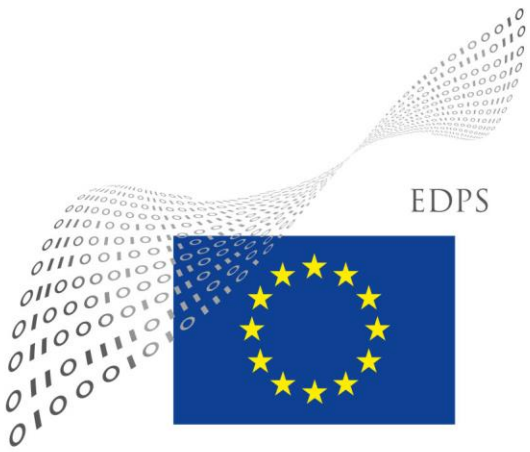
EUROPEAN DATA PROTECTION SUPERVISOR

# Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit




11 April 2017

## TABLE OF CONTENTS

**I. The purpose of this Toolkit and how to use it** ..... **2**

*Note on terminology* ..... *3*

**II. Legal analysis: the necessity test applied to the right to the protection of personal data** ..... **4**

1. THE TEST OF NECESSITY IN ASSESSING THE LEGALITY OF ANY PROPOSED MEASURE INVOLVING PROCESSING OF PERSONAL DATA ..... 4

2. THE RELATIONSHIP BETWEEN PROPORTIONALITY AND NECESSITY ..... 5

3. THE CHARTER AND THE ECHR ..... 6

4. MEASURES SHOULD BE *STRICTLY NECESSARY* ..... 7

5. LIMITATION OF A FUNDAMENTAL RIGHT ..... 7

6. CONCLUSION: NECESSITY IN DATA PROTECTION LAW - A CASE- AND FACTS-BASED CONCEPT REQUIRING ASSESSMENT BY THE EU LEGISLATOR ..... 8

**III. Checklist for assessing necessity of new legislative measures** ..... **9**

**STEP 1: FACTUAL DESCRIPTION OF THE MEASURE PROPOSED** ..... 9

*Guidance* ..... *10*
*How to proceed* ..... *10*
*Relevant examples* ..... *11*

**STEP 2: IDENTIFICATION OF FUNDAMENTAL RIGHTS AND FREEDOMS LIMITED BY THE PROCESSING OF PERSONAL DATA** ..... 11

*Guidance* ..... *11*
*How to proceed* ..... *12*
*Outcome* ..... *12*
*Relevant examples* ..... *13*

**STEP 3: DEFINE OBJECTIVES OF THE MEASURE** ..... 14

*Guidance* ..... *14*
*How to proceed* ..... *15*
*Outcome* ..... *15*
*Relevant examples* ..... *16*

**STEP 4: CHOOSE OPTION THAT IS EFFECTIVE AND LEAST INTRUSIVE** ..... 17

*Guidance on effectiveness and intrusiveness* ..... *17*
*How to proceed* ..... *19*
*Outcome* ..... *19*
*Relevant examples* ..... *20*

**Notes** ..... **24**

## I. The purpose of this Toolkit and how to use it

Fundamental rights, enshrined in the Charter of Fundamental Rights of the European Union (hereinafter, 'the Charter'), constitute the core values of the European Union[1]. These rights must be respected whenever the EU institutions and bodies design and implement new policies or adopt any new legislative measure. Other fundamental rights norms also play an important role in the EU legal order, in particular the European Convention for the Protection of Human Rights and Freedoms (ECHR).

This Toolkit responds to requests from EU institutions for guidance on the particular requirements stemming from Article 52(1) of the Charter, which states that any limitation on the exercise of the right to personal data protection (Article 8 of the Charter) must be "necessary" for an objective of general interest or to protect the rights and freedoms of others[2].

Meanwhile, the conditions for possible limitations on the exercise of fundamental rights are amongst the most important features of the Charter because they determine the extent to which the rights can effectively be enjoyed.

Necessity is an essential requirement with which any proposed measure that involves processing of personal data must comply.

This Toolkit is intended to help assessment of compliance of proposed measures with EU law on data protection. It has been developed to better equip EU policymakers and legislators responsible for preparing or scrutinising measures that involve processing of personal data and limit the right to the protection of personal data and other rights and freedoms laid down in the Charter.

The EDPS fully respects the responsibility of the legislator to assess the necessity and proportionality of a measure. This Toolkit therefore does intend to provide, nor can it provide, a definitive assessment as to whether any specific proposed measure might be deemed necessary or otherwise. Rather the Toolkit offers a practical, step-by-step checklist for assessing the necessity of new legislative measures, accompanied by a legal analysis of the notion of necessity with regard to the processing of personal data.

It complements and deepens existing guidance produced by the Commission and the Council on the limitations of fundamental rights in general concerning, for example, impact assessments and compatibility checks[3].

The Toolkit consists of this introduction, which sets out the content and purpose of the Toolkit, a practical step-by-step Checklist for assessing the necessity of new legislative measures and a legal analysis of the necessity test applied to the processing of personal data. The Checklist is the core of the toolkit and can be used autonomously.

The Toolkit is based on the case law[4] of the Court of Justice of the European Union (hereafter CJEU), the European Court of Human Rights (ECtHR), and previous Opinions of the EDPS and of the Article 29 Working Party. It follows a background paper[5] issued in 2016 for public consultation.

We are grateful to respondents for their feedback which we have used to improve the document.

*Note on terminology*

With regard to rights in the Charter of Fundamental Rights a number of similar terms, including "limitation", "restriction", "interference" and "affecting" and their respective derivations, are used seemingly interchangeably in policy discussions and even in legal texts, including CJEU case law. For the purpose of simplicity, this Toolkit will follow Article 52 of the Charter and use the term 'limitation' throughout, except in the case of citations.

## II. Legal analysis: the necessity test applied to the right to the protection of personal data

### 1. The test of necessity 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[6]. The same analysis applies to the right to respect for private life enshrined in Article 7 of the Charter.

To be lawful, any limitation on 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,
- 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 subject of this Toolkit, and
- it must be proportional.

This list of criteria sets out the required order of the assessment of lawfulness. First it must be examined whether an accessible and foreseeable law[7] provides for a limitation, and 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[8.] 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.

The next test is 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. It is therefore important to identify the objective of general interest in sufficient detail so as to allow the assessment as to whether the measure is necessary.

The next step is to assess the **necessity** of a proposed legislative measure which entails the processing of personal data.

If this test is satisified, the **proportionality** of the envisaged measure will be assessed. Should the draft measure not pass the necessity test, there is no need to examine its proportionality. A measure which is not proved to be necessary should not be proposed unless and until it has been modified to meet the requirement of necessity.

