Guidelines for conducting a data protection impact assessment in regulatory development

V. June 2023

EXECUTIVE SUMMARY

The purpose of these guidelines is to serve as a guide for carrying out a data protection impact assessment (DPIA) in the framework of the preparation of the Regulatory Impact Assessment Report (RIAR), when legislative initiatives, of entities under the competence of the Spanish DPA, involve the processing of personal data.

The DPIA of a rule in which personal data processing is proposed must assess the impact that these have on the fundamental rights and freedoms of individuals taken individually and as a society. Therefore, it is not a legal or compliance risk assessment. The case-law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR) indicates that necessity and proportionality in data protection rules is a fact-based concept, rather than a merely abstract legal notion, and that processing personal data must be considered in the light of the specific circumstances surrounding each case, as well as the provisions of the legislative initiative and the specific purpose to be achieved. Therefore, the DPIA requires applying a step-by-step methodology without automatisms.

This document is aimed to the Public Administration bodies, such ones under the competence of the Spanish DPA, that promote regulatory projects that involve the processing of personal data to which apply Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of personal data (GDPR), as well as the Spanish Fundamental Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and execution of criminal sanctions (F.L. 7/2021). Therefore, it is too aimed to the Data Protection Officers of such Public Bodies to help them to carry out their advisory duties regarding regulatory development.

Keywords: Impact assessment for data protection, DPIA, suitability, necessity, proportionality, risks, rights and freedoms, data protection officer, DPO, Public Administrations, Regulatory Impact Analysis Report, MAIN, RIAR, RIA legislation.

I. CONTENT

I. INTRODUCTION

The purpose of these guidelines is to serve as a guide for carrying out a data protection impact assessment (DPIA) in the framework of the preparation of the Regulatory Impact Analysis Report (RIAR), when legislative initiatives, of entities under the competence of the Spanish DPA, involve the processing of personal data.

The DPIA must be carried out **from the design of the regulation**, as established in the Methodological Guide for the Preparation of a Regulatory Impact Report (R.D. 931/2017):

- The Regulatory Impact Analysis is a continuous process that must allow to adapt the regulation to minimize its impact.
- It is not a mere procedure that is be fulfilled once a new regulatory proposal has been completed.
- Either is it a procedure that ends with the preparation of the Report.
- The Report will be carried out simultaneously with the preparation of the regulation project, from its beginning to its completion.

This document is aimed to the Public Administration bodies, such ones under the competence of the Spanish DPA, that promote regulatory projects that involve the processing of personal data to which apply Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of personal data (GDPR), as well as the Spanish Fundamental Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and execution of criminal sanctions (F.L. 7/2021). Therefore, it is too aimed to the Data Protection Officers of such Public Bodies to help them to carry out their advisory duties regarding regulatory development.

These guidelines are mainly based on the following documents:

- European Data Protection Supervisor (EDPS): Guide to assess the need for processing in policies and legislative measures.
- EDPS: Guide to assess the proportionality of processing in policies and legislative measures.
- European Data Protection Board (EDPB)[1] Opinion 01/2014 on the application of the concepts of necessity and proportionality and data protection in law enforcement agencies.

These documents contain more than 40 examples of necessity and proportionality assessments. To limit the length of this text, a reference is made to some of them without transferring their literal text.

[1] Formerly known as the Article 29 Group (WP29)

II. PREREQUISITES FOR CARRYING OUT THE DATA PROTECTION IMPACT ASSESSMENT

Before performing a DPIA, it is necessary to determine whether certain minimum requirements are met.

A. DETERMINE THE EXISTENCE OF A PROCESSING OF PERSONAL DATA

The notion of personal data is very broad, as it includes any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, by an unique identifier or by one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Therefore, a name, surname, vehicle registration plate, telephone, passport number, location data, IP address, profile linked to a person in any of the abovementioned areas, any other unique identifier, including data or data sets acting as pseudo-identifiers, and those linked to them, shall be considered personal data.[2]

Data processing means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of making available, alignment or combination, limitation, suppression or destruction. (Art. 4.2 GDPR and Art. 5.b F.L. 7/2021). In the case of non-automated processing, the regulation on data protection is applicable when processing data is contained or intended to be included in a file.[3]

The processing of personal data for the purpose of implementing network, information or other security measures, in itself, is a processing of personal data.

Milestone: If the regulation does not propose or involve any processing of personal data, it is not necessary to carry out the DPIA.

B. DETERMINING WHEN AN IMPACT ASSESSMENT NEEDS TO BE CONDUCTED

Both the case-law of the Court of Justice of the European Union (CJEU)[4], as well as the opinions of the EDPS (section II.5 of the EDPS Necessity Guide) state that the impact assessment of a regulation in relation to data protection should be carried out in cases where the proposed legislative measure involves the processing of personal data. Any data processing operation provided for by law constitutes a limitation of the right to the protection of personal data, regardless of whether such a limitation may be justified.

[2] See Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
[3] Art.4.6 of the GDPR "filing system: any structured set of personal data, accessible according to certain criteria, whether centralized, decentralized or distributed functionally or geographically"
[4] 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.

