INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

JUST-JTRA-EJTR-AG-2016
Action grants to support European judicial training
JUSTICE PROGRAMME
GA No. 763866

INtroduction of the data protection reFORM to the judicial system
INFORM

WP2: Data Protection regulatory review & training material elaboration

D2.10 Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights

Lead partner: Inthemis
Author: Estelle De Marco

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Project co-funded by the European Commission within the JUST Programme		
Dissemination Level:		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version 1	Originated by: Estelle De Marco Inthemis	27/2/2018
Version 1	Reviewed by: Matthias Eichfeld, University of Göttingen	1/3/2018
Version 2	Reviewed by: George Dimitrov, Law and Internet Foundation	8/3/2018

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Executive summary

Despite a wording that might sometimes differ, both Directive 1995/46/EC and the General Data Protection Regulation (GDPR) protect the right to personal data and the other fundamental rights that might be impacted by a personal data processing, including non-exhaustively the right to private life, the right to freedom of expression, the freedom of thought, conscience and religion, the freedom of assembly and association, the freedom of movement, the right to conduct a business, the right to the integrity of the person, the right to liberty and security, the right to self-determination and to personal autonomy, the right to a fair trial, the freedom of the arts and science and other cultural rights, the freedom to choose an occupation, and the right to property.

This protection has been strengthened in the letter of the GDPR, but an ethical approach of Directive 1995/46/EC, following especially the Article 29 data protection working party's opinions, enabled to make identical conclusions in relation to most of legislative requirements. Indeed, both instruments constitute practical implementations of the requirements of the European Convention on Human Rights (ECHR) and of the EU Charter of Fundamental Rights (EUCFR) for limiting so-called "conditional"[1] fundamental rights, in particular the principles of necessity and proportionality. As a result, in an approach based on legal ethics[2], real differences that can be noticed between these two legal instruments lie in the practical choices that have been made in order to ensure the necessity and the proportionality of processing operations in particular contexts, which differ for example drastically (and essentially) in relation to data controllers' liability and accountability, in relation to the obligation of security and in relation to the territorial scope of application of the data protection legislation. This *inter alia* confirms that data processors should be encouraged to master the concepts of necessity and proportionality, and to properly apply them to processing operations that cannot

[1] Some of the rights identified in the European Convention on Human rights are called "absolute", such as the right to life or to not be subjected to torture, while others are called "conditional" because they can be subjected to dispensations and/or limitations, as the right to respect for private life and the right to freedom of expression: Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", *in Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, pp.44-45).
[2] See below the Sections 2.1 and 2.4.3 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

comply with law in certain situations, in order to find alternative safeguards that enable to protect adequately personal data and natural persons while allowing the implementation of innovative processing chains, under the supervision of the relevant supervisory authority. Further, the application of the principles of necessity and of proportionality in the GDPR or by the data processor him or herself constitutes also a mean to balance the right to the protection of personal data with the other rights that might be affected by this protection, since the necessity and proportionality tests are contextual and take into account the value and legitimacy of the rights that oppose the protected right[3].

[3] See below the Section 2.3.2.4 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Table of Contents

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

1. Introduction

1.1 Project summary[4]

INFORM[5] is an 18-month project, funded by the European Commission under the Justice (JUST) Programme 2014-2020, introducing to the judiciary, legal practitioners, and court staff the new data protection legislation provisions. The project is designed to contribute to the effective and coherent application of the General Data Protection Regulation (GDPR) and to facilitate the implementation and practical application of Directive (EU) 2016/680. Under the coordination of Law and Internet Foundation, the project will cater to the training needs of the judiciary, legal practitioners, and court staff and present them with a comprehensive overview of the new EU data protection legislation. The project concept is to reach the judiciary, legal practitioners and court staff utilising train-the-trainer approach. INFORM will engage trainers, empowering them with tailor-made materials and customised training methodology.

The project team includes ten European partner organisations from leading universities and research centres in Bulgaria, Cyprus, the Czech Republic, France, Germany, Hungary, Italy, the Netherlands, Poland, and Slovakia.

1.2 Project context and objectives[6]

Ensuring personal data protection has emerged as a fundamental objective in achieving the European Digital Single Market Strategy. The EU acknowledged the urgent need for responding the challenges posed by the digital era - the large-scale deployment of information and communication technologies in people's daily life, business and the new channels of communicating such as online social networks have profoundly changed the ways and the scope of sharing, collecting and storing

[4] The current summary has been prepared by Bart Custers and Georgios Stathis, University of Leiden.
[5] http://www.inform-project.eu.
[6] The current Section has been prepared by Rosaliya Kasamska, Law and Internet Foundation.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

personal information. Citizens, overall, tend to feel that their data has been left unprotected - according to the statistics in the Special Eurobarometer 431 - Data Protection report (June 2015) two-thirds of respondents (67%) are concerned about not having complete control over the information they provide online. This altered environment demanded higher safeguard of this yet fundamental right, which ultimately lead to the adoption of the General Data Protection Regulation (GDPR) and Directive 2016/680 in April 2016, after 4 years of hard work on the exact provisions. The new legal acts will enter into force in May 2018. Until then, private, public sectors and individuals have to familiarise with their new rights and obligations. In the Impact assessment report regarding the new data protection legislation (DPL) the Commission identifies that as regards administrative and judicial remedies and compensation, individuals are in most cases not aware of the possibility to lodge a complaint to public authority responsible for the protection of personal data and therefore, in many Member States judicial remedies, while available, are very rarely pursued in practice. However, this situation will be reversed with the new rights and obligations under the DPL. Now the new regulation provides data subjects with improved administrative and judicial remedies in cases of violations, which will ultimately lead to an increased rate of cases, related to data protection. However, this requires increased recognition of the relevance of EU law. As stated in a study regarding Judicial Training in the European Union Member States (2011) there is general lack of sufficient knowledge of EU law. This additionally emphasises the need to ensure that judicial systems are aware and ready to provide adequate protection of personal data. Courts should act as a counterbalance to the unlawful acts of the competent authorities in the field. To this end, all actors involved in the performance of court activities should have extensive knowledge, skills and competences which will ensure the correct implementation, interpretation and application of the new DPL.

To meet this challenge INFORM aims to provide comprehensive and multidisciplinary understanding of the new DPL through the development of high qualitative training materials, trained trainers in the field throughout all MS and e-Learning programme. Moreover, the analytical activities of the INFORM project will examine the balance between personal data protection and the

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

other fundamental rights in order to deepen the expertise of the professionals, especially when it comes to judges and lawyers. Therefore, the INFORM project targets the following groups of professionals - the judiciary, legal practitioners and court staff.

The target groups were chosen to encompass all relevant actors in the judicial system. The first INFORM target group is the Judiciary. Acknowledging the differences between legal systems INFORM will customize its activities, while aiming to cover this diversity. Therefore, for the purposes of this project, "judiciary" will refer to judges and prosecutors. Additionally, the partnership decided that this group should include also the authorities responsible for the prevention, investigation, detection or prosecution of criminal offences as well, as these are the "competent authorities" as defined in Directive 2016/680 and a main focus of it.

Legal practitioners are another target group. The group refers to lawyers, notaries, bailiffs, mediators. Enriching their knowledge in the field of DPL will enhance Data Subjects' rights, as will enable this group to provide adequate advocacy that considers DPL.

Furthermore, INFORM targets court staff since court clerks and officers are the ones handling courts' communications with citizens, data handling and storage, etc. INFORM initial desk-based research revealed that in all partner countries there is no data protection training aimed at court staff.

These target groups will be reached on two levels. On the one hand, the to-be developed e-Learning programme will directly focus on the aforementioned groups. On the other hand, INFORM will train trainers from the national institutions responsible for the trainings of the target groups. Thus, trainers are the last INFORM target group. The interaction with the trainers will happen during the INFORM workshops. INFORM employs "Training of Trainers" (ToT) approach to effectively reach out the first three target groups. It is worth stressing that ultimately the indirect beneficiaries of the project results will be the data subjects themselves.