The proportionality test, to which any limitation of fundamental rights is subject, will be addressed by the EDPS in a separate document.

**A proper description of the measure in question** is important as it may affect several of the above mentioned criteria. The courts therefore may sometimes assess the criteria

in tandem. For instance, a measure that is unclearly or too broadly defined may prevent assessment of whether it is "provided by law" and "necessary"[9].

## 2. The relationship between proportionality and necessity

**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*"[10]. 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*"[11]. 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)*"[12].

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 (...*)".

Proportionality in a broad sense encompasses both the necessity and the **appropriateness** of a measure, that is, the extent to which there is a logical link between the measure and the (legitimate) objective pursued. Furthermore, for a measure to meet the principle of proportionality as 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 the fundamental rights[13]. This latter element describes proportionality in a narrow sense and consitutes the proportionality test. It should be clearly distinguished from **necessity.**

**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.

"Necessity" is also a data quality principle and a recurrent condition in almost all the requirements on the lawfulness of the processing of personal data stemming from EU data protection secondary law[14]. There is also a link between Article 8(2) of the Charter and the secondary law, as Article 8(2) refers to the legitimate basis for processing "laid down by law" and the Explanatory Note on Article 8 refers to this secondary law stating that the Directive 95/46 and the Regulation 45/2001 "contain conditions and limitations for the exercise of the right to the protection of personal data".

This Toolkit is based on the premise that only a measure proved to be *necessary* should proceed to the proportionality test. In recent cases, the CJEU did not proceed to assess proportionality after finding that the limitations to the rights in Articles 7 and 8 of the Charter were not strictly necessary[15]. For example, a law enforcement measure, if and when assessed to be necessary, should then be analysed according to whether it would be more proportionate if it were limited to only serious crimes. A proportionality test could involve assessing what rules should accompany a surveillance measure before or after it is authorised: such rules, often referred to as 'safeguards', would serve to reduce the risks to the fundamental rights posed by the envisaged measure.

In practice, a specific aspect of, or provision contained within, a draft measure can be relevant to both the necessity and proportionality assessments. For instance, the question of whether a measure should target any crime or only serious crimes may be

considered a matter of necessity; however, should such a provision be assessed to be necessary, an assesment would still be needed of its proportionality and its risk of eroding the values of a democratic society. In practice, therefore, there is some overlap between the notions of necessity and proportionality, and depending on the measure in question the two tests may be carried out concurrently or even in reverse order[16].

**As a general approach, however, it must first be ascertained whether a limitation on a fundamental right is necessary before proceeding to assess proportionality.**

## 3. The Charter and the ECHR

While the **right to the respect for private life** (also called the right to privacy) is addressed by the Charter (Article 7) and the ECHR (Article 8), the **right to personal data protection** as such is a separate fundamental right in the Charter (Article 8)[17].

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[18]. 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*"[19]. 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*"[20].

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[21]. 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 insofar 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]*" while Union law may provide more extensive protection (Article 52(3) of the Charter).

On the one hand, the right to the respect for private life in Article 7 of the Charter directly corresponds to Article 8 ECHR. On the other hand, the right to the protection of personal data is formulated in the Charter but not the ECHR and therefore is not listed amongst the rights which correspond to a right protected by the ECHR according to Article 52(3) of the Charter[22]. However, the Explanatory Note to Article 8 of the Charter states that this right has been based on, amongst others, Article 8 ECHR. Therefore the case law of the ECtHR under Article 8 ECHR is relevant, although not necessarily conclusive, when assessing whether a limitation is compliant with the Charter[23]. There is also constant dialogue between the CJEU and the ECtHR, observed in numerous references in each other's court case-law[24].

The criteria provided under Article 8(2) ECHR and Article 52(1) of the Charter for a lawful limitation on the right to the respect for private life are similar[25]. Article 8(2) ECHR states, in addition, that the limitation must be necessary "in a democratic society". Even though Article 52(1) does not use the same language, the "democratic society" element is intertwined in the EU legal order as it flows from the core values of the EU, which include the respect for democracy (Article 2 TEU).

**Therefore, the main reference when assessing the necessity of measures that limit the exercise of the rights guaranteed under Article 8 of the Charter is Article 52(1) of the Charter and the case law of the CJEU. In addition, the criteria in Article 8(2) ECHR -and specifically the condition for a limitation to be necessary in a democratic society[26], as interpreted in the case-law of the ECtHR, should also be taken into account in the analysis.**

## 4. Measures should be *strictly necessary*

The case law of the CJEU applies a *strict necessity* test for any limitations on the exercise of the rights to personal data protection and respect for private life with regard to the processing of personal data: "*derogations and limitations in relation to the protection of personal data* ***must apply only in so far as is strictly necessary***". The ECtHR applies a test of *strict necessity* depending on the context and all circumstances at hand, such as with regard to secret surveillance measures [27].

It flows from the CJEU case-law that the condition of strict necessity is a horizontal one, irrespective of the area at issue, such as the law enforcement or commercial sector[28].The requirement of "strict necessity" flows from the important role the processing of personal data entails for a series of fundamental rights, including freedom of expression. Even if specific rules are adopted in the field of law enforcement, as for instance Directive 2016/680[29], this does not justify a different assessment of necessity.

The requirement of strict necessity has as a further consequence in that the judicial review of the measure is also strict; in other words, the legislature's discretion in selecting the measure is limited. That said, the conditions for a strict judicial review of the legislator's discretion are also viewed alongside the seriousness of the interference that a particular measure may cause[30]. Similarly, the EDPS stressed in the pending case on the EU-Canada PNR Draft Agreement that because of the systematic and particularly intrusive processing of personal data the Agreement entails, the judicial review must be strict[31].

## 5. Limitation of a fundamental right

The necessity test should be performed in cases where the proposed legislative measure entails the processing of personal data.

The CJEU assesses limitations on the exercise of the rights and freedoms provided for under EU law on the basis of Article 52(1) of the Charter. The Court has stated that an act 'constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data'[32]. In principle, therefore, any data processing operation (such as collection, storage, use, disclosure of data) laid down by legislation is a limitation on the right to the protection of personal data, regardless of whether that limitation may be justified.

Furthermore, the CJEU has held in the vast majority of the cases dealing with legislative acts that a processing operation limited both the right to the protection of personal data and the right for respect of private life[33]. The Court has held also that for the establishment of a limitation "*it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way*"[34].

Regarding the right to respect for private life enshrined in Article 8 ECHR, the case law of the ECtHR indicates that the processing of personal data may limit the right depending on the context, such as the sensitive nature of the data or the way the data are used[35].