In turn, the European Court of Human Rights (ECHR) has held that the storage by a public authority of data or information relating to a person's private life amounts to a limitation of the right to respect for his or her private life.[5]

The settled jurisprudence of the CJEU establishes that "to determine the existence of an interference in the fundamental right of respect for private life, it is irrelevant whether or not if the information is sensitive or if those affected have suffered some type of inconvenience".[6]

Separate processing operations or all operations (i.e., collection and other operations, such as storage or transfer of or access to data) may constitute separate limitations on the right to the protection of personal data and, where applicable, on the right to respect for private life.[7]

C. DETERMINE THE APPROPRIATE RANGE OF THE REGULATION

Art. 8 of the LOPDGDD (F.L. 3/2018) establishes that the processing of personal data by legal obligation (6.1.c GDPR), public interest or exercise of public powers (6.1.e GDPR), as well as the specialties of the processing subject to F.L. 7/2021, can only be considered founded when it is foreseen or derived from a competence attributed by a rule of European Union Law or a regulation with the rank of law.[8]

Milestone: If the regulation does not have the rank of law, the legal obligations that regulate the processing must be identified with the appropriate requirements and guarantees and allow the development of partial aspects of it. If there is no such rule or does not comply with the legal and jurisprudential requirements to limit the fundamental right, the DPIA cannot be continued and the elaboration of a norm with the rank of law must be proposed.[9]

D. DETERMINE THE QUALITY OF THE REGULATION FROM A DATA PROTECTION PERSPECTIVE

Any legislative measure that legitimates a personal data processing must comply with the premise of "provided for by the law". This means that it must be clear and precise, and its application accessible and predictable for its addressees, in accordance with the

[5] ECHR, Leander v. Sweden, paragraph 48.
[6] CJEU, Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others, paragraph 75 and Digital Rights Ireland, paragraph 33.
[7] As regards Article 8 of the ECHR, see Leander v. Sweden, 26 March 1987, paragraph 48; Rotaru v. Romania GC], no. 28341/95, para. 46 and Weber and Saravia v. Germany no. 54934/00, paragraph 79, ECHR 2006-XI. For Article 7 of the Charter, see CJEU, Digital Rights Ireland, paragraph 35.
[8] F.L. 7/2021, through art.6.2, leads to the obligations of art.8 of the LOPDGDD, for processings that are beyond what is established in art.1 of F.L. 7/2021, also specifically for the processing of special categories of data (art.13) and automated decisions (art14). In addition, this is stated in the explanatory memorandum: "Certain conditions are also required that determine the lawfulness of any processing of personal data, that is, that they be processed by the competent authorities; that are necessary for the purposes of this Organic Law and that, if necessary and in each particular area, the specialties are specified by a norm with the rank of law that includes minimum contents".
[9] STC 292/2000, of 30 November, FJ 15:, *This dual function of the reservation of law translates into a double requirement: on the one hand, the necessary intervention of the law to enable interference; and, on the other hand, this legal norm "must meet all those indispensable characteristics as a guarantee of legal certainty", that is, "it must express each and every one of the presuppositions and conditions of the intervention" (STC 49/1999, FJ 4). In other words, "it not only excludes powers of attorney in favour of regulatory rules [...], but also implies other requirements with respect to the content of the law establishing such limits".*

ECHR[10], the CJEU[11] and the Constitutional Court (TC)[12]. Therefore, the regulation must be clearly defined, precisely and appropriately:

1.- The purpose or purposes of the processing.

The purpose of the processing must be final. For example, a biometric surveillance processing is not an end in itself, but a means (among others) to implement an ultimate purpose such as the security of the State, facilities or others. In the same sense, a technology is not an end, but a means.

2.- The legitimacy of the processing.

Consent (6.1.a GDPR) is not, in general, the appropriate legal basis for a processing established by a regulation due to the clear imbalance between data subjects and a public controller authority, although in certain cases it may be required as an additional guarantee, provided that the requirements for consent in the GDPR are met, particularly that it is free because equivalent alternatives are offered[13].

3.- The description of the processing implementation[14] (In the GDPR, the term "nature" is used) in its relevant aspects, such as the operations and procedures determining the processing (for example, collection, storage, access, transmission, dissemination,...), the technologies proposed to implement the operations (artificial intelligence, cloud storage, biometrics, IoT, mobile, video surveillance,...), the existence of automated decisions, as well as participation or possible participation of processors and/or sub-processors in different operations of the processing, among others.

Section III.B of the Risk Management and DPIA guide develops the elements that define the nature, context, scope and purposes of a processing.

4.- The scope and extent of the processing in relation to the categories of personal data processed (especially if they are special categories), the categories of data subjects concerned, the circumstances in which the personal information is used (for example: systematically, only in certain cases, for a limited period of time, etc.), the retention periods of the data, the frequency of data collection, the granularity of the data and other factors defining the scope of processing[15].

[10] ECHR Benedik v Slovenia, paragraph 132: "the Court considers that the law on which the contested measure was based, namely the collection by the police of subscriber information associated with the dynamic IP address at issue ..., and the manner in which it was applied by the national courts were unclear and did not provide sufficient guarantees against arbitrary interference with the rights provided for in Article 8. In those circumstances, the Court considers that the interference with the applicant's right to respect for his private life was not "in accordance with the law" as required by Article 8(2) of the Convention.".