To tackle the aforementioned problems INFORM sets the following objectives:

- to contribute to the effective and coherent application of GDPR;

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- to facilitate the implementation and practical application of Directive 2016/680;
- to elaborate specific training materials and methodologies tailored to the needs of judiciary, legal practitioners and court staff, which will involve multidisciplinary knowledge of the DPL as well;
- to train trainers from all MS as multipliers of INFORM outputs and impact mainly at national level;
- to develop interactive practical-oriented e-Learning programme targeting judiciary, legal practitioners and court staff as a training tool for distance self-learning and as an advanced training means;
- to improve target groups' knowledge, competences and attitudes to the DPL;
- to strengthen data subjects' right to data protection.

1.3 Purposes of this report

The current report aims at performing a comparative analysis on the differences between Directive 95/46/EC & the GDPR, and on the relations of these texts, the GDPR in particular, to the other fundamental rights.

Such a study implies first to conduct an analysis of the interrelations between the GDPR and Directive 95/46/EC on the one hand and the right to personal data protection, the right to private life and the other fundamental rights on the other hand, since the existence of the latter rights is the reason for the protection that is organised in the GDPR and Directive 95/46/EC. As a result, the comparison of the provisions of both legal instruments, which we will be performed as a second step in the third section of the current report, must take this context into account.

Indeed, the GDPR is announced to be a text that, *inter alia*, reinforces data controllers' liability and data subjects' rights. These rights include the right to personal data protection and its components, and all the other fundamental rights that can be limited in case of interference with the right to

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

personal data protection. These fundamental rights are *inter alia* the right to private life, the right to freedom of expression, the right to presumption of innocence and related rights, the right to non-discrimination, the right to freedom of assembly, the freedom of movement, the right to liberty and security, and the right to conduct a business[7].

At the same time, the GDPR intends to ensure "*the free flow of personal data throughout the Union*"[8] and to secure data controllers' activities in order to enable the exercise of rights that might have to be balanced against the right to protection of personal data[9], such as the right to freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity[10].

Directive 1995/46/EC appears to have the same goals and to protect exactly the same rights, and both legal instruments appear to be, in effect, practical applications of Article 8 of the European Convention on Human Rights (ECHR) and of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (EUCFR).

As a consequence, the analysis of the interrelations between the right to personal data protection and private life on the one hand, and between the right to both privacy and personal data protection and a series of other rights on the other hand, will enable to understand the philosophy that underlies the protection mechanisms that are organised in the ECHR and in the EUCFR, which will also be detailed. A complementary analysis of the way the GDPR and Directive 95/45/EC have transcribed these interrelations between rights and the afore-mentioned protection mechanisms will enable to understand the philosophy that underlies the protection mechanisms that are organised in both these

[7] For an overview of all these rights see for ex. Estelle De Marco *et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework*, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 4.

[8] GDPR, Recital n° 9. The GDPR notably aims at securing the pursuit of economic activities at the level of the Union.

[9] GDPR, Recital n° 4.

[10] GDPR, Recital n°4. See also *Handbook on European data protection law*, European Union Agency for Fundamental rights and Council of Europe, 2014, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, Section 1.2 pp. 21 *et seq.*, in which is evoked the right to access documents, the freedom of the arts and science and the protection of property, based on ECtHR and CJEU court cases.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

data protection legislations, and therefore to compare efficiently their provisions, through a better understanding of differences, advantages and disadvantages of each of them, and a better perception of the way fundamental rights must be balanced in case they are found in conflict.

1.4 Structure of this report

The document structure is as described below:

Section 1 provides an introduction.

Section 2 provides an analysis of the relations of the GDPR and of Directive 95/46/EC to the other fundamental rights.

Section 3 provides a comparative analysis between the GDPR and Directive 95/46/EC.

Section 4 provides a conclusion.

An Annex presents an explanation of the meaning of the fundamental principles relating to processing of personal data the way they are part of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2. The relations of the GDPR and of Directive 95/46/EC to the other fundamental rights

The question of the relations between the protection of personal data and other fundamental rights including privacy is a crucial question in order to understand the data protection legislation (2.1). It implies to analyse the interrelations that do exist between private life protection, personal data protection and other fundamental rights protection (2.2) and to shed light on the mechanism that is used at the ECHR and the EUCFR levels in order to protect both these spheres (2.3). It implies finally to study the way they are transcribed both in Directive 95/46/EC and in the GDPR (2.4).

2.1 - The interrelations between rights: a crucial question to understand the data protection legislation

The question of the interrelations between the right to personal data protection, the right to private life and the other fundamental rights is a crucial one, since it enables to apprehend the philosophy underlying Directive 95/46/EC and the GDPR. As a result, it enables to have an ethical[11] - and, therefore, accurate[12] - approach and application of these instruments, and enables to distinguish, where legal instruments use different wording, between variations of shape and fundamental differences.

[11] Taking into account the philosophy that underlies the legal system is considered as constitutive of legal ethics: see Jean-Claude Rocher, *Aux sources de l'éthique juridique - Les présocratiques*, June 2001, ed. Fac 2000, coll. Reflechir, especially pp. 11-13; Estelle De Marco *in* Estelle De Marco *et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework*, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 3.3.

[12] The spirit of law makers being to protect citizens' fundamental rights, an application of legal instruments that takes correctly into account the system of values that underlies these instruments and the very meaning of each of the notions they use seems to be appropriate to reach an accurate application of these texts (and the results that law makers wanted to reach).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Indeed, all these rights are named in Directive 95/46/EC and in the GDPR. However, they are mentioned in slightly different ways, which might have consequences on the content of the protection which legal instruments offer to citizens.

For example, Directive 95/46/EC announces protecting "*the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*"[13], whereas the GDPR disconnects privacy and personal data by outlining that the "*Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*"[14].

This being said, and despite this obscurity, all these rights appear closely linked. The right to the protection of personal data is a fundamental right[15] protected independently by Article 8 of the European Charter of Fundamental Rights (EUCFR), but before the adoption of the EUCFR, this right was already protected under Article 8 of the European Convention on Human Rights (ECHR)[16], which lays down the right to private and family life.

Therefore, the right to private and family life protection does pre-exist to the right to personal data protection as a stand-alone right, and is often considered as including the latter right[17]. As a result, and for example, the notion of privacy impact assessment (PIA) has preceded the notion of data protection impact assessment (DPIA)[18], and the concepts of privacy by design and by default have

[13] Article 1, §1 of Directive 95/46/EC.
[14] Article 1, §2 of the GDPR.
[15] GDPR, Recital n° 1.
[16] In relation to other instruments that protect privacy and personal data see Estelle De Marco *in* Estelle De Marco *et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework, op. cit.*, Sections 4.1.1 and 4.2.1.
[17] See below our Section 2.2.2.1.
[18] The concept of PIA is known since the mid-1990s: see Paul De Hert, Dariusz Kloza, David Wright *et al.*, Recommendations for a privacy impact assessment framework for the European Union, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.5, available at http://www.piafproject.eu/Deliverables.html (last accessed on 24 January 2018); see also Estelle De Marco, *MANDOLA Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2 of 11 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 3.1 (last accessed on 24 January 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

preceded the concepts of data protection by design and by default[19]. Further, a large part of the doctrine considers that the right to private life enables the exercise of other fundamental rights, and therefore offers protection to these rights[20], one consequence being that traditional PIAs analyse not only the risks that projects pose to privacy but also the risk they create for other fundamental rights[21].

On the opposite, in the EUCFR wake, other authors consider that the right to personal data protection is or must be an independent right, which does not protect only the information that relates to private life but also information of non-private nature, and which enables in turn to safeguard other fundamental rights that are not always elements of or protected by the private sphere[22].

Everyone therefore agrees that the protection of private life and the protection of personal data both offer protection to other fundamental rights, and that, as a result, a limitation of the one or of the other of these rights may bring a limitation to another fundamental right. However, the debate on the interrelations between private life and personal data protection on the one hand, and on the nature of the fundamental rights that both private life and personal data protection do protect in addition, stay unresolved.

