* v *Commission*, C-398/13 P, paragraph 45, and, C-601/15 PPU *J.N. v Staatssecretaris van Veiligheid en Justitie*, 15.02.2016, paragraph 45.

[10] CJEU, judgments in *Otis and Others*, C-199/11, paragraph 47, and *Inuit Tapiriit Kanatami and Others* v *Commission*, C-398/13 P, paragraph 46 and *J.N. v Staatssecretaris van Veiligheid en Justitie*, paragraph 46.

[11] CJEU, *J.N. v Staatssecretaris van Veiligheid en Justitie*, paragraph 77.

[12] For a detailed analysis of the ECtHR case law on the application of the requirements in Article 8(2) of the Convention, see Opinion 01/2014 of the Article 29 Working Party on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 27.02.2014.

[13] For ECHR, see, for instance, **Article 8(2)** of the European Convention on Human Rights – "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and **is necessary in a democratic society** in the interests of national security, public safety or the economic well-

being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." For the Charter, see **Article 52(1)** – "Any 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."

[14] ECtHR, *Handyside vs UK*, paragraph 48.

[15] ECtHR, *Handyside vs UK*, paragraph 48, in particular "whilst the adjective 'necessary', within the meaning of Article 10(2), is not synonymous with 'indispensable' (cf., in Articles 2(2) and 6(1), the words 'absolutely necessary' and 'strictly necessary' and, in Article 15(1), the phrase 'to the extent strictly required by the exigencies of the situation' (...)".

[16] See Article 5(4) of the Treaty establishing the European Union.

[17] K. Lenaerts, P. Van Nuffel, *European Union Law*, Sweet and Maxwell, 3rd edition, London, 2011, p. 141. (Case C-343/09 *Afton Chemical*, paragraph 45; *Volker und Markus Schecke and Eifert*, paragraph 74; Cases C-581/10 and C-629/10 *Nelson and Others*, paragraph 71; Case C-283/11 *Sky Österreich*, paragraph 50; and Case C-101/12 *Schaible*, paragraph 29).

[18] For instance, in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, the Court first established that the interferences with the rights protected in Articles 7 and 8 were not necessary (see paragraphs **from 51 to 65**). This finding, in addition to the earlier finding in **paragraph 49** lead in the end to the finding that the interferences were not proportionate (**paragraph 69**).

[19] Case C-362/14 *Schrems*, paragraphs 92, 93 - where the CJEU analyses necessity and paragraph 98 - where the CJEU found the Safe Harbor Decision to be invalid, without making any reference to proportionality before reaching this conclusion.

[20] See Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke*, paragraph 77; Case C-473/12 *IPI*, paragraph 39; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, paragraph 52; Case C-212/13 *Rynes*, paragraph 28 and Case C-362/14 *Schrems*, paragraph 92.

[21] In addition, the following grid could be read together with the Better Regulation toolbox #24, as it complements the general assessment regarding fundamental rights with specific details concerning the limitations of the rights to respect for private life and the protection of personal data.

[22] CJEU, *Digital Rights Ireland*, paragraphs 33, 34 and 35.

[23] CJEU, Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others*, paragraph 75 and *Digital Rights Ireland*, paragraph 33.

[24] ECtHR, *Leander v. Sweden*, paragraph 48.

[25] ECtHR, *Amman v. Switzerland*, paragraphs 65, 69 and 80.

[26] As regards Article 8 of the ECtHR, see *Leander v. Sweden*, 26 March 1987, paragraph 48; *Rotaru v. Romania* [GC], no. 28341/95, paragraph 46 and *Weber and Saravia v. Germany* no. 54934/00, paragraph 79, ECtHR 2006-XI. For Article 7 of the Charter, see CJEU, *Digital Rights Ireland*, paragraph 35.

[27] CJEU, *Schrems*, paragraph 97.

[28] CJEU, *Huber*, paragraphs 75, 79, 80, 81.

[29] CJEU, *Digital Rights Ireland*, paragraph 28.

[30] CJEU, *Digital Rights Ireland*, paragraph 47.

[31] See Article 29 Working Party, Opinion WP193 on developments in biometric technologies, 27.04.2012.

[32] ECtHR, *S. and Marper v. UK*, paragraph 101. The CJEU incorporated this jurisprudence in its case-law, re-stating it in one of the first cases on the interpretation of Directive 95/46 (CJEU, *Österreichischer Rundfunk and Others*, paragraph 83).

[33] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, 27.04.2012, WP193, p. 8.

[34] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, 27.04.2012, WP193, p. 8.

[35] CJEU, *Digital Rights Ireland*, paragraph 59.

[36] Article 29 Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services, WP 99, 9.11.2004.

[37] CJEU, *Digital Rights Ireland*, paragraph 54 and the cited ECHR case-law (*Liberty and Others v. the United Kingdom*, paragraphs 62 and 63; *Rotaru v. Romania*, paragraphs 57 to 59, and *S. and Marper v. the United Kingdom*, paragraph 99).

[38] CJEU, *Digital Rights Ireland*, paragraph 57 and CJEU, *Schrems*, paragraph 93.

[39] CJEU, *Digital Rights Ireland*, paragraph 60 and CJEU, *Schrems*, paragraph 93.

[40] CJEU, *Digital Rights Ireland*, paragraph 61.

[41] CJEU, *Digital Rights Ireland*, paragraph 62.

[42] CJEU, *Digital Rights Ireland*, paragraph 62.
[43] CJEU, *Digital Rights Ireland*, paragraph 63.
[44] CJEU, *Digital Rights Ireland*, paragraph 64.
[45] ECtHR, *Kennedy v. UK*, paragraph 153.