[11] The STJUE of 6 October 2020, in joined cases C-511/18, C-512/18 and C-520/18, The Quadrature du Net and Others, paragraph 175, points out that: *As regards the justification for such an interference, it should be noted that the requirement, laid down in Article 52(1) of the Charter, that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis permitting it must itself define the scope of the limitation on the exercise of the right in question (see, to that effect, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 175 and the case-law cited)*. In the same vein, ECJ of 6 October 2020 (C-623/17), Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others (paragraph 65), More recently, the Judgment of the CJEU (Grand Chamber) of 21 June 2022, when ruling on Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, I remember his own doctrine in the paragraphs 112 to 118.

[12] STC 76/2019, of 22 May, and STC 292/2000, of 30 November

[13] Recital 43, Guidelines 5/2000 on consent within the meaning of the GDPR

[14] In the GDPR, the term "nature" is used for the description of the implementation of processing.

[15] In the case *Szabo and Vissy v. Hungary*, the ECHR considered that the notion of "*affected persons identified (...) as a series of persons*» could include anyone without the need for the authorities to prove the relationship of the people affected and the prevention of a terrorist attack.

5.- The controller/joint controllers or categories of controllers and, where appropriate, the processors or categories of processors and/or sub-processors, from the point of view GDPR-F.L. 7/2021 must be well defined.

Do not misunderstand the figure of controller GDPR-F.L. 7/2021, legal figure defined in articles. 4.7 GDPR and 5.g F.L. 7/2021, which generally corresponds to a legal person, with the assignment or distribution of responsibilities within the corresponding body/entity or the natural person holding the Direction of the body/entity.

6.- The entities that access and to which personal data may be communicated, as well as the purposes of such communication, in particular, the conditions of the communication of data between public authorities by virtue of a legal obligation for the exercise of an official mission according to the conditions of the GDPR (recital 31):

- In the framework of a specific investigation of general interest.
- In accordance with Union or Member State law.
- In writing and in a reasoned manner.
- Occasionally.
- They should not refer to complete file.
- They must not result in the interconnection of several files[16].

7.- The justification of the solution adopted for the access[17] to personal data, taking into account that it involves the use of data in accordance with specific technical, legal or organizational requirements, without necessarily implying the transmission or download of the data[18].

8.- The measures to guarantee lawful and fair processing, taking into account the nature, scope (especially in relation to special categories of data), context and purposes of the processing or categories of processing, information and transparency mechanisms, as well as those relating to other specific processing situations within the meaning of Chapter IX of GDPR, in particular, that aimed at preventing access or transfer of illicit or abusive data[19].

---

[16] Likewise, it is necessary to recall the doctrine of the Constitutional Court against the massive processing of personal data, collected In its judgment 17/2013, of 31 January 2013, according to which (i) indiscriminate and massive access to personal data must be prevented (ii) the data in question requested must be relevant and necessary (iii) for the purpose established in the precept (iv) the request for access to the specific personal data must be expressly motivated and justified, (v) in such a way that this allows its control by the assignor (vi) and avoids a torticero use of that faculty with massive access. This implies (vii) that the possibility of analyzing whether in each specific case the access was protected by the provisions of the law must be guaranteed.

[17] Recital 7 of the Regulation (UE) 2022/868 dthe European Parliament and dCouncil of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation) "*There are techniques that allow analysis of databases containing personal data, such as anonymization, differential privacy, generalization, deletion and randomization, use of synthetic data or similar methods, and other cutting-edge methods of privacy protection that can contribute to more privacy-friendly data processing. Member States should support public sector bodies in order to make optimal use of such techniques and thereby provide as much data as possible for their exchange...*"

[18] Art.4.2.13 of the Regulation (UE) 2022/868 dthe European Parliament and dCouncil of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation).

[19] As the STC 76/2019, of May 22, regarding the regulation in which these guarantees must be included (F.J.8): *(...) The provision of adequate safeguards cannot be deferred to a time after the legal regulation of the processing of personal data in question. Adequate safeguards must be incorporated into the legal regulation of the processing itself, either directly or directly or by express and perfectly delimited reference to external sources that have the appropriate normative rank. (...). According to settled constitutional doctrine, the reservation of law is not limited to requiring that a law enables the measure restricting fundamental rights, but is also necessary, in accordance with requirements called – sometimes – normative predetermination and – others – the quality of the law and respect for the essential content of the right, that in that regulation the legislator, which is primarily obliged to weigh up competing rights or interests, predetermines the cases, conditions and guarantees under which*

9.- In the case of limitation by law of rights or obligations under article 23 of GDPR or 24 of F.L. 7/2021, its determination must be very clear, the specific conditions of limitation of obligations and rights (GDPR Recital 19), and the concrete damages to the achievement of the purposes that justify the lack of information to the interested parties about the limitation.

The above list is not exhaustive, but any other relevant provision, for each specific case, should be included in the description of the processing.