As a result, in order to deeply apprehend the rights that are being protected and the mechanism of their protection, which will enable in turn to appreciate the differences between Directive 95/46/EC and the GDPR as well as the impact of these differences, it appears important to analyse the notion of private life and of personal data, their relations to the other fundamental rights, the mechanism

[19] The privacy by design concept has been developed by Dr. Ann Cavoukian, former Information and Privacy Commissioner of Ontario, in the 1990s. See Ann Cavoukian, *Privacy by Design in Law, Policy and Practice, A White Paper for Regulators, Decision-makers and Policy-makers*, August 2011, https://gpsbydesign.org/resources-item/privacy-by-design-in-law-policy-and-practice-a-white-paper-for-regulators-decision-makers-and-policy-makers/ (last accessed on 24 January 2018), p. 3.

[20] See below our Section 2.2.1.2; see also Estelle De Marco *in* Estelle De Marco *et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework, op. cit.*, Section 4.2.2.

[21] See below our Section 3.7.3.5; Estelle De Marco, *MANDOLA Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes, op. cit.,* Section 3.1.1.

[22] See for instance the discussion *in* Paul De Hert, Dariusz Kloza, David Wright *et al., Recommendations for a privacy impact assessment framework for the European Union*, *op. cit.* p. 14.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

that is used to protect them at the level of fundamental instruments, and the way these findings have been transcribed into Directive 95/46/EC and the GDPR.

2.2 - The interrelations between the right to private life, the right to the protection of personal data and the other fundamental rights

The analysis of these interrelations implies to analyse in turn the notion of private life and its relations to other fundamental rights, the notion of personal data and its relations to other fundamental rights, and the nature and extent of the protection offered to both these rights by the ECHR and the EUCFR.

2.2.1 - The notion of private life and its relations with other freedoms

The analysis of the notion of private life enables to identify the relations between private life and other freedoms.

2.2.1.1 - The notion of private life

The right to privacy, or more exactly, in the continental European legal tradition, the right to respect for private and family life, receives several definitions[23], which has led Prof. Daniel J. Solove to consider privacy as being a "*concept in disarray*", a notion that "*suffers from an embarrassment of meanings*"[24]. This situation is due to the silence of legal instruments in relation to the content of privacy, which is in practice casuistically identified by courts.

However, four main doctrinal approaches of privacy can be identified, and a fifth one issued from them. The first approach consists of endeavouring to identify the boundaries of private life through

[23] In relation to this section and for further developments see Estelle De Marco *in* Estelle De Marco *et al., MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework, op. cit.*, Section 4.1.2.
[24] Daniel J. Solove, « A taxonomy of privacy », University of Pennsylvania Law Review, vol. 154, n° 3, Jan. 2006, http://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf (last accessed on 14 February 2018).See also Daniel J. Solove, *Understanding privacy*, Harvard University Press, 2008, esp. p.1 *et seq.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the identification of its elements of content. Two other approaches - which are not incompatible with the first one - do define privacy in relation to several sub-categories or "dimensions" that are considered as composing the notion. The fourth approach does not define anymore privacy positively in relation to its components, but negatively, in relation to third parties' rights. All these definitions enable to draw a fifth approach in which privacy is broadly defined as including all the information pieces and freedoms exercised by a given person, but in which the protected privacy is defined in relation to third parties' rights. This last approach seems to be the most relevant to the authors of the current study, since it does not contradict the other approaches while it takes into account the extent of the protection offered to privacy in practice.

These five approaches of privacy can be briefly[25] detailed as follows:

2.2.1.1.1 Definition of private life in relation to its elements of content, expressed as information pieces, activities and freedoms

The content of privacy has been extensively defined by some authors as the "*right to be left alone*"[26], which refers to "*the right of everyone to take decisions at his own discretion into his zone of private life*"[27], or to the right to an opportunity to shape one's own life, with minimal outside interference[28]. More

[25] An extensive presentation of these approaches can be found in Estelle De Marco *in* Estelle De Marco *et al., MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework, op. cit.*, Section 4.1.2. An overview of different conceptions of privacy, including its deny, can also be found in Judith DeCew, "Privacy", The Stanford Encyclopedia of Philosophy (Spring 2015 Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/spr2015/entries/privacy/ (last accessed on 14 February 2017)

[26] See for ex. Stéphane-Dimitri Chupin, *La protection de la vie personnelle délimitée par les frontières des sphères privées et publiques*, thesis, Université Paris I, 2002, p. 32; Samuel D. Warren and Louis D. Brandeis, "The right to privacy", Harvard Law Review, vol. IV, 15 Dec. 1890, n°5. For an history of privacy including comments on S. Warren and L. Brandeis conception of privacy, Ahti Saarenpää, "Perspectives on privacy", in Ahti Saarenpää, *Legal privacy*, LEFIS Series, 5, Prensas Universitarias de Zaragoza, p. 20 (http://puz.unizar.es/detalle/898/Legal+privacy-0.html), available at http://lefis.unizar.es/images/documents/outcomes/lefis_series/lefis_series_5/capitulo1.pdf (last accessed on 12 February 2018); François Rigaux, "Les paradoxes de la protection de la vie privée", *in La protection de la vie privée dans la société d'information*, under the direction of Pierre Tabatoni, tome 1, Cahier des sciences morales et politique, PUF, Oct. 2000, p. 37, quot. p. 41.

[27] According to the Supreme Court of the United States in a decision of 1965. Translated from French. Pierre Tabatoni, "Vie privée : une notion et des pratiques complexes", in *La protection de la vie privée dans la société d'information*, under the direction of Pierre Tabatoni, tome 1, Cahier des sciences morales et politique, PUF, Oct. 2000, p. 3, quotation p. 4.

[28] Formula from Prof. Stig Strömholm according to Advocate General Cabannes in conclusions sous CA Paris, 15 mai 1970, D. 1970, jurisp. p. 466, quot. p. 468. Prof. Stig Strömholm conception of privacy is also mentioned by Alexandre Maitrot de la Motte, "Le droit au respect de la vie privée", in *La protection de la vie privée dans la société d'information*, under the

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

restrictively, a large doctrine classify information pieces and freedoms that compose privacy (identified as such by courts) into virtual "circles" or spheres that surround a given natural person, each of these spheres being shared by more or less third parties. For example[29], can be identified a sphere of "personal life", which contains "*data related to identity, to racial origin, to physical or mental health, to one's character or morals*"[30], and which is and will be shared with some particular groups of third parties only, such as the family and close relatives, but will be prohibited to other persons (and therefore protected against these persons). On the same line but without precise classification, and providing perhaps a wider perspective, the ECtHR protects a series of information pieces and freedoms that go beyond purely private activities, such as the "*right to identity*[31] *and personal development*"[32]; the right, to a certain degree, "*to establish and develop relationships with other human beings*"[33]; the right to *"self-determination and personal autonomy*"[34]; "*the physical and psychological integrity of a person*"[35]; "*professional and business activities*"[36]; and correspondence[37], which includes notably letters[38],

dir. of Pierre Tabatoni, tome 3, 4 et 5, Cahier des sciences morales et politique, PUF, Jan. 2002, p. 271, and by Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 329.

[29] For other national examples, see for instance Estelle De Marco *et al.,* Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), project n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, available at https://www.epoolice.eu/EPOOLICE/servlet/document.listPublic, Section 3. (last accessed on 12 February 2018)

[30] François Terré, "La vie privée", *in La protection de la vie privée dans la société d'information*, under the dir. of Pierre Tabatoni, tomes 3, 4 et 5, Cahier des sciences morales et politique, PUF, 1re éd., janv. 2002, page 138.

[31] The ECtHR adds that article 8 of the convention protects "*aspects of an individual's physical and social identity"* in ECtHR, 1st Sect., 7 February 2002, *Mikulić v. Croatia*, application no. 53176/99, §53.