## 6. Conclusion: necessity in data protection law - a case- and facts-based concept requiring assessment by the EU legislator

A proposed measure should be supported by evidence describing the problem to be addressed by the measure, how it will be addressed by the measure, and why existing or less intrusive measures cannot sufficiently address it.

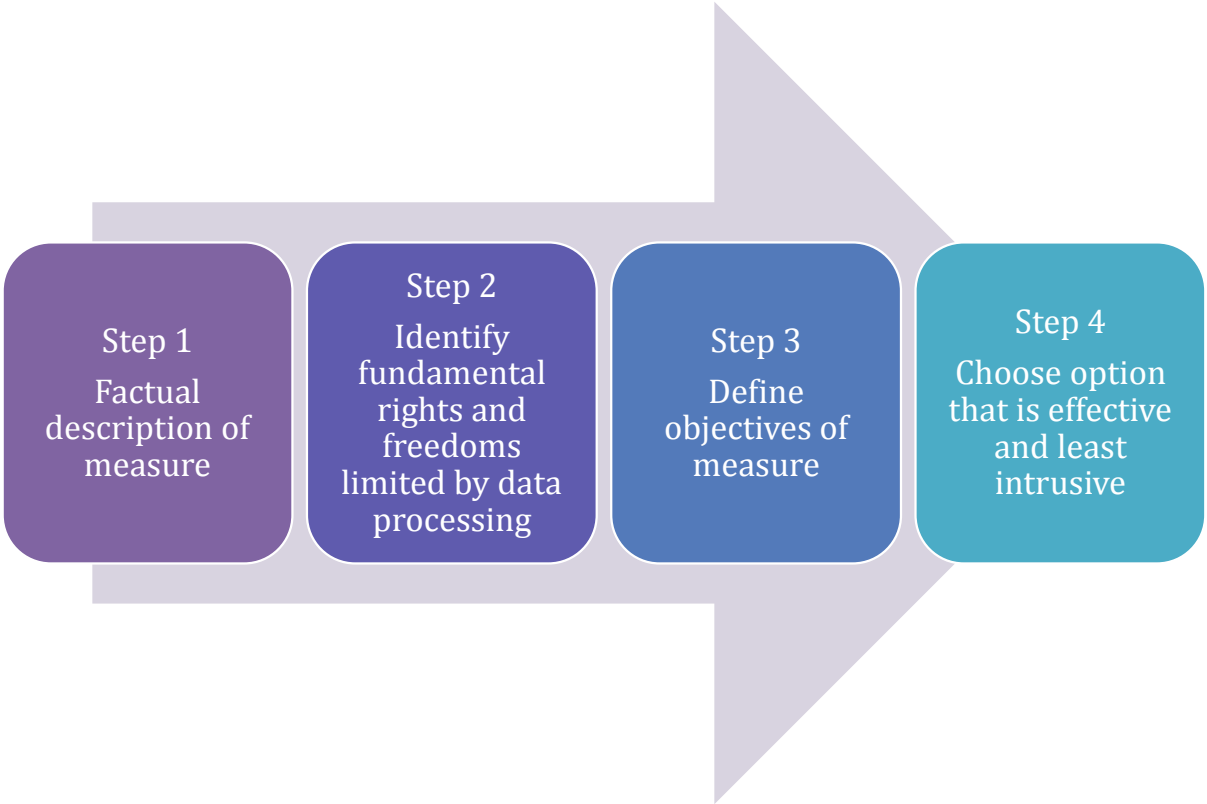
An analysis of the case law of the CJEU and ECtHR indicates that necessity in data protection law is a facts-based concept, rather than a merely abstract legal notion, and that the concept must be considered in the light of the specific circumstances surrounding the case as well as the provisions of the measure and the concrete purpose it aims to achieve[36].

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

The Checklist for assessing necessity consists of four consecutive steps. Each step corresponds to a set of questions which will facilitate the assessment of necessity.

- **Step 1** is preliminary; it requires **a detailed factual description** of the measure proposed and its purpose, prior to any 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 with 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.**

**If the assessment of any of the elements detailed in Steps #2 to #4 leads to the conclusion that a measure might not comply with the requirement of necessity, then the measure should either not be proposed, or should be reconsidered in line with the results of the analysis.**




### Step 1: Factual description of the measure proposed

A detailed description of the envisaged measure is not only a prerequisite to the necessity test, but it also helps demonstrating compliance with the first condition of Article 52(1) of the Charter, *i.e.* the quality of the law.

*Guidance*

- ✓ The measure should be sufficiently described to enable a clear understanding of what exactly is being proposed and for which purpose.
    - It is particularly important to precisely identify what the proposed measure entails in terms of personal data processing and what the objective(s) and the concrete purpose(s) of the measure is.
    - As mentioned above (Section II.1), an ill-defined measure may also affect other requirements for a lawful limitation of fundamental rights and would impede the identification of the rights which may be affected.

*How to proceed*

- ✓ **Describe the measure**
    - Determine whether the measure implies the use of personal data.
        - The **notion of personal** data is very broad since it means *"any information relating to an identified or identifiable natural person" ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification* number or to one or more factors specific to his physical, *physiological, mental, economic, cultural or social identity"*[37]. Therefore, a name, surname, vehicle registration plate number, telephone, passport number, IP address, or any other unique identifier is considered as a personal data[38].
    - If personal data are processed, describe:
        - the objective of general interest pursued by the measure;
        - the exact purpose of the processing of personal data, explained in more detail than the objective;
        - the categories of data;
        - the persons whose data are processed (*e.g.* passengers, workers, migrants);
        - who is processing and accessing the data (*e.g.* a private company, a public organisation);
        - which processing operations are envisaged (*e.g.* collection, storage, access, transfer);
        - any other relevant provisions, such as the duration of processing.

*Relevant examples*

**EXAMPLE 1: EDPS advice *during the public consultation organised by the Commission in 2011 (see Council of the European Union, Doc 6370/13) on the Amendment to the Commission proposal COM (2011) 628 final/2 for a Regulation of the European Parliament and of the Council on the financing, management and monitoring of the common agricultural policy* (rules adopted to comply with the *Schecke* judgment on the publication of personal data of beneficiaries in the context of the common agriculture policy - now Regulation 1306/2013, in particular Articles 111 - 113 and Recitals 73 - 87)**

"*The EDPS points out that for assessing the compliance with privacy and data protection requirements, it is of crucial importance to have a clear and well-defined purpose which the envisaged measure intends to serve. .. Commenting on the control objective, the representative of the EDPS said that the Commission should thereby be clear on whether the aim of the measure also includes to allow a certain form of public control over the spending of EU money by the recipients as such for which the disclosure of the identity of the recipients would be indispensible. However, if the aim only concerns public control over the EU institutions and over how the EU budget is spent, it is less obvious that the identity of the recipients should be provided to the public...*".