Milestone: If the regulation does not have the necessary quality from the point of view of data protection, before starting the DPIA process it will be necessary to write it precisely.

III. DATA PROTECTION IMPACT ASSESSMENT

The impact assessment for data protection requires an assessment based on objective facts. There must be a solid justification for the proposed measures that could stand up to scrutiny. Therefore, the proposed measures should be based on research, statistics, evidence-based foresights, etc.

The depth and formality of DPIA needs to be more comprehensive when there is a high risk to the rights and freedoms of data subjects (WP248).

The elements to be evaluated will be:

- Limitations and risks to rights and freedoms.
- Respect for the essence of the law.
- The purpose.
- The proportionality of the processing, including the assessment of suitability, necessity and proportionality in strict sense.

Evaluating each of these elements is not reduced to a mere affirmation or manifestation of its conformity with law requirements. Evaluation is a process to rationally construct a conclusion from the examination and study of concrete evidence.

A. ASSESS LIMITATIONS AND RISKS TO RIGHTS AND FREEDOMS

Within the framework of the DPIA, the limitations and risks to the rights and freedoms for natural persons that the processing or the processing operations necessary to achieve the objectives that the regulation may entail, must be identified.

The mere fact that a measure limits or poses risks to the exercise of these rights does not mean as such that the measure should not be proposed. However, the measure will have to be considered in such a way that it exceeds a DPIA, i.e., that the risks to natural persons could have been adequately mitigated and the suitability, necessity and proportionality analysis in the strict sense has been passed.

measures restricting fundamental rights are appropriate. That predetermination mandate in respect of essential elements, also ultimately linked to the proportionality assessment of the limitation of the fundamental right, cannot be deferred to further legal or regulatory development, nor can it be left in the hands of individuals themselves. (...)

The rights and freedoms of data subjects mainly concern the rights to data protection and privacy, but also refer to other fundamental rights (WP248), such as freedom of expression, freedom of thought, freedom of movement, freedom for personal self-determination, the prohibition of discrimination (difference in processing between persons), freedom of conscience and religion, inviolability of communications, right to effective judicial protection, freedom to receive information, right of assembly and demonstration, etc.

It is necessary to carry out a deeper analysis than simply determining whether there is processing of special categories of data. Those initiatives that involve processing in which their implementation involves artificial intelligence, automated decisions, biometrics, mass surveillance, large-scale centralization, massive data processing, data of minors, vulnerable people, etc., could imply additional risks and unwanted collateral impacts.

Taking into account that the processing carried out by a Public Administration affect large social groups, if not the whole society, the risks must be studied in two dimensions:

- Risk to the rights and freedoms of individuals.
- Risk to society itself (or to a representative group of it)[20].

It is important to note that the materialization of a risk factor, its impact may be minor with regard to the person concerned and yet significant or very significant with regard to society as a whole. Some hypothetical examples are: damage to the electoral and political processes (misuse of data for political manipulation); illegal profiling and discrimination, which lead to mistrust of public authorities; the 'chilling effect' on freedom of expression of pervasive surveillance measures or other negative effects on the freedom of individuals resulting from a pervasive and systematically applied profiling and scoring system (step III.6.2 of the EDPS Proportionality Guide).

In determining individual and societal risks, it must be considered the possibility of personal data breaches, even massive ones.

To help to identify risks for the rights and freedoms, we recommend consulting the guide "Risk management and impact assessment on personal data processing", the "List of tables of the Risk Management and Impact Assessment guide in editable format", or the Evalúa Riesgo tool, in which more than 130risk factors that appear in the data protection regulations are identified. The risk factors identified there do not constitute an exhaustive or enforceable[21] list for all cases, but only an orientation of those that could be found in a processing.

B. RESPECT FOR THE ESSENCE OF THE LAW

The processing of personal data constitutes a limitation of the right to data protection. As provided for in art. 52.1 of the Charter of Fundamental Rights of the European Union,

[20] See Omri Ben-Shahar, Data Pollution, University of Chicago, June 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191231 See page 3: "The privacy paradigm is based on the premise that the harm produced by the personal data company is private in nature, to the 'core of the self', although by mere aggregation (or by more nuanced channels) these harms of a deeply private nature have a derived social impact"; and page 4: "The literature has examined all aspects of private damage resulting from data collection, possible infringements of the privacy of the persons whose data are collected. However, the problem of externality has been completely neglected: how people's participation in data collection services affects others, and the general public."

[21] That is, not all that could appear in a processing are there, nor all those shown arise in all processing. It has been detected that when the data protection regulation lists examples or uses the expressions "among others" or "as...", it is being interpreted as an exhaustive and enforceable list (e.g. in the case of article 25.1 or 32.1.a in relation to pseudonymization).

as well as the CJEU[22], the limitation must **respect the essence** of **the right** to data protection so that its fundamental elements are not empty of content and thus end up preventing the exercise of it[23].

The evaluation of respect for the essence of the law may, in some cases, need a thorough legal analysis and be the most critical point of the DPIA.

Milestone: If the essence of the right was affected, the measure would be illegal[24] and would have to be reformed before the DPIA could continue.