[32] ECtHR, 3rd Sect., 25 September 2001, *P.G. and J.H. v. the United Kingdom*, appl. n°. 44787/98, §56, referring to ECtHR, ch., 22 February 1994, *Burghartz v. Switzerland*, §24, Series A, n° 280 B, p. 28. See also ECtHR, 4th Sect., 29 April 2002, *Pretty v. The United Kingdom*, appl. n° 2346/02, §61, referring to the same judgment.

[33] See the judgments mentioned in the previous note and ECtHR, *Niemietz v. Germany*, *op. cit.*, §32; Relating to the non-exclusion of "*the right to establish and develop relationships with other human beings*" and of "*activities of a professional or business nature*", see also the judgment ECtHR, gr. ch., 16 February 2000, *Amann v. Switzerland*, appl. n° 27798/95, §65.

[34] Ivana Roagna, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe human rights handbooks, Council of Europe, 2012, p. 12, available at: www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf (last accessed on 12 February 2018); see also for instance the case ECtHR, *Pretty v. The United Kingdom*, *op. cit.,* §§ 61 and 67.

[35] Ivana Roagna, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, *op. cit.*, p. 22, referring to ECtHR, gr.ch., 16 December 2010, *A, B, and C v. Ireland*, application n° 25579/05; see also ECtHR, ch., 26 March 1985, *X and Y v. the Netherlands*, appl. n°8978/80, § 22.

[36] ECtHR, *Niemietz v. Germany*, *op. cit.*, §28 and 29; See Pierre Kayser, op cit, page 43 and 44 and footnote n° 158. Before the ECtHR has ruled on this subject, the Court of Justice of the European Union stated that the need for a protection of

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

telephone calls and conversations[39], pager messages[40], professional correspondence[41], correspondence intercepted in the course of business or from business premises[42], and electronic communications (including the right for an individual to control "*information derived from the monitoring of (his or her) personal Internet usage*"[43]). Information relating to correspondences is also protected, such as the latter's date or the number dialled[44]. Personal data are also protected[45] and the ECtHR considers especially that both the storing and the release by a public authority of information relating to an individual's private life amounts "*to an interference with his right to respect for private life*[46]", no matter how the stored information will be used[47] and particularly within the context of "*surveillance methods resulting in masses of data collected*"[48]. More generally, "*mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8*"[49].

2.2.1.1.2 Definition of private life in relation to the different categories or "dimensions" that compose this notion, defined according to the context of the private life exercise

Some legal authors break privacy into several categories, dimensions or types of privacy, which are

---

legal persons' private sphere of activities "*must be recognized as a general principle of Community law*": judgment of 21 September 1989, *Hoechst v. Commission*, joined cases 46/87 and 227/88, European Court Reports 1989, pp. 2859-2924.

[37] See for instance Commission, plen., 27 February 1995, *B.C. v. Switzerland*, Application n°21353/93; ECtHR, ch., 25 March 1983, *Silver and others v. the United Kingdom*, appl. n°5947/72, § 84.

[38] See for instance ECtHR, *Silver and others v. the United Kingdom*, *op. cit.* §84.

[39] See for instance ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, §41; ECtHR, ch., 16 December 1992, *Niemietz v. Germany*, appl. n°13710/88, §32.

[40] ECtHR, 2nd Sect., 22 October 2002, *Taylor-Sabori v. the United Kingdom*, appl. n°47114/99, §18.

[41] ECtHR, *Niemietz v. Germany*, *op. cit.*, §32.

[42] ECtHR, ch., 25 March 1998, *Kopp v. Switzerland*, appl. n°23224/94, §50; ECtHR, ch., 25 June 1997, *Halford v. the United Kingdom*, appl. n°20605/92, §§ 44-46.

[43] See ECtHR, 4th Sect., 3 April 2007, *Copland v. the United Kingdom*, appl. n° 62617/00, § 41; Ivana Roagna, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe human rights handbooks, Council of Europe, 2012, www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf, p.32 (URL last accessed on 12 February 2018).

[44] ECtHR, 3rd Sect., 25 September 2001, *P.G. and J.H. v. the United Kingdom*, appl. n°. 44787/98.

[45] ECtHR, gr. ch., 16 February 2000, *Amann v. Switzerland*, appl. n° 27798/95, §65.

[46] ECtHR, ch., 26 March 1987, *Leander v. Sweden*, appl. n°9248/81, §48; See also ECtHR, gr.ch., 4 May 2000, ECtHR, *Rotaru v. Romania*, appl. n°28341/95, §45 *et seq.*

[47] ECtHR, gr.ch., 16 February 2000, *Amann v. Switzerland, op. cit.* §69; See also (rel. to phone calls) ECtHR, ch., *Kopp v. Switzerland, op.cit.* §53.

[48] ECtHR, 4e sect., 12 janvier 2016, *Szabó and Vissy v. Hongrie*, appl. n°37138/14, §68.

[49] European Court of Human Rights, Factsheet, « Protection of personal data », Press Unit, April 2017, p. 1, available on the Council of Europe website: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf (last accessed on 12 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

not based on the precise identification of the information and freedoms that compose privacy, nor on the links that exist between the privacy owner and third parties that take part in this context. The research consortium of the PIAF project[50] highlights that for example, Dr. Roger Clarke "*considers four conventional yet overlapping categories: privacy of personal information, of a person, of personal behaviour, and of personal communications*"[51]. The research consortium of the PRESCIENT EU project "*identified seven types of privacy*" (namely *"of a person, of thought and feelings, of location and space, of data and image, of behaviour and action, of communications, and of association, including group privacy"*[52]). For their part Prof. Daniel J. Solove and Prof. Beate Rössler identified respectively six and three "*categories*" or "*dimensions*" of privacy[53]. Among other authors following this approach[54], Prof. Ahti Saarepää identifies "*at least (…) eleven main core areas*" of privacy (namely physical privacy, spatial privacy, social privacy, media privacy, anonymity, privacy in the processing of personal data, ownership of information, right to be assessed in the proper light, patient privacy, privacy in working life, and communicative privacy)[55].

2.2.1.1.3 Definition of privacy in relation to different dimensions corresponding to the actions that are required to preserve privacy

Beside the afore-mentioned conceptions of privacy, Prof. Pierre Kayser divides private life into two

[50] Paul De Hert, Dariusz Kloza, David Wright and all., Recommendations for a privacy impact assessment framework for the European Union, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.13, available at http://www.piafproject.eu/Deliverables.html (last accessed on 12 February 2018).

[51] *Ibid.*, p. 13, referring to Roger Clarke, *What's Privacy'?*, 2006, http://www.rogerclarke.com/DV/Privacy.html (last accessed on 12 February 2018).

[52] *Ibid*, p. 13, referring to Serge Gutwirth, Michael Friedewald, David Wright, Emilio Mordini *et al.*, Legal, social, economic and ethical conceptualisations of privacy and data protection, Deliverable D1 of the PRESCIENT project [Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment], p. 8, http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf (last accessed on 12 February 2018). See also Rachel Finn, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al., *European data protection: coming of age?*, Springer, Dordrecht, 2012, pp. 3-32.

[53] *Ibid.*, p. 13, referring to Daniel J. Solove, "Conceptualizing Privacy" *California Law Review*, Vol. 90, 2002, p. 1087 and to Beate Rössler, *The Value of Privacy*, Polity Press: Cambridge, 2005, p 86.

[54] See for example, in the context of ambiant intelligence, Antoinette Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", in *Studies in Ethics, Law and Technology*, Volume 2, Issue 1, 2008, Article 3, p. 25, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 (last accessed on 12 February 2018), who identifies five aspects of privacy (spatial, informational, emotional, relational and communicational privacy).

[55] Ahti Saarenpää, *Legal privacy*, Lefis series 5, PUZ/LEFIS, 2008, *op. cit.,* pp. 27 *et seq.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

privacy spheres or dimensions which can be referred to as the "*secrecy of private life*" and the "*freedom of private life*"[56].

- The secrecy of private life is the "*opaqueness for others of the personal and family life*". It notably includes the secrecy of communications, the secrecy of relationships built up with third parties, the right to be forgotten, and the secrecy of one person's image and voice[57].