## Step 2: Identification of fundamental rights and freedoms limited by the processing of personal data

*Guidance*

- ✓ If the proposed measure involves the processing of personal data, the measure is a limitation on the right to personal data protection under Article 52(1) of the Charter.
- ✓ Depending on the nature of the data and how it is used, the proposed measure may also limit the right to respect for private life (also called right to privacy) (see Section II.5).
- ✓ 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**"[39].
- ✓ Furthermore, the ECtHR has repeatedly held that the **storing by a public authority of data** relating to the private life of an individual amounts to a limitation on the right to respect for his private life[40] irrespective of the use made of the data[41].
- ✓ Distinct processing operations or set of operations (i.e. collection and another operation, such as retention or transfer or access to data) may constitute separate limitations on the right to the protection of personal data and, where applicable, with the right to respect for private life. For instance, the CJEU held that 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[42].

- ✓ The refusal to allow the individual an opportunity to refute the data stored and accessed (*i.e.,* the right to access and rectify the data) also amounts to a limitation on his right to respect for private life[43].

**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[44], the right to non-discrimination[45], or the right to freedom of expression[46].

- ✓ According to Article 52 (1) of the Charter, the '**essence'** or basic content **of the right should be respected** (see Section II.1). This means that the limitation may not go so far as to empty the right of its core elements and thus prevent the exercise of the right.

*How to proceed*

- ✓ **Determine whether the measure proposed involves in any way the use of personal data. If that is the case, describe:**
  - What sort of processing operations are envisaged (*e.g.*: collection, storage, disclosure, transfer etc.);
  - Who is processing the data (*e.g.*: private entities, public entities, organisations, competent authorities, certain individuals, etc.);
  - Who has access to it;
  - For how long the data is retained[47];
  - The circumstances in which the personal information is used (*e.g.*: on a systematic basis, only in certain cases, during a limited period of time, etc.);
  - To whom the data is related (*e.g.*: certain categories of persons, users of a service, suspects of a crime, foreigners, nationals, etc.).
- ✓ **Identify which fundamental rights and freedoms are limited**
  - Consider the extent to which the data processing limits the right to respect for private life;
  - Identify a potential "difference of treatment" created between individuals which could lead to discrimination;
  - Assess the consequences on the possibility of individuals to seek effective, judicial remedies;
  - Assess the extent to which freedom of speech, freedom of thought, freedom to receive information; are limited
  - Assess whether the essence or basic content of the rights is limited.

*Outcome*

- ✓ **Where a right is affected**, the mere fact that a measure limits the exercise of these rights does not mean as such that the measure should not be proposed. However,

the measure should comply with the conditions laid down in Article 52(1) of the Charter, including necessity.

- ✓ If the **essence of the right** is adversely affected by the measure, then the limitation is not lawful and the measure should be withdrawn or modified before proceeding to the next steps (see Section I.1).

*Relevant examples*

**EXAMPLE 2: *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 3: 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 aims 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 "*the 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).

**EXAMPLE 4: *Rechnungshof* (CJEU, Case C-465/00)**

The Court found that "*the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life*". However, the Court found that the "*communication of that data to third parties, in the present case a public authority, infringes the right of the persons concerned to respect for private life*" (paragraph 74).

**EXAMPLE 5: *Schecke* (CJEU, Case C-92/09)**

The publication on the internet of the names and the amounts received by beneficiaries of public funds constitutes a limitation on their private life within the meaning of Article 7 of the Charter (paragraph 58).

**EXAMPLE 6: *Digital Rights Ireland* (CJEU, Case C-293/12)**

In the case of the Data Retention Directive, the Court found that the obligation imposed on providers of publicly available electronic communications services or of public communications networks to retain, for 6 months to two years, communications data, such as the calling and called telephone line, the email addresses, the IP addresses used for accessing the Internet, "*constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter*" (paragraph 34). "*The access of the competent national authorities to the data constitutes a further interference with that fundamental right*" (paragraph 35). The Court also found also that "Directive 2006/24 constitutes a limitation on the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data" (paragraph 36).

## Step 3: Define objectives of the measure

*Guidance*

- ✓ Pursuant to Article 52(1) of the Charter, the measure **must genuinely meet:**
  - **an objective of general interest recognised by the Union or**
  - **the need to protect the rights and freedoms of others.**
- ✓ The **Union's objectives of general interest** include for instance the general objectives mentioned in Articles 3 or 4 (2) TEU and other interests protected by specific provisions of the treaties[48], as well as interpreted in the case law of the Court of Justice.
  - Article 23 of the General Data Protection Regulation 2016/679 includes a list of aims considered legitimate for limiting the rights of the individual, such as the right to access an individual's personal data, and the obligations of the controller.
  - Transparency and public control are also legitimate aims (Articles 1 and 15(1) TEU) enabling the citizen to participate more closely in the decision-making process[49].
- ✓ The **rights of others** are in the first place those enshrined in the Charter. The right to the protection of personal data may need to be balanced with other rights, such as the protection of intellectual property rights and the rights to an effective remedy, to freedom of expression and to carry out a business[50].
- ✓ While the description of the measure is separate from the necessity test, it is prerequisite for the assessment of necessity since necessity must be assessed against the objective(s) pursued.
  - the **problem to be addressed by the measure**, *i.e.* the purpose of the processing of personal data must be specified. This is all the more important when an objective of general interest might encompass various aspects or a measure should address various objectives of general interest. For instance, the objective of safeguarding public security may be considered to encompass both internal and external security[51], therefore a given measure should clearly

state whether it seeks to address either one of these notions of security or each of them.

- ✓ The problem to be addressed should be concrete and not merely hypothetical. To this end, **objective evidence of the problem** should be provided. The evidence can consist of facts or statistical data, and should allow scientific verification and convincingly support the existence of the problem.
- ✓ For the ECtHR, a **limitation will be considered "necessary in a democratic society**" for a legitimate aim "if it answers a **pressing social need".** The problem to be addressed must not only be real, present or imminent, but critical for the functioning of the society.
- ✓ If a measure pursues more than one objective, justification is necessary for each of them[52].

*How to proceed*

- ✓ **Identify and assess the legitimacy of the aim pursued by the measure:**
  - Make sure that the problem is suffiently and clearly described in the measure;
  - Integrate sufficient and scientifically verifiable evidence supporting the existence of the problem;
  - Define precisely the objective of general interest or the right of others which the measure seeks to address;
  - Make sure that the purpose of the processing of personal data genuinely aims to achieve an objective of general interest recognised by the Union or the need to protect the rights and freedoms of others;
  - Explain the importance of the objective to be achieved and how it is critical for the functioning of society.