C. PURPOSE ASSESSMENT

For each of the purposes, it is necessary to evaluate:

1.- If there is a correct application **of the principle of purpose**, being as specific as possible about the purposes for which a proposed measure could authorize the collection and processing of personal data (WP211 pag.16). Compliance with the SMART criterion, defined by the European Commission, can help to detail this. This criterion establishes that the purposes must be:

a.- **Specific** (sufficiently precise and concrete);

b.- **Measurable** (define a desired future state in measurable terms, for example, estimated decrease in crimes by a percentage, etc.);

c.- **Achievable**;

d.- **Realistic**; and

e.- **Time-dependent** (related to a fixed date or period of time in which the results must be achieved).

2.- The regulation pursues a **legitimate** objective or objectives (WP211), that is, an objective of general interest recognized by the Union or the need to protect rights and freedoms, within a democratic society, defined in a concrete and not hypothetical way.

For example, the general objectives referred to in Articles 3 or 4 (2) TEU, other interests protected by specific provisions of the Treaties, those thus interpreted by the CJEU, those listed in Art. 23.1 GDPR or Art. 1 of F.L. 7/2021, the right of access to personal data, the obligations of the controller or transparency and public scrutiny (Articles 1 and 15.1 TEU), protection of intellectual property

[22] Michael Schwarz vs. Stadt Bochum, CJEU, C-291/12, (CJEU, 17 October 2013), not published. The applicant disputed the refusal of the authorities in the German city of Bochum to issue him with an (EU) passport unless he had two fingerprints stored in that passport. This obligation has its origin in Regulation (EC) No 2252/2004 of 13 December 2004 on rules for security features and biometrics in passports and travel documents.

[23] STC 292/2000, of 30 November. FJ 7 7. *"It follows from all of the foregoing that the content of the fundamental right to data protection consists of a power of disposition and control over personal data which entitles the individual to decide which of that data to provide to a third party, be it the State or an individual, or which that third party may collect, and that also allows the individual to know who owns that personal data and for what, being able to object to that possession or use. These powers of disposition and control over personal data, which constitute part of the content of the fundamental right to data protection, are legally specified in the power to consent to the collection, obtaining and access to personal data, their subsequent storage and processing, as well as their possible use or uses, by a third party, be it the State or an individual. And that right to consent to the knowledge and processing, computer or not, of personal data, requires as indispensable complements, on the one hand, the ability to know at all times who has those personal data and to what use they are subjecting, and, on the other hand, the power to oppose that possession and uses. "*

[24] In According to Ms. Schrems, the CJEU considered that the right to effective judicial protection was affected.

rights and the right to effective judicial protection, freedom of expression and enterprise, among others.

3.- The purpose established in the regulation must be **defined with fairness**, as established in GDPR articles 5.1 and 6.1.a F.L. 7/2021, so that the processing is not framed in a measure that does not really address the declared problem but a different purpose[25].

The implementation of video surveillance of a public access area justified in an increase in security might not be loyal if what you are really looking for is an image measure in the face of social unrest, or cost reduction.

D. ASSESSMENT OF SUITABILITY AND NECESSITY

According to the CJEU and the ECHR, the necessity in data protection regulations is a fact-based concept, rather than a merely abstract legal notion. The need should be considered in light of the specific circumstances surrounding the processing.

The need assessment should consider the following elements:

1.- Application of the concept of **strict necessity**[26]: It must be evaluated that a processing that restricts fundamental rights solves a problem that must be real, present or imminent, and critical for the functioning of society[27].

The ECHR[28] established that "necessary" "...It was not synonymous with indispensable... nor does it have the flexibility of expressions such as 'permissible', 'ordinary', 'useful', 'reasonable' or 'desirable'". Mere convenience or profitability is not enough[29].

It follows from the case-law of the CJEU that the condition of strict necessity is transversal, regardless of the area concerned, such as the police or commercial sector[30].

The factual answer to the following question (WP211) must be reasonably answered on the basis of facts: Is the processing attempting to address a problem that, if not addressed, could result in harm or have detrimental effects on society or a part of society?

Examples can be found in paragraph 3.15 of WP211.

2.- The **suitability of a measure** must be established: it must be assessed that there is a logical and direct link between the processing and the objective pursued.

[25] «Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017
[26] The Sunday Times v United Kingdom Case No 6538/74 (ECHR, Thursday, 6 November 1980, paragraph 59).
[27] ECHR, Szabo and Vissy v. Hungary, paragraph 73.
[28] Handyside v United Kingdom Case No 5493/72 (ECHR, 7 December 1976, paragraph 48).
[29] Article 29 Working Party, Opinion 3/2012 on the evolution of biometric technologies, WP 193, 27.04.2012, p. 8.
[30] 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 Opinion AG 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 passenger name records, paragraph 226.

3.- It is necessary to determine the real effectiveness of the **processing**, that is, to determine by means of proof that it is capable of reaching a minimum level of effectiveness in solving the need raised.

We must accept the reality that in any type of purpose and for any processing it is impossible to achieve perfection. Apart from the fact that it is not economically efficient, nor technically feasible, there are multiple factors that prevent total effectiveness, especially in security issues. Assuming this reality, it is necessary to determine the acceptable level of efficiency required to meet the strict need and demonstrate that the proposed processing achieves it.