- The freedom of private life is defined as "*the power, for a person, to take the decisions that seem to her the bests for this part of her life*"[58], as a "*general freedom which includes several particular freedoms*", which may be described as physical (as the physical freedom, the freedom of movement) or as moral (as the freedom of belief)[59]. It notably includes the release from the home "*to develop one's physical, intellectual, moral and spiritual personality*"[60], the freedom of movement on the Internet, the freedom to make decisions, to make choices, notably regarding purchased goods and services[61], to communicate these choices to third parties, to open the doors of one's own private life to certain persons and to close these doors to other people[62]. The freedom and the secrecy of private life are interrelated, since the exercise of the freedom of private life creates a privacy content that is covered by the secrecy, and since the secrecy might be a condition to the proper exercise of some privacy freedoms[63].

---

[56] Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 12. On the secrecy of privacy, see also M. Rudinsky, Civil Human Rights in Russia: Modern Problems of Theory and Practice, Transaction Publishers, 2008, IBSN 978-0-7658-0391-7.

[57] See Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n°s 41, 107, 109, 114, 122, 135, 137, 147, 162, 171-172, 332.

[58] Translated from French. Pierre Kayser, *La protection de la vie privée par le droit*, *op. cit.* p. 11; see also Estelle De Marco, *L'anonymat sur Internet et le droit*, *op cit* p.99 *et seq*.

[59] Pierre Kayser, *op. cit.*, p. 344 and p. 12.

[60] Pierre Kayser, *op. cit.*, p. 12. See also Estelle De Marco, *L'anonymat sur Internet et le droit*, *op. cit.* n° 133 *et seq*.

[61] See the French Supreme Court decision: Cass. soc., 22 Jan. 1992, Bull. civ. V, n° 30.

[62] See for instance Emmanuel Dreyer, "Le respect de la vie privée, objet d'un droit fundamental", Com. com. élec., n° 5, May 2005, I, 18.

[63] See for ex. Virginie Peltier, Le secret des correspondances, PU d'Aix-Marseille, 1999, p. 99 : "*the tranquillity in which the action of correspondence takes place determines the* [existence of the] *freedom* [to correspond]" (translated from French: "*c'est la quiétude dans laquelle se déroule l'acte de correspondance qui détermine la liberté*"); see also Estelle De Marco, *L'anonymat sur Internet et le droit*, *op. cit.* n° 147-148.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2.2.1.1.4 Negative definition of privacy, in relation to third parties' rights

Several authors consider that privacy must be negatively defined, through the identification of its limits, which are the measures that allow pursuing public interests[64] in addition to the bounds that a person assigns to his or her own privacy sphere[65] or that are implied by the participation of this person in social and public life[66]. Under this approach, the notion of private life is not anymore considered as being a "*secret garden*", in a pure "*geographical conception*"[67], but as a personal zone that must be reconciled with the necessary interactions a person has with others[68] or as a sphere where the individual can do anything that is not prohibited by law[69], which also implies relations with third parties. The lack of third parties' rights[70] to interfere with the personal zone is therefore the criterion that will enable to identify if an element relating to the life of a given person will be considered as private or non-private, each third party being more or less legitimate to control this person's freedom

---

[64] On this issue see for example Amitai Etzioni, *The limits of privacy*, Basic Groups, 1999, notably p. 4.

[65] Unless prohibited by law, the right to privacy includes the right to choose to not benefit from this protection. In this sense see for ex. Ruth E. Gavinson, "Privacy and the limits of law", The Yale Law Journal, Vol. 89, n° 3 (Jan. 1980), pp. 421-471, http://www.jstor.org/stable/795891 or http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957 (last accessed on 24 February 2018), p. 428: the author refers to Edward Shils who argues that any privacy limitation which is controlled by the individual does not constitute a loss of privacy : "*Privacy exists where the persons whose actions engender or become the objects of information retain possession of that information, and any flow outward of that in-formation from the persons to whom it refers (and who share it where more than one person is involved) occurs on the initiative of its possessors*". A similar theory is developed by Adam D Moore, *Privacy Rights: Moral and Legal Foundations*, Pennsylvania State University press, 2010: "*Privacy may be understood as the right to control access to and use of physical items, like bodies and houses, and information, like medical and financial facts*" (p. 5); see also Charles Fried, "*who understands privacy as control over information*" according to Daniel J. Solove, *Understanding privacy*, Harvard University Press, 2008, quotation p. 35.

[66] Mats G. Hansson, *The Private Sphere: An Emotional Territory and Its Agent*, Springer, 2008, p. 3.

[67] Emmanuel Dreyer, "Le respect de la vie privée, objet d'un droit fondamental", Com. com. élec., n° 5, May 2005, I, 18.

[68] See for example Ruth E. Gavinson, "Privacy and the limits of law", The Yale Law Journal, Vol. 89, n° 3 (Jan. 1980), pp. 421-471, http://www.jstor.org/stable/795891 or http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957 (URLs last accessed on 12 May 2017); Mats G. Hansson, *The Private Sphere: An Emotional Territory and Its Agent*", Springer, 2007, pp. 2 *et seq*.

[69] See for instance Emmanuel Dreyer, *op. cit.*

[70] See for instance Florence Deboissy, "La divulgation d'une information patrimoniale", D. *2000, chron. p. 26: "The right to respect for private life is completely directed against others. Its object must therefore be defined in relation to third parties"* (translated from French); José Duclos, *L'opposabilité - Essai d'une théorie générale*, Thesis, LGDJ, 1984, n° 177. See also Ruth E Gavinson, "Privacy and the limits of law", *op. cit.*: "*Our interest in privacy, I argue, is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention*" (p. 423); "*The desire not to preempt our inquiry about the value of privacy by adopting a value-laden concept at the outset is sufficient to justify viewing privacy as a situation of an individual vis-a-vis others, or as a condition of life*" (p. 425).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

to act or this person's personal information[71].

This definition of privacy is highly interesting since it tends to consider that the protection of personal life against disclosure and interference of third parties will depend on the legitimacy of these third parties to access information or to prevent the exercise by someone else of one of his or her freedom, which drives to apply a very clear methodology that enables to find out, in each individual case, what relates to private life and what is excluded from this sphere. Indeed, this methodology is well-known and is proposed in the ECHR and the EUCFR[72]. However, this conception suffers from a difficulty: it tends to consider that non-protected elements of private life are not elements of private life, which might be an issue since the application of the ECHR and EUCFR principles imply the private zone as field of inquiry. It might also appear as being contradictory to identify one given element of life as private toward one given third party and as non-private toward another third party... since such a statement leads to admit that absolutely no element of life is private in nature (most intimate information being susceptible to be legitimately known by a spouse, a partner or a medical practitioner).

These conclusions might lead to keep considering the principle of a definition in relation to third parties' rights, but to apply this principle to the protected privacy sphere and not to privacy as a whole.

2.2.1.1.5 Definition of privacy as the whole sphere of information and freedoms that surround an individual, the protected privacy being defined in relation to third parties' rights

To conclude all the preceding analyses, the most relevant definition of privacy appears to be a

[71] On the legitimacy criterion, see for instance Florence Deboissy, "La divulgation d'une information patrimoniale"*, D. 2000, chron. p. 267: "The debate is (…) about the legitimacy of the control of the information, which special characteristic is to be personal, that is to say representative of a personality. Moreover, such a conception of private life allows forestalling the classical criticism of the theory of rights in the personality, that is to say the confusion between object and subject of law. Indeed, each individual has a prerogative not on himself but on an object that is outside of himself, the information"* (translated from French). On the coexistence of freedoms and personal data in the content of private life, see for instance Ahti Saarenpää, "Perspectives on privacy", available at http://lefis.unizar.es/images/documents/outcomes/lefis_series/lefis_series_5/capitulo1.pdf p. 21: "*when privacy is mentioned, we have to determine in each case whether we are talking about privacy as it relates to information and the processing of data or privacy more broadly in the sense of an individual's right to be left alone*" (last accessed on 12 February 2018).
[72] See below our Section 2.3.2.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

definition of privacy that consists in the whole sphere of information and freedoms that surround an individual, the protected privacy being defined in relation to third parties' rights.