*Outcome*

- ✓ **If the problem to be addressed is not sufficiently described**, it should be better explained and developed. Otherwise, the assessment of the necessity of the measure will not be possible.
- ✓ **If the problem is not supported by sufficient evidence**, further evidence should be sought.
- ✓ **If the measure does not genuinely meet an objective of general interest recognised by the Union or the need to protect the rights and freedoms of others**, then the measure should not be proposed.
- ✓ **If the measure does meet such an objective** sufficiently supported by relevant evidence, then the analysis may proceed to assessing the necessity of the measure according to Step 4.

*Relevant examples*

**EXAMPLE 7: *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 8: *Promusicae* (CJEU, Case C-275/06)**

The CJEU held that the protection of the right to intellectual property is a legitimate aim for the processing of communications data (IP addresses) by reference to Article 13 of Directive 95/46/EC which sets out the legitimate aims for limitations to the right to respect for private life with regard to the processing of personal data (paragraphs 26).

**EXAMPLE 9: EDPS Opinion of 9 October 2012 *on the Amendment to the Commission proposal COM (2011) 628 final/2 for a Regulation of the European Parliament and of the Council on the financing, management and monitoring of the common agricultural policy* (rules adopted to comply with the Schecke judgment on the publication of personal data of beneficiaries in the context of the common agriculture policy - now Regulation 1306/2013, in particular Articles 111 - 113 and Recitals 73 - 87)**

While the EDPS recognised that transparency and public control are objectives of general interest as put in the *Schecke* ruling (paragraphs 65, 68, 69, 75), the problem of reduced controls and on-the-spot-checks by the authorities as a result of economic constraints cannot fall within aforementioned objective"*...Transparency and public control are legitimate aims by themselves...and cannot be presented as a replacement for specific controls and on-the-spot-checks by competent authorities. ...*" (paragraph 17).

**EXAMPLE 10: EDPS Opinion 3/2016 *on the exchange of information on third country nationals as regards the European Criminal Records Information System (ECRIS)***

The EDPS found that the ECRIS Proposal of the Commission to facilitate access to convictions of third country nationals fall within the scope of the fight against terrorism and fight against serious crime in order to ensure public security which are recognized as objectives of general interest in EU law. "*The proposed measures, therefore, meet an objective of general interest and can be justified, subject to the principle of proportionality*" (paragraph 9).

## Step 4: Choose option that is effective and least intrusive

In Section II.2 we noted that the *appropriateness* of a measure is not the same as its *effectiveness*. Even if it is appropriate, the chosen measure should also be effective and less intrusive than other options for achieving the same goal.

An appropriate measure is one capable of attaining the aim pursued:

- There must be **a logical link between the limitation and** the legitimate aims identified;
- The objective pursued must be achieved as a direct consequence of the measure;
- An appropriate measure does not, however, have to address all particular aspects of the problem[53].

*Guidance on effectiveness and intrusiveness*

✓ **The measure should be genuinely effective**, *i.e.* essential to achieve the objective of general interest pursued.

- 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"[54]. Mere convenience or cost effectiveness[55] is not sufficient.
- The selected categories of persons affected, the categories of personal data collected and processed, the storage period of the data, etc., should effectively contribute to achieve the aim pursued.
- If the proposed measure includes the processing of **sensitive data**, a higher threshold should be applied in the assessment of effectiveness.
  - Sensitive data encompass amongst others data revealing: ethnic or racial origin, political opinions, religious or similar beliefs, health status. Data relating to criminal convictions and offences have a similar status[56]. Genetic and biometric data are recognised as sensitive data by the new legal instruments on the protection of personal data[57]. The "sensitivity" of such data, however, was already highlighted by the Working Party of Article 29 on several occasions[58].
  - Other categories of data, although not strictly categorised as sensitive, in certain contexts may present a higher risk for the individual and trigger the application of a higher threshold of what is strictly necessary. This is the case, for instance, of unique identifiers, such as national identification numbers or financial data.

✓ The measure envisaged should be **the least intrusive for the rights at stake.**

- Alternative measures which are less of a threat to the right of personal data protection and the right for respect of private life should be identified.

- An alternative measure can consist of a combination of measures.
- Alternatives should be real, sufficiently and comparably effective in terms of the problem to be addressed[59].
- Imposing a limitation to only part of the population/geographical area is less intrusive than an imposition on the entire population/geographical area; a short-term limitation is less intrusive than a long-term; the processing of one category of data is in general less intrusive than the processing of more categories of data[60].
- Savings in resources should not impact on the alternative measures – this aspect should be assessed within the proportionality analysis, as it requires the balancing with other competing objectives of public interest (see Section II.2).

✓ **Each particular aspect** of the measure is subject to the strict necessity test.

- Some specific provisions, like processing of a category of personal data, the categories of persons affected, the duration of the retention of the data, may be proven necessary, but others not. The assessment depends "clear and precise rules governing its scope and application"[61]. As mentioned in Section II.1, clear and precise rules are important also in order to comply with most of the other criteria of Article 52(1) of the Charter.
- If the measure implies access by authorities to the data, the measure must lay down **objective criteria** in particular restricting the number of persons authorised to access and use the data to what is strictly necessary[62].
- The measure should **differentiate**, **limit** and **make subject to exceptions** the persons whose information is used in the light of the objective pursued[63].
- When establishing **a retention period** for the data, the measure should make **a distinction between categories of data** based on their **effective contribution** for the purposes pursued and must use objective criteria for the determination of the length of the retention period[64].
- The limitation of **the right to information** about the processing of personal data should also be necessary for the purpose pursued by the proposed measure. For example, the purpose of secret surveillance measures may justify the restriction of notification of the persons concerned. "*As soon as information can be given without jeopardising the purpose of the measure after termination of the surveillance measure, information should, however, be provided to the persons concerned*"[65].

✓ **The reasons why action is needed** should be detailed in the measure, explaining:

- why existing measures are insufficient to address the problem;
- why alternative, less intrusive measures, are insufficient to address the problem;

- why the proposed measure can address the problem **more effectively than other measures**;
- Objective evidence of all the above should be provided, including facts or statistical data, capable of scientific verification, convincingly supporting the proposed measure;
- The necessity test does not need to be applied to each Member State individually, though it is relevant for the impact assessment which considers the added value of EU intervention[66].