4.- **Evaluation of the level of intrusion.** Estimating among others:

a.- The **nature of the interference**: or how rights and freedoms are limited or put at risk as established in section III.c.

b.- The **scope/extent** of the processing.

c.- The **context** in which the regulation is to be applied or the nature of the activity that is the subject of the measures[31].

c.- If "**collateral intrusions**" may appear, that is, interferences in the privacy of people other than the subjects of the measures[32].

5.- **Minimum intrusion**: It is necessary to evaluate the scope, extent and intensity of interference in terms of impact on fundamental rights, explaining with evidence why other possible alternatives are not enough to satisfy this need sufficiently:

a.- Among the measures already existing in relation to the proposals, in particular, consider a more appropriate application than the existing measures.

b.- Among the measures proposed in relation with other options that allow to achieve the same objective, including a possible combination of measures.

With regard to the level of effectiveness required to meet the strict need, it must be determined that the existing measures did not comply with it, and that the consequences of this non-compliance are no longer acceptable.

Milestone: Make a decision ("yes/no") about whether processing meets the principle of necessity. If the result is "no", the rule needs to be amended and the assessment of the DPIA is stopped.

E. ASSESSMENT OF PROPORTIONALITY[33]

Data protection is not an absolute right and can always be limited within a fair balance. A processing developed in a rule must respect the principle of proportionality,

[31] In the case In the event of Mr. Dudgeon, the ECHR emphasised the particularly sensitive nature of the activity affected, as well as the circumstances in which the measure was applied. While the sensitivity of the activity or information in question will be relevant, it is equally relevant to consider whether a measure will be applied in circumstances where individuals may have high expectations of respect for their privacy.

[32] See Big Brother Watch and Others v. United Kingdom, ECHR, 13 September 2018, paragraph 2.43.

[33] ECJ of 16 July 2020, Schrems 2 (section 176): *Finally, in order to satisfy the requirement of proportionality according to which exceptions to the protection of personal data and limitations of that protection must not go beyond what is strictly necessary, the legislation at issue entailing the*

which 'restricts the authorities in the exercise of their powers by striking a balance between the means used and the intended objective (or the result achieved)'[34].

As with all evaluations, assessing proportionality is not reduced to simply stating proportionality.

The assessment of proportionality requires a positive evaluation of the assessment of necessity[35] and draws on the conclusions drawn from it. Therefore:

1.- Using the result of **the strict evaluation of necessity** of the processing and the level of intrusion carried out in the evaluation of the need, is necessary to proceed with the evaluation of the **fair balance** (advantage/disadvantage; individual and social benefit/cost) of the measure[36].

a.- The CJEU explained that it is essential to point out that proportionality is a **specific assessment,** on a **case by case**[37] processing.

b.- **Importance of the purpose**: it is necessary to evaluate whether, in addition to the strict necessity, the purpose to be fulfilled tries to protect a constitutional value or a fundamental right.

b.- It must be taken into account all possible **circumstances** of the known matter within a given **contextual**[38] issue.

The right to the protection of personal data may play the role of a concurrent right, i.e. not the one that is primarily affected by the measure, but together with other rights (freedom to conduct a business; freedom to receive or impart information), may tip the balance in favour of the non-proportionality of the measure[39].

c.- It is necessary to determine if **the scope** of the proposed processing is sufficiently limited. This may cover the number of persons affected by

---

interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum requirements, so that persons whose data have been transferred have sufficient safeguards to effectively protect their personal data against the risks of abuse. In particular, that legislation must indicate under what circumstances and under what conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is of particular importance where personal data are subject to automated processing (see, to that effect, Opinion 1/15 (EU PNR Agreement)-Canadaá) of 26 July 2017, EU:C:2017:592, paragraphs 140 and 141 and the case-law cited).

Conforme to the doctrine of our Tribunal Constitutional, (STC 14/2003, of 28 January):*"In other words, in accordance with a settled doctrine of this Court, the constitutionality of any measure restricting fundamental rights is determined by strict observance of the principle of proportionality. For the purposes of the present matter, it is sufficient to recall that, in order to determine whether a measure restricting a fundamental right passes the proportionality test, it is necessary to ascertain whether it satisfies the following three conditions or conditions: whether the measure is capable of achieving the objective proposed (suitability assessment); if, in addition, it is necessary, in the sense that there is no other more moderate measure for the achievement of that purpose with equal effectiveness (judgment of necessity); and, finally, if it is weighted or balanced, because it derives more benefits or advantages for the general interest than damage to other goods or values in conflict (proportionality judgment in the strict sense; STC 66/1995, of 8 May, F. 5; STC 55/1996, of 28 March, FF. 7, 8 and 9; STC 270/1996, of 16 December, F. 4.e; STC 37/1998, of 17 February, F. 8; STC 186/2000 of 10 July, F. 6)."*

[34] 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).