Under this conception, the notion of private life is still considered as being a personal zone that must be reconciled with the necessary interactions a person has with others[73], including measures that allow pursuing public interests[74] or the defence of third parties rights[75], in addition to the bounds that a person assigns to his or her own privacy sphere[76] or that are implied by the participation of this person in social and public life[77].

The difference with the previous conception of privacy is that, under the current one, the content of private life covers all the information pieces and all the freedoms that concern a person, while third parties' rights will enable to define the boundaries of the protected privacy zone, and not anymore the privacy sphere as a whole. Under this approach, all what relates to an individual will be private in nature, but private elements of life will only be protected by legal instruments, casuistically, depending on third parties' rights[78], third parties who may be more or less legitimate to control

[73] See for example Ruth E. Gavinson, "Privacy and the limits of law", *op. cit.,* pp. 2 *et seq*.
[74] On this issue see for example Amitai Etzioni, *The limits of privacy*, Basic Groups, 1999, notably p. 4.
[75] The defence of several public interests and third parties' rights are generally the objectives that enable the limitation of conditional rights according to the ECHR.
[76] Unless prohibited by law, the right to privacy includes the right to choose to not benefit from this protection. In this sense see for ex. Ruth E. Gavinson, "Privacy and the limits of law", op. cit.,p. 428. In relation to the fact that the person' expectations of privacy might be decisive in order to identify if an element of private life will or not be protected from certain kinds of interferences, see ECtHR, 3rd Sect., 25 September 2001, *PG and J.H. v. The United Kingdom*, appl. n° 44787/98, §57: "*There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor*".
[77] Mats G. Hansson, *The Private Sphere: An Emotional Territory and Its Agent*, Springer, 2008, p. 3.
[78] See for instance Florence Deboissy, "La divulgation d'une information patrimoniale", D. *2000, chron. p. 26: "The right to respect for private life is completely directed against others. Its object must therefore be defined in relation to third parties"* (translated from French); José Duclos, *L'opposabilité - Essai d'une théorie générale*, Thesis, LGDJ, 1984, n° 177. See also Ruth E Gavinson, "Privacy and the limits of law", *op. cit.*: "*Our interest in privacy, I argue, is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention*" (p. 423); "*The desire not to preempt our inquiry about the value of privacy by adopting a value-laden concept at the outset is sufficient to justify viewing privacy as a situation of an individual vis-a-vis others, or as a condition of life*" (p. 425).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

another person's freedom to act or another person's personal information[79].

This approach of privacy seems at first glance very extensive, but after appropriate consideration it seems to be the more accurate one, since it does not contradict the other approaches[80], while it enables to give a practical content to privacy as it is protected by legal instruments, the ECtHR itself considering that, for example, "*there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life*"[81], underlining the concordance between "*such broad interpretation and the one of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 2011*"[82]. Indeed, this approach includes all the distinctions already analysed through the different definitions of privacy, including the "*right to be left alone*"[83], while it drives to apply the very clear ECHR and EUCFR methodology that enables to find out, in each individual case, what relates to protected private life and what is excluded from this sphere. This methodology consists schematically of analysing if one given third party' intrusion into private life has a legal basis, pursues a legitimate aim, and is necessary and proportionate to the aim pursued, which might also lead to analyse if the protection of privacy is not itself illegitimate,

[79] On the legitimacy criterion, see for instance Florence Deboissy, "La divulgation d'une information patrimoniale", *D. 2000, chron. p. 267: "The debate is (…) about the legitimacy of the control of the information, which special characteristic is to be personal, that is to say representative of a personality. Moreover, such a conception of private life allows forestalling the classical criticism of the theory of rights in the personality, that is to say the confusion between object and subject of law. Indeed, each individual has a prerogative not on himself but on an object that is outside of himself, the information"* (translated from French). On the coexistence of freedoms and personal data in the content of private life, see for instance Ahti Saarenpää, "Perspectives on privacy", available at http://lefis.unizar.es/images/documents/outcomes/lefis_series/lefis_series_5/capitulo1.pdf p. 21: "*when privacy is mentioned, we have to determine in each case whether we are talking about privacy as it relates to information and the processing of data or privacy more broadly in the sense of an individual's right to be left alone*" (last accessed on 12 February 2018).

[80] Prof. Pierre Kayser itself (who defines privacy according the first and the third approaches proposed above) shows that the apparent indecision of the French court of cassation in relation with the content of private life is due to the fact that the court does not characterise the privacy limitation according to the private nature of the concerned element of life, but does characterise it according to the severity of the limitation, and, in other words, according to the legitimacy of the limitation brought to the personal sphere of an individual by a third party: Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 350.

[81] ECtHR, *Rotaru v. Romania*, appl. n°28341/95, §43.

[82] Translated from French, ECtHR, 3rd Sect., *Haralambie v. Romania*, 27 October 2009 (final: 27/01/2010), appl. n°21737/03, §77.

[83] Samuel D. Warren and Louis D. Brandeis, "The right to privacy", Harvard Law Review, vol. IV, 15 Dec. 1890, n°5. See our first definition of privacy at the beginning of Section 2.2.1 above.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

unnecessary and non-proportionate, where its exercise limits another fundamental right[84].

In other words, under this approach, the notion of privacy is understood extensively within the boundaries set up by the ECHR and the EUCFR in order to balance conflicts of fundamental rights, which also means that the definition of the protected privacy is definitely contextual, and depends on the concerned individuals and stakeholders, in addition to the morals of a time[85] and to the value and the legitimacy of the other rights at stake[86].

2.2.1.2 - The interrelations between the right to private life and other fundamental rights and freedoms

During the preceding analyses, we have noticed that all the definitions of private life include the exercise of several rights and freedoms.

Some of these rights appear to belong in nature to the private sphere, such as the right to identity, the right to image and voice, the right to correspond and of personal communications, the right to establish and develop private relationships, and the right of everyone to take decisions at his or her own discretion into his or her zone of private life.

However, some of these rights appear to be or to belong to other stand-alone fundamental rights, such as the physical and psychological integrity of a person (right to the integrity of the person[87] and

[84] See below the Section 2.3 of the current report.
[85] Without explicit authorisation (from law or the concerned person) to interfere with the sphere of privacy of another person, third parties legitimacy will depend on what belongs to their own sphere of "freedom", subject to (generally civil) liability in case of fault or abuse of right. The latter are generally assessed in the light of what it is common to do or to not do in certain circumstances and of what it is admitted in terms of being at a certain place at a certain moment, or of behaving in a certain manner in certain circumstances, or even of what should or not contribute to a debate of public interest. On this discussion see Estelle De Marco *in* Estelle De Marco *et al.*, MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 4.1.2.5.2.
[86] Indeed, the necessity and the proportionality tests take account of the importance of the opposed right or value. See below our Section 2.3.2.
[87] See *inter alia* EUCFR, Article 3.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

prohibition of inhuman or degrading ill-treatment[88]), physical freedom (right to liberty and security[89]), professional and business activities (right to conduct a business[90]), the right to thought and feelings and the freedom of belief (freedom of thought, conscience and religion[91]), the right of location and space (freedom of movement[92]), the right to association (freedom of assembly and association[93]), the right to self-determination and personal autonomy (right to self-determination[94]), the right to be assessed in the proper light (right to a fair trial[95]); the right to personal behaviour, to personal action and to shape one's own life with minimal outside interference (freedom of the arts and science[96], freedom of expression[97], right to education[98], other cultural rights[99], freedom to choose an occupation[100], right to property[101]...).