*How to proceed*

- ✓ **Describe how and why the measure is essential for satisfying the need to be addressed:**
  - Why existing measures are insufficient to address the problem;
  - Why and how the measure can achieve the objective.
- ✓ **Consider whether alternative, less intrusive measures could be comparably effective at meeting the objective pursued.**
- ✓ Provide scientifically verifiable evidence that can genuinely support the claim that existing measures and less intrusive alternative measures cannot effectively address the problem.

*Outcome*

- ✓ **Consider proper implementation of existing measures instead of new intrusive measures.**
- ✓ **Consider an alternative measure which is comparably effective but with less impact on the protection of personal data or the right to respect of private life.** Aspects of higher costs can be assessed within the proportionality test.
- ✓ **Only if existing or less intrusive measures are not available according to** an evidence-based analysis, and only if such analysis shows that the envisaged measure is **essential and limited to what is absolutely necessary** to achieve the objective of general interest, this measure should proceed on to the proportionality test (See Section II.2).

*Relevant examples*

**EXAMPLE 11: *Österreichischer Rundfunk and Others* (CJEU, Joined Cases C-465/00, C-138/01 and C-139/01, 20.05.2003)**

When assessing whether a wide 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 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 12: *Schecke* (CJEU, Joined Cases C-92/09 and C-93/09, 9.11.2010)**

When examining the necessity of the publication of the personal data of all beneficiaries received public funds, the Court highlighted that the legislature did not take into account alternative, less intrusive measures, such as limiting publication to those beneficiaries according to the periods for which they received aid, or the frequency or nature and amount of aid received. The Court also stressed that a less intrusive approach might be achieved by a combination of those measures: "*Such limited publication by name might be accompanied, if appropriate, by relevant information about other natural persons benefiting from aid under the EAGF and the EAFRD and the amounts received by them*". The Court concluded that "*Regard being had to the fact that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Satakunnan Markkinapörssi and Satamedia, paragraph 56) and that it is possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives of the European Union rules in question...*". (paragraphs, 81, 82, 83, 86).

**EXAMPLE 13: Tele2 Sverige AB(CJEU, Joined cases C-203/15 and C-698/15)**

In his Opinion the Advocate General re-stated that "*Given the requirement of strict necessity, it is imperative that national courts do not simply verify the mere utility of general data retention obligations, but rigorously verify that no other measure or combination of measures, such as a targeted data retention obligation accompanied by other investigatory tools, can be as effective in the fight against serious crime. I would emphasise in this connection that several studies that have been brought to the Court's attention call into question the necessity of this type of obligation in the fight against serious crime.*" Such other measures should be effective to the aim pursued. "*Retention obligations may indeed have a greater or lesser substantive scope, depending on the users, geographic area and means of communication covered.*" (paragraphs 209, 211).

The CJEU held that a targeted retention could be justified provided that the retention is limited to what is strictly necessary for the objective of the fight against serious crime: "*...the targeted retention of traffic and location data, for the purpose of fighting serious crime, [should be] limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary."* Moreover, *"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."* The Court also held that access to that data by competent authorities must be based on objective criteria, as a general rule only to data of suspects. As an exception, *"... where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities*." (paragraphs 102, 103, 108, 111, 115, 119).

**EXAMPLE 14: AG Opinion 1/15 (Request for an opinion submitted by the European Parliament) *on the Draft Agreement between Canada and the EU on the transfer and processing of PNR***

With regard to the strict necessity of the measure, the Advocate General emphasised that the terms of the PNR Draft Agreement "*must consist of the least harmful measures to the rights recognised by Articles 7 and 8 of the Charter, while making an effective contribution to the public security objective pursued by the agreement envisaged.... Those alternative measures must also be sufficiently effective, that is to say, their effectiveness must ... be comparable with those provided for in the agreement envisaged, in order to attain the public security objective pursued by that agreement.*" Towards this necessity test the Advocate General tackles various aspects of the measure, such as: "*...the categories of data in the annex to the agreement envisaged should be drafted in a more concise and more precise manner, without any discretion being left to either the air carriers or the Canadian competent authorities as regards the actual scope of those categories." "That suggests in the absence of a fuller explanation in the agreement envisaged of why the processing of sensitive data is strictly necessary, that the objective of combating terrorism and serious international crime could be attained just as effectively without such data even being transferred to Canada. "... in order to limit to what is strictly necessary the offences that may entitle the relevant authorities to process PNR data and ensure the legal security of passengers whose data is transferred to the Canadian authorities, ... should be listed exhaustively...*". As to the duration of storage the Advocate General stated that "*the agreement envisaged does not indicate the objective reasons that led the contracting parties to increase the PNR data retention period to a maximum of five years.*" (paragraphs 205, 220, 222, 235, 261, 267).

**EXAMPLE 15: 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*, 25.03.2011.**

The EDPS noted that the Impact Assessment of the proposed directive included extensive explanations and statistics to justify the measure, 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 measure aiming at 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 proposed directive 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).

**EXAMPLE 16: 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 17: 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 enshrines 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 asked for more evidence demonstrating the necessity of storing fingerprints "*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).

**EXAMPLE 18: EDPS Opinion 5/2015 Second Opinion *on the Proposal for a Directive on the use of PNR***

The EDPS stressed that "*According to the available elements, the latest versions of the Proposal fail to show that a proper assessment has been done in conformity with the ECJ judgments, on the remaining gaps in the fight against terrorism and the possible ways to address them with the existing instruments at disposal of the Member States. While this assessment should also refer to new investigative approaches to more effectively monitor well known suspects by police and judicial authorities, various recent events in the EU demonstrate intelligence gaps unrelated to air travellers and that by targeting resources and intensifying efforts on known suspects would in some cases be more effective than profiling by default millions of travellers."* (paragraph 14).

**EXAMPLE 19: Article 29 Working Party Letter to LIBE Committee *on EU PNR*, 19.3.2015**

Article 29 emphasised that the necessity of the EU PNR should be justified, i.e. why the existing instruments (SIS, API) are not sufficient, why less intrusive alternatives would not achieve the purpose, how is EU PNR the solution to achieve the purpose as opposed to less intrusive measures. The explanations should be supported by evidence, possibly statistics, by EU or Member States' studies.

**EXAMPLE 20: EDPS Opinion 07/2016** ***on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)***

The EDPS emphasised that the necessity to add a second category of biometric data, i.e. facial images, in a large scale data base should be based on "*...an assessment ....relying on a consistent study or evidence-based approach*".
With regard to the retention period, the EDPS stressed that increasing the retention period to five years in order to align it with what other instruments provide for "*is not relevant as such as these instruments may have other purposes and their retention period might be justified by other elements*". In his Opinion, the EDPS considered that the retention period of five years is not sufficiently justified, and recommended further supporting evidence (paragraphs, 22, 30 - 31).