[35] In Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, the Court of Justice held that the limitation of the rights protected in Articles 7 and 8 was not necessary (see paragraph 65 above) and therefore concluded that the limitations were not proportionate (paragraph 69). Similarly, in Case C-362/14 Schrems, paragraphs 92, 93, where the CJEU assessed the necessity and considered that the Safe Harbour Decision was invalid, without making any reference to proportionality before reaching this conclusion (paragraph 98).

[36] See, for example, case C-83/14 *Razpredelenie Bulgaria Ad,* aloof. 123. The Court notes that *«... Assuming that no measure of equal effectiveness than the practice at issue could be identified, the referring court will also have to ascertain whether the disadvantages caused by the practice at issue are not disproportionate to the objectives pursued and whether that practice does not unduly prejudice the legitimate interests of the people living in the neighbourhoods concerned.*».

[37] CJEU, Case C-101/01, Linqvist, ECLI:EU:C:2003:596, paragraph 89.

[38] ECHR, M.K. v. France, paragraph 46

[39] Scarlet Extended (CJEU, C-70/10, ECLI:EU:C:2011:771)

the measure or the amount of information collected or the period for which that information will be retained. The scope may cover all, part or none of these elements depending on the measure in question.

d.- It is necessary to take into account the **general opinion** (social, historical or political aspects, etc.) of society on the subject in question.

e.- It must also be taken into account the **objections** expressed by society.

A number of examples can be found in paragraph 3.20 of WP211.

f.- A **holistic approach** must be applied. In order to be able to say whether a new legislative proposal is proportionate, it is necessary to assess how the new measure will complement existing ones and whether all legislative proposals together would continue to proportionately limit fundamental data protection and privacy rights (WP211 under paragraph 6.1).

In paragraph 5.11 of WP211 there is an example on the limitation of scope

2.- It is necessary to evaluate what "**safeguards**" accompany the measure to reduce the risks to fundamental rights (See next section).

Steps 1 and 2 can be repetitive, that is, if the processing is not proportional, more safeguards can be applied, and the fair balance assessment can be performed once again.

3.- Make a decision ("yes/no") on whether the processing complies with the principle of proportionality. If the result is 'no', not least because it does not secure sufficient safeguards to make the measure proportionate, then a rewording of the rule will be necessary.

F. SAFEGUARDS

Art. 24.1 GDPR and art. 27.1 F.L. 7/2021 establish that the controller **will apply appropriate** technical and organizational measures, taking **into account** the **nature, scope/extent[40], context and purposes** of the processing as well as the risks of varying probability and severity **for the rights and freedoms of natural persons**, in order to **guarantee and be able to demonstrate[41]** that the processing takes place in accordance with data protection regulations. Those measures shall be **reviewed** and **updated** as necessary.

They will need to be reviewed and updated, at least when the nature, context, scope/extent, purposes or risks change. In addition, in case of security measures, these will have to be reviewed periodically (art. 32.1d GDPR).

The measures that can be incorporated into a normative text may have certain specificities in relation to a processing.

[40] Both expressions are used in the translation of the GDPR into Spanish, and with both their semantic extension is established more precisely.
[41] The text "and be in a position to demonstrate" that appears in article 19.1 of the LED Directive 680/2016 has not been transposed to the text of article 27.1 of F.L. 7/2021, although it is presumed that it must be interpreted in that sense.

In Chapter VIII "Controls to reduce risk" of the Risk Management and DPIA guide, as well as in the Guidelines of Data Protection by default and by the design, more than 200 measures are listed.

Among these specificities, and as an example since it is not an exhaustive or required list for all cases, we could find:

- Regarding the measures on the concept of processing:
  - Application of the precautionary principle[42]. Where it is difficult to determine in advance any or part of the impact of processing, it could be suggested to the legislator to adopt an 'incremental approach', in the deployment of processing (geographical limitation, in categories of data subjects, etc.)., so that this incremental deployment allows identifying risk cases that have not been adequately assessed, thus mitigating the possible impact of these initially unidentified consequences.
- Legal Measures:
  - Incorporate an independent monitoring system to prevent a temporary measure from becoming permanent.
  - Establish a total or partial expiration of the processing operations in the same norm (e.g., termination clauses "unless confirmed or revised, the measure will no longer be applicable from ...")
  - Implement a prior judicial control of the processing operations carried out[43] in the cases of greater interference in the rights and freedoms[44].
- Organizational and governance measures:
  - Establishment of obligations to carry out DPIA and/or Prior Consultations to the subjects obliged by the norm to implement part or all of the processing.
  - Periodic reassessment of the necessity and proportionality of processing.

There is an example in paragraph 5.16 of WP211

  - Periodic evaluation of the safeguards in place.
  - Audits of the concrete implementation of processing by independent third parties
- Data protection measures by design and by default:
  - Limit the conservation of data, including anonymization, pseudonymization, selective elimination of sensitive attributes, or others based on their effective contribution to the purposes pursued.

[42] On 2 February 2000, the European Commission stated in its Communication on the precautionary principle (COM(2000)1 final): 'Although only the precautionary principle in the environmental field is explicitly mentioned in the Treaty, its scope is much broader. This principle covers specific cases where scientific data are insufficient, inconclusive or uncertain, but where a preliminary objective scientific assessment raises suspicions. What There are reasonable grounds to fear that potentially hazardous effects on the environment and human, animal or plant health might be incompatible with the high level of protection chosen.';

[43] SEPD, pleadings at the hearing in the case of the draft EU-Canada PNR 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.