In addition, some of the rights protected or considered as being protected by the right to private life can further be identified as belonging to the principle of freedom in a society governed by the rule of

---

[88] See *inter alia* ECHR, Article 3; EUCFR, Article 4; see Aisling Reidy, *The prohibition of torture, A guide to the implementation of Article 3 of the European Convention on Human Rights*, Human rights handbooks, No. 6, Council of Europe 2002, https://rm.coe.int/168007ff4c, p. 16 (last accessed on 26 January 2018).
[89] See *inter alia* ECHR, Article 5 ; Article 1 of the Protocol n°4 to the ECHR; EUCFR, Article 6.
[90] EUCFR, Article 16; in relation to the protection of this right under other legal instruments including the ECHR, see European Union Agency for Fundamental Rights, *Freedom to conduct a business: exploring the dimensions of a fundamental right*, 2015, p. 10, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-freedom-conduct-business_en.pdf (last accessed on 25 January 2018).
[91] See *inter alia* ECHR, Article 9; EUCFR, Article 10.
[92] See *inter alia* Article 2 of the Protocol n°4 to the ECHR; EUCFR, Article 45.
[93] See *inter alia* ECHR, Article 11; EUCFR, Article 12.
[94] Article I of the Charter of the United Nations; in relation to the recognition of this right at the EU and Council of Europe level, see Nicolas Levrat, *The Right to National self-determination within the EU: a legal investigation*, https://ecpr.eu/Filestore/PaperProposal/d0d39dde-15ad-4462-994a-a9e4a2fa24a6.pdf (last accessed on 25 January 2018).
[95] See *inter alia* ECHR, Article 6; EUCFR, Article 47.
[96] See *inter alia* EUCFR, Article 13; ECHR, Article 10; *Cultural rights in the case-law of the European Court of Human Rights*, January 2011 (updated 17 January 2017), Council of Europe, Research division, http://www.echr.coe.int/Documents/Research_report_cultural_rights_ENG.pdf, pp. 5 *et seq.* (last accessed on 25 January 2018).
[97] See *inter alia* ECHR, Article 10; EUCFR, Article 11.
[98] See *inter alia* Article 2 of Protocol No. 1 to the ECHR; EUCFR, Article 14.
[99] *Cultural rights in the case-law of the European Court of Human Rights*, *op. cit.*
[100] See *inter alia* EUCFR, Article 15; see also *Work-related rights*, Factsheet, January 2018, ECtHR, Press Unit, http://www.echr.coe.int/Documents/FS_Work_ENG.pdf (last accessed on 25 January 2018).
[101] See *inter alia* See *inter alia* Article 1 of Protocol No. 1 to the ECHR; EUCFR, Article 17.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Law[102], which enables to do everything that is not prohibited[103], subject to (generally civil) liability in case of fault[104] or abuse of right[105]. For example, appears to belong to this category the right to personal (physical, intellectual, moral and spiritual) development (beyond the right to education) including the right to establish and develop relationships with other human beings, and the right to an opportunity to shape one's own life and to make decisions with minimal outside interference (outside the rights evoked in the previous paragraph).

To conclude, the right to private life seems to offer protection to the rights to the freedom and to the secrecy of all that relates to the behaviour of the concerned person in his or her private sphere, in addition to provide refuge for the exercise of a series of other fundamental rights where a full enjoyment of these rights implies either a secret exercise (actual or future - which might lead to the right to be forgotten), or an exercise that is particularly protected from external influences or

---

[102] The preservation and promotion of fundamental rights is considered as "*an ideal*" for democracy, which is itself considered to be "*the best way of achieving these objectives*", being also "*the only political system that has the capacity for self-correction*" ("Universal declaration on democracy" adopted without a vote by the Inter-Parliament Union Council at its 161st session, http://www.ipu.org/cnl-e/161-dem.htm, Article 3, last accessed on 26 January 2018). However the preservation of fundamental rights is not inherent to democracy (see for ex. Larry Diamond, "Defining and Developing Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, *The democracy sourcebook*, Massachusetts Institute of Technology, 2003, p.30), but is a choice of what Larry Diamond calls "liberal democracies" (Larry Diamond, *op. cit.* p. 29). On this discussion see Estelle De Marco *in* Cormac Callanan, Marco Gercke, Estelle De Marco and Hein Dries-Ziekenheiner, *Internet blocking - balancing cybercrime responses in democratic societies*, October 2009, available at http://www.aconite.com/blocking/study, French version available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/, last accessed on 26 January 2018.

[103] This principle is part of the definition of freedom and is proclaimed by the Constitutions of several countries including France (Art. 4 of the Human and Citizen Rights Declaration of 1789: "*Liberty consists in being able to do anything that does not harm others: thus, the exercise of the natural rights of every man has no bounds other than those that ensure to the other members of society the enjoyment of these same rights. These bounds may be determined only by Law*" - official English translation at translation at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/english/constitution/declaration-of-human-and-civic-rights-of-26-august-1789.105305.html, last accessed on 24 February 2018). In the criminal area, it is included in the principle "*nulla poena sine lege*" protected by Art. 7 of the ECHR (see Section 4.4.2 of the current study).

[104] Legal actions, in case of fundamental right violation, are generally based on general rules organising civil liability. See Section 4.3.3.2 of the MANDOLA *Deliverable D2.2 - Identification and analysis of the legal and ethical framework*, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, and the *MANDOLA deliverable D2.1 - Definition of illegal hatred and implications*, MANDOLA project, available at the same address, especially the Annex.

[105] Article 17 of the ECHR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

interferences[106]. This is perfectly illustrated by the doctrine which highlights that judges and courts refrain from giving too restrictive boundaries to privacy, in order to make it possible, in a casuistic manner, to provide refuge for certain secrets or certain individual freedoms[107] in this protected private zone[108].

Regarding the fundamental rights that are affected by the right to the protection of private life (therefore the rights that enter in conflict with the right to private life), they might be exactly the same as those that are protected by the privacy sphere, and even more numerous. Indeed, for example, the freedom of expression and the right to information, as well as the freedom to conduct a business or a given inquiry on a crime, might legitimately require the release or the use of information relating to the private life of another individual. The right to the protection of the private life of a given individual might also itself require that another person is prevented from attending certain places in order to not disturb his or her quietness[109]. The balance to be made between the right to the protection of private life and these other rights is proposed by the mechanism for privacy protection itself (under the ECHR and the EUCFR), which requires - as already analysed - that any privacy limitation has a legal basis, pursues a legitimate aim, and is necessary and proportionate to the aim pursued. These tests take into account the precise context of the exercise of privacy and the value and the legitimacy of the other right at stake[110].

---

106 Without prejudice to the question of whether the way the right is exercised, or the purposes and impacts of such exercise, are legitimate - which might have to be assessed independently, possibly on another legal basis such as the right to freedom and expression and its limits.

107 See Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995 p. 12, quoting Marie-Thérèse Meulders-Klein, "Vie privée, vie familiale et droits de l'homme", Rev. intern. dr. comp., 1992, p. 771: "*It is an essential qualitative leap to get from the secret and intimacy protection to the idea that the secret is only the means of protecting individual freedom (…), which is in turn only the means of ensuring the personal achievement of each individual*". See also Alan Westin, *Privacy and Freedom*, Athenum, 1967.

108 See for instance Advocate General Cabannes, conclusions sous (ie opinion under the Paris Court of Appeal decision) CA Paris, 15 mai 1970, D. 1970, jurisp. p. 466, quotation p. 468: According to the author, French judges appropriately refrain from "*formulating a general definition in an area whose limits are undecided. In each individual case, they simply give an outline that enables giving to private life an assessment that is wide enough to protect the right to live in peace at home*" (translated from French).

109 Which will for ex. be the purpose of a no-contact order.

110 See below our Section 2.3.2.4.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2.2.2 - The notion of personal data and its relations with other freedoms

The analysis of the notion of personal data and its links with privacy enables to identify the relations between the protection of personal data and the protection of other freedoms.

2.2.2.1 - The notion of personal data and its relations with privacy

In order to define personal data, the ECtHR refers *inter alia* to the Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data ("the Data Protection Convention"), which considers a personal data as being "*any information relating to an identified or identifiable individual ("data subject")*"[111]. This definition has the same meaning that the definition offered by the GDPR, in which a personal data is "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*"[112]. In substance, a personal data (also referred to as "personal information" in this report) is therefore any information that might enable to identify a single natural person, even indirectly, a person being indirectly identifiable when one or several pieces of information held by one or several third parties could, in association with the known or processed data, lead to the identification of this person, even if the data possessor or controller does not have the necessary resources or power to make such identification.