## 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 recognises 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 has 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] Intention of the EDPS to publish this toolkit was announced to Civil Liberties Committee of the European Parliament on 24 May 2016.

[3] See 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. 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. These documents are more general, although several case-law examples in these guidelines relate to the rights enshrined in Articles 7 and 8 of the Charter, as the CJEU pronounced important judgments on the limitation of these rights.

[4] 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 November 2016 by the ECtHR through the Press Unit, available at: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[5] See "Developing a "toolkit" for assessing the necessity of measures that interfere with fundamental rights", available at:https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Papers/16-06-16_Necessity_paper_for_consultation_EN.pdf.

[6] In *Schecke*, the AG Opinion stated that "Like 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", paragraph 73. The approach is then followed by the judgement of the CJEU, paragraphs 48 - 50.

[7] On the notion of 'provided for by law', the criteria developed by the European Court of Human Rights should be used as suggested in several CJEU Advocates General opinions, see for example Advocate General opinions in *Tele2 Sverige AB* paragraphs 137-154, C-70/10 *Scarlet Extended* paragraphs and C-291/12 paragraphs 88-114. This approach is followed in the General Data Protection Regulation 2016/679 recital (41).

[8] While the case-law is not abundant regarding the conditions under which the essence of a right is affected, one can state 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 *Schrems*, the CJEU found that the essence of the right to an effective remedy was affected. "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). It then did not go on with the examination whether such a limitation was necessary but invalidated -also on other grounds- the Commission's Decision on the adequacy of the Safe Harbour Principles. In *Digital Rights Ireland*, 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. The CJEU similarly found that the essence of the right to the protection of personal data is 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 (paragraphs 39, 40). Only then did the Court proceed to examine the necessity of the measure. The

deprivation of review, by an independent authority, of compliance with the level of protection guarnteed 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 "*If that were not so, persons whose personal data was retained would be deprived of the right, guararnteed 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 *Tele2 Sverige AB*, paragraph 123.

[9] In *Szabo and Vissy v. Hungary*, the ECtHR found that the notion of "*persons concerned identified …as a range of persons*" might include any person without a requirement for the authorities to demonstrate the relation of the persons concerned and the prevention of a terrorist attack. Such a measure does not satisfy the requirement of foreseeability and the necessity (paragraphs, 58 62, 66, 67).

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

[11] Case C-62/14 Gauweiler (OMT), paragraph 67.

[12] 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).

[13] See for instance the case C-83/14 *Razpredelenie Bulgaria Ad,* para. 123. The Court states that *"…assuming that no other measure as effective as the practice at issue can be identified, the referring court will also have to determine whether the disadvantages caused by the practice at issue are disproportionate to the aims pursued and whether that practice unduly prejudices the legitimate interest of the persons inhabiting the district concerned*". See also the AG Opinion in the joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, paragraphs 132,172, 247, 248 stating that the CJEU in the Digital Rights Ireland did not examine the proportionality "*since the regime established by Directive 2006/24 went beyond the bounds of what was strictly necessary for the purposes of fighting serious crime*".." He then stated that the "*requirement of proportionality in a narrow sense (stricto sensu) within a democratic society 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*".He also pointed to that the requirement of proportionality in the particular case of data retention of such large amount of data "*opens a debate about the values that must prevail in a democratic society and, ultimately, about what kind of society we wish to live in*". The ruling of the Court, in paragraphs 102-103, sets out its analysis with considerations relating rather to the proportionality when it analyses whether the fight against crime, even serious crime, justifies a general and indiscriminate retention of electronic communications data. The Court states that *"...while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, 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*". It also states that only the fight against serious crime could justify a targeted retention and access to electronic communications data. "*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". "Further, since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data*".

[14] See Article 6 (1.c) and 7 of Directive 95/46, Article 4 (1.c) and 5 of Regulation 45/2001, Article 5(1.c) and 6(1) of Regulation 2016/679 as well as recital (49), which empasises the strict necessity test regarding the processing of personal data for the purpose of ensuring network and information security of the systems of the controller, and Article 8(1) of Directive 2016/680.

In the guidance issued to the EU institutions to assess whether video-surveillance measures are necessary in accordance with Regulation 45/2001, 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" (section 5.4) and if "adequate alternatives are available. An alternative can be considered adequate unless it is not feasible or significantly less effective than video-surveillance... Mere availability of the technology at a relatively low cost is not sufficient to justify the use of video-technology.*" (section 5.5). Only then he examined whether the measure is proportional "*Finally, even if an Institution concludes that there is a clear need to use video-surveillance and there are no other less intrusive methods available, it should*

*only use this technology if the detrimental effects of video-surveillance are outweighed by the benefits of the video-surveillance*." (section 5.6). See EDPS Video-surveillance guidelines, Brussels, 17.03.2010, available at:https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf . 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*" (Section 3), see EDPS letter on "Prior checking notification concerning "Processing of leave and flexitime", 13.10.2014, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Letters/2014/14-10-13_Letter_Mr_Mifsud_EBA_EN.pdf.

[15] In Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, the Court first stated that proportionality consists of the steps of appropriateness and necessity (paragraph 46), It then established that the limitation with the rights protected in Articles 7 and 8 were not necessary (see paragraph 65) and therefore concluded, that the limitations were not proportionate (paragraph 69). Similarly, in case C-362/14 *Schrems*, paragraphs 92, 93, where the CJEU analysed necessity and found the Safe Harbour Decision to be invalid, without making any reference to proportionality before reaching this conclusion (paragraph 98).

[16] For instance, in joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, the CJEU in paragraphs 102-103 sets out its analysis with considerations relating to the proportionality in that narrow sense when it assesses whether the fight against crime, even serious crime, justifies a general and indiscriminate retention of electronic communications data. The Court states that *"...while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, 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*". It also states that only the fight against serious crime could justify a targeted retention and access to electronic communications data. "*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*". "*Further, since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data*". It only then proceeds with the analysis of the necessity requirements for a targeted retention of communications data (paragraph 108).

[17] See also Opinion of the Article 29 Working Party 4/2007 on the concept of personal data, page 7.

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

[19]See CJEU cases C-617/10, *Åkerberg Fransson*, paragraph 44, C-398/13 P, *Inuit Tapiriit Kanatami and Others* v *Commission*, paragraph 45, C-601/15 PPU *J.N. v Staatssecretaris van Veiligheid en Justitie*, , paragraph 45 and joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, paragraph 127-129.

[20] See CJEUcase C-199/11, *Otis and Others*, paragraph 47, case C-398/13 P, *Inuit Tapiriit Kanatami and Others* v *Commission*, paragraph 46 and case C-601/15 PPU, *J.N. v Staatssecretaris van Veiligheid en Justitie*, paragraph 46.