[44] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland

- There is an example in paragraph 5.17 of WP211
    - Limit the extent of the individuals affected (e.g., certain categories of persons, users of a service, suspects of a crime, foreigners, nationals, etc.).
    - Incorporate additional guarantees according to the categories of stakeholders (e.g., for vulnerable groups that are within the scope of application).
    - Incorporate additional guarantees in case of, for example, automated decisions.
    - Limit the categories of data collected (e.g., video, audio, temperature, biometrics, etc. can be processed in video surveillance).
    - Differentiate, limit and subject to exceptions the persons whose information is used according to the objective sought[45].
    - Limit geographical extent.
    - Limit the extent of affected behaviors.
    - Limit possible processing operations (e.g., in relation to analyzing, combining and communicating information.)
    - Limit the period of data processing, reducing this from a long term to a short term.
    - Fast data locking.
    - Set restrictive access policies for retained data.
    - Establish supervised and non-automatic procedures for access to retained data.
    - In relation to the previous point, increase the requirements of level of conservative data access with temporal criteria.
    - Keep detailed records of who accesses the data.
    - Keep detailed records of data communication between public entities.
- Personal Data Breach Management
    - Extend the obligations established in articles 33 and 34 of the GDPR and 38 and 39 of F.L. 7/2021.

IV. DPIA QUALITY ASSESSMENT

DPIA carried out within the framework of regulatory development must meet the following requirements to be considered acceptable:

- Be carried out from the design of the regulation and incorporated into the Regulatory Impact Analysis Report.
- To answer all the questions identified in chapters II and III.
- Exceed the milestones established in the chapters indicated.
- Base all responses on appropriate evidence, establishing that the assessments required in these guidelines have been carried out and retaining (recording and storing) all relevant documentation obtained or produced during the conduct of the assessments and the drafting of the DPIA Report. Such documentation

[45] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, paragraph 57; C-362/14 Schrems, paragraph 93.

should be relevant and sufficient to justify, or identify, the critical issues of the measure under consideration, and should be referenced in an annex to the report.

- Achieving information symmetry, for example in the proportionality assessment, where there are known benefits but unknown costs, or vice versa, will be difficult, if not impossible, to establish whether the measure is proportionate. (Step III.6.3 of the EDPS Proportionality Guide). In the same way it can happen in the evaluation of the least intrusive measure.

Milestone: In the event that the above conditions are not met, it will be presumed that the DPIA has not been correctly performed and will have to be reviewed.

V. CONCLUSIONS

The DPIA of a rule in which personal data processing is proposed has to assess the impact that these have on the fundamental rights and freedoms of individuals taken individually and as a society. Therefore, it is not a legal or compliance risk assessment.

The jurisprudence of the CJEU and the ECHR indicates that necessity and proportionality in data protection regulations is a fact-based concept, rather than a merely abstract legal notion, and that processing must be considered in the light of the specific circumstances surrounding the case, as well as the provisions of the measure and the specific purpose it seeks to achieve (section II.6 of the Guide to the Necessity of the EDPS).

The DPIA of a rule in which processing of personal data is proposed is not a legal report that justifies a processing from a position of immutability of the pre-established idea. Although it has a very important legal analysis part, it also has a part of management of limitations and risks to fundamental rights and freedoms, of organizational management measures and also an approach of legal and technical measures.

The DPIA requires applying a step-by-step methodology, it is not an activity that can be automated, although tools can be used to help in the process of carrying it out, such as Evalúa-Riesgo Risk Assessment Tool[46].

Finally, it should be noted that in the Public Administration Area of the AEPD website, the most relevant reports of the Legal Office will be collected in relation to the realization of an impact assessment for data protection in regulatory development.

VI. MATERIAL TO SUPPORT THESE OBLIGATIONS

Resources can be found on the AEPD website that expand on the content of these guidelines or help the implementation of the DPIA in the MAIN[47]:

A. GENERAL RISK

- Risk management and impact assessment on the processing of personal data

[46] The FACILITA or DPIA manager tools are not suitable for the DPIA of a regulation.
[47] MAIN: Memoria del Análisis de Impacto Normativo.

- List of tables of the Risk Management and Impact Assessment guide in editable format
- Checklist for determining the formal adequacy of a DPIA and the submission of prior consultation
- RISK-ASSESSMENT v2 tool for the analysis of risk factors

B. SPECIFIC FOR AA.PP.

- Data Protection Impact Assessment (DPIA) report template for Public Administrations
- Guide to Technologies and Data Protection in AA. PP

C. SPECIFIC TO REGULATORY DEVELOPMENT

- EDPS: A Guide to Assessing the necessity of measures in Policies and Legislative Measures
- EDPS: A Guide for Assessing the Proportionality of measures in Policies and Legislative Measures
- WP29: Opinion 01/2014 on the application of the concepts of necessity and proportionality and data protection in law enforcement (WP211)