[21] See case C-601/15 PPU,*J.N. v Staatssecretaris van Veiligheid en Justitie*, paragraph 77.

[22] See Explanatory Note on Article 52 of the Charter.

[23] See H. Kranenborg, Article 8, pg. 235, in S. Peers and J. Kenner, EU Charter of Fundamental Rights, 2014 and S. Peers, Article 52, pg. 1515 et. seq., ibid.

[24] See for instance CJEU joined cases C-92/09 and C-93/09, *Volker und Markus Schecke*, , paragraph 59, joined cases C-293/12 and C-594/12,*Digital Rights Ireland*, paragraph 35 ,joined cases C-203/15 and C-

698/15, *Tele2 Sverige AB* paragraphs 119, 120 and ECtHR *Zakharov v. Russia* and *Szabo and Vissy v. Hungary*, paragraph 23.

[25] Article 8(2) ECHR: "*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*".

[26] 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.

[27] ECtHR, *Szabo and Vissy v. Hungary*, paragraph 73.

[28] See CJEU case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy*, paragraph 56; 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, C-698/15, *Tele2 Sverige AB*, paragraph 96 and the AG Opinion 1/15 (Request for an opinion submitted by the European Parliament) on the Draft Agreement between Canada and the EU on the transfer and processing of PNR, paragraph 226.

[29] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard ot the processing of personal data by competent authorities for the purposes of teh prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L119, 4.5.2016.

[30] CJEU joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paragraphs 47-48.

[31] EDPS, pleading at the oral hearing in the case of the EU-Canada PNR Draft Agreement, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2016/16-04-05_Pleading_Canada_PNR2_EN.pdf.; The AG Opinion 1/15 (Request for an opinion submitted by the European Parliament) on the Draft Agreement between Canada and the EU on the transfer and processing of PNR, states that the strict review of the legislature's discretion is based on the important role the processing of personal data has in society and the seriousness of the limitation that the measure at hand may cause (paragraph 201). See also CJEU, joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paragraph 47.

[32] CJEU, joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paragraphs 34 - 36; see also joined cases C-92/09 and C-93/09 *Volker und Markus Schecke*, paragraph 58.

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

[34] CJEU, Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof et al v. Österreichischer Rundfunk*, paragraph 75and joined cases C-293/12 and C-594/12 *Digital Rights Ireland*, paragraph 33.

[35] CJEU, Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof et al v. Österreichischer Rundfunk*, paragraph 75, Joined casesC-293/12 and C-594/12 *Digital Rights Ireland*, paragraph 33. ECtHR, *S. and Marper v . UK*, paragraph 67. The Court stated that "*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 (see, mutatis mutandis, Friedl, cited above, §§ 49-51, and Peck, cited above, § 59)*".

[36] In addition, as the CJEU stated, necessity has its own independent meaning in EU secondary law. On the independent meaning of the necessity concept within Article 7 (e) of Directive 95/46/EC, see CJEU, C-524/06, *Huber v. Bundesrepublik Deutschland*, paragraph 52.

[37] See Directive 95/45, article 1 (a).

[38] See Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, available on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

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

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

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

[42] 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.

[43] ECtHR, *Leander v. Sweden*, 26 March 1987, paragraph 48; *Rotaru v. Romania* [GC], no. 28341/95, paragraph 46.

[44] CJEU, C-362/14, *Schrems*, paragraph 97.

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

[46] CJEU, joined cases C-293/12 and C-594/12 *Digital Rights Ireland*, paragraph 28, *Tele2 Sverige AB,* paragraph 92.See also C. Docksey, Four Fundamental rights: finding the balance, (2016) 6 International Data Privacy Law, pp. 2.

[47] AG Opinion 1/15 (Request for an opinion submitted by the European Parliament) on the Draft Agreement between Canada and the EU on the transfer and processing of PNR, paragraphs 274-281.

[48] As for instance Articles 36 and 346 TFEU. See on the objectives of general interest also the Explanatory Note on Article 52 of the Charter.

[49] CJEU, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke*, paragraphs 65, 68, 69, 75.

[50] CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, paragraph 65; C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, paragraphs 46, 49, 53.

[51] CJEU, C-145/09, *Tsakouridis*, on the notion of public security, paragraphs 43 and 44; C-601/15 PPU *J. N. v. Staatssecretaris voor Veiligheid en Justitie*, paragraph 66.

[52] EDPS, Opinion on the proposed European Border and Coast Guard Regulation, 02/2016, paragraph 8.

[53] CJEU, *Digital Rights Ireland,* paragraphs 49-50.

[54] 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.

[55] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP 193, 27.04.2012, p. 8.

[56] See Article 8 of Directive 95/46, Article 9 and 10 of the General Data Protection Regulation 2016/679, and Directive 2016/680.

[57] Article 9 of Regulation 2016/679, Article 10 of Directive 2016/680.

[58] See for instance, Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, p. 4.

[59] CJEU, C-291/12, *Schwarz*, The Court held that "*In those circumstances, the Court has not been made aware of any measures which would be both sufficiently effective in helping to achieve the aim of protecting against the fraudulent use of passports and less of a threat to the rights recognised by Articles 7 and 8 of the Charter than the measures deriving from the method based on the use of fingerprints*."..." paragraph 53; See also AG Opinion 1/15 (Request for an opinion submitted by the European Parliament) on the Draft Agreement between Canada and the EU on the transfer and processing of PNR, according to which the PNR Agreement

must consist of measures least harmful to the rights recognised by Articles 7 and 8 of the Charter, while making an effective contribution to the public security objective, paragraphs 208, 244.

[60] This, however, does not apply to identifiers of general application. See Article 87 of Regulation 2016/679.

[61] CJEU, *Digital Rights Ireland*, paragraph 54 and the cited ECtHR 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).

[62] CJEU, joined cases C-293/12 and C-594/12, *Digital Rights Ireland,* paragraph 60; C-362/14, *Schrems*, paragraph 93.

[63] CJEU, joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paragraph 57; C-362/14*Schrems*, paragraph 93.

[64] CJEU, joined cases C-293/12 and C-594/12 , *Digital Rights Ireland,* paragraph 63-64.

[65] ECtHR, *R. Zakharov v. Russia*, paragraph 287. See also ECtHR, *Szabo and Vissy v. Hungary*, paragraph 86.

[66] See with regard to the subsidiarity principle Tool#3 on Legal Basis, Subsidiarity and Proportionality as part of the Better Regulation Toolbox, available at: http://ec.europa.eu/smart-regulation/guidelines/tool_3_en.htm.