However, the ECtHR remains silent on the question of whether all personal data are private information, and assesses casuistically the existence of an interference with the applicants' right to respect for their private lives in relation to the alleged personal data use[113], recalling however that "*the concept of "private life" is a broad term*"[114]. This might be interpreted as a willing to not give a definition of

111 ECtHR, gr. ch., 4 December 2008, *S and Marper v. The United Kingdom*, appl. n° 30562/04 and 30566/04, § 41. See also ECtHR, *Rotaru v. Romania*, appl. n°28341/95, §43.
112 GDPR, Article 4.
113 See for ex. ECtHR, *S and Marper v. The United Kingdom, op. cit.,* § 69.
114 See for ex. ECtHR, *S and Marper v. The United Kingdom, op. cit.,* § 66.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

privacy that could hurt some of the more restrictive conceptions of the notion, since the definition of the boundaries of private life partly falls traditionally within the sovereign sphere of the Council of Europe Member States[115].

This being said, the ECtHR considers globally that "*the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention*"[116], and it does not seem that the ECtHR has already qualified a personal data as lying outside - or at least as not impacting, where processed - the sphere of private life. As a result, the CJEU considers, by reference of ECHR court cases, that "*it must be considered that the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual*"[117], and that, consequently, "*the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the* [ECtHR]"[118]. In the same line, the *Handbook on European Data Protection Law* edited by the European Union Agency for Fundamental Rights and the Council of Europe[119] states as a general principle that "*the right to protection of personal data forms part of the rights protected under Article 8 of the ECHR which guarantees the right to respect for private and family life, home and correspondence and lays down the conditions under which restrictions of this right are permitted*"[120].

In this sense, we can note that the notion of personal data is perfectly included in the definition of private life considered as the whole sphere of information and freedoms that surround an individual, whose protection is defined in relation to third parties' rights[121]. Indeed, in the latter definition, are

---

115 See for example Véronique Huet, *L'autonomie constitutionnelle de l'État : déclin ou renouveau ?*, Revue de Droit Constitutionnel 2008/1 (n° 73), pp. 65-87, also available at https://www.cairn.info/revue-francaise-de-droit-constitutionnel-2008-1-page-65.htm (last accessed on 26 January 2018).
116 ECtHR, gr. ch., 4 December 2008, *S and Marper v. The United Kingdom*, appl. n° 30562/04 and 30566/04, § 103.
117 CJEU, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, joint cases C-92/09 and C-93/09, §52.
118 Ibid.
119 Handbook on European data protection law, European Union Agency for Fundamental rights and Council of Europe, 2014, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (last accessed on 26 January 2018).
120 *Ibid.*, p. 15.
121 See above the Section 2.2.1.1.5 of the current report. In relation to the legal authors who support this approach see for ex. Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p.42; Ahti

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

covered all the data that surround an individual who might be identified as being their subject, these data being protected against any interference of third parties that would not be legitimate, necessary and proportionate in the sense given to these terms by the ECHR and the ECtHR, along with the freedoms exercised based on the secrecy or on the control of these data[122].

On the opposite, a comparison between more restrictive definitions of privacy and the notion of personal data enables to draw two spheres that overlap without being exactly the same, since personal data that are not considered to be related to private life, such as elements of the public life of an individual, will not be protected under this legal basis[123]. This approach, which is perfectly understandable, appears however to be questionable in the light of the ECtHR court cases, since the Court protects also the "social life" of public figures under Article 8 of the ECHR, unless the context of the interference appears to be necessary in order to protect a contradictory interest (such as the right to information of the general public) and to be proportionate to this aim[124]. This argues once again in favour of a very large conception of privacy, combined with a conception of the privacy protected zone that depends on third parties' legitimacy to interfere with its content.

Saarenpää, "Perspectives on privacy", in Ahti Saarenpää, *Legal privacy*, LEFIS Series, 5, Prensas Universitarias de Zaragoza, p. 21 (http://puz.unizar.es/detalle/898/Legal+privacy-0.html), accessible at http://lefis.unizar.es/images/documents/outcomes/lefis_series/lefis_series_5/capitulo1.pdf (last accessed on 12 February 2017): "*Thus, when privacy is mentioned, we have to determine in each case whether we are talking about privacy as it relates to information and the processing of data or privacy more broadly in the sense of an individual's right to be left alone*". P. 23, this author also notices that "*In the United States, Canada, Australia and New Zealand, for example, legislation enacted under the heading 'privacy' deals primarily with the processing of personal data*". See also F. M. Rudinsky, *Civil Hulan Rights in Russia - Modern Problems of Theory And* Practice, Transaction Publishers, 2008, p. 40: "*The constitutional term "secret" expresses inadmissibility of illegal and unreasonable penetration into the sphere of individual freedom with a view of illegal acquirement of personal information of a citizen against their will*".

[122] At least as far as it relates to the action that consist of exercising a freedom at stake; the protection or the balance of the other aspects of that freedom - such as the content and extent of this exercise - with third parties' rights might be based on another legal basis such as the right to freedom of expression or the freedom of assembly.

[123] See for instance Paul De Hert Dariusz Kloza, David Wright and all., *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.14, available at http://www.piafproject.eu/Deliverables.html (last accessed on 12 February 2017).

[124] See for ex. ECtHR, *Mosley v. the United Kingdom*, appl. n° 48009/08, 10 May 2011, §§ 129-130; *Handbook on European data protection law*, European Union Agency for Fundamental rights and Council of Europe, 2014, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, p. 22 *et seq.* (last accessed on 26 January 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2.2.2.2 - The interrelations between the right to protection of personal data and other freedoms

If we consider privacy as being broadly defined while its protection is determined in relation to third parties' rights, personal data are a sphere of private life, as we have analysed it. The protection of personal data therefore benefits to all information pieces and freedoms that are lying or are exercised in the private sphere and that may be illegitimately affected by a third-party access to an information piece relating to the privacy owner. In line with the analysis in Section 2.2.1.2, these rights and freedoms are numerous and include (non-exhaustively) the right to image and voice, the right to correspond and of personal communications, the right to establish and develop private relationships and more generally relationships with other human beings, the right of everyone to take decisions at his or her own discretion into his or her zone of private life, the right to the integrity of the person and the prohibition of degrading ill-treatment, the right to liberty and security, the right to conduct a business, the freedom of thought, conscience and religion, the freedom of movement, the freedom of assembly and association, the right to self-determination and personal autonomy, the right to be assessed in the proper light and the right to a fair trial, and the right to personal action and to shape one's own life with minimal outside interference which is protected through different stand-alone rights (such as the freedom of the arts and science, the freedom of expression, the right to education and other cultural rights, the freedom to choose an occupation and the right to property) or through the protection of the general principle of freedom.

In a more restrictive conception of privacy, only a part of the secrets and freedoms identified as being protected by the privacy wall in our first paragraph above will benefit from a personal data protection, but will come in addition to a protection relating to all the other freedoms that might be affected by the access to or the use of a personal information that would not be considered as being a private one, based on the right to the protection of personal data, which offers an equivalent protection that the one offered to privacy under the ECHR and the EUCFR[125]. As a result, since this

[125] See below our Section 2.3.2.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

second group of personal data is also an integral part of the protection offered to privacy in its very extensive conception proposed above, the freedoms that are protected through the protection of personal data are exactly the same as those that we have identified to be protected under this broad conception of privacy, in our first paragraph, where the concerned freedoms are affected on the basis of the use, secrecy or control of a personal information.

And indeed, the use of a personal data, even of a non-intimate nature such as the information revealing the purchase of a good or the visit of a public place might have several impacts on other rights and freedoms recognised or not as stand-alone fundamental rights, particularly within the framework of the use of new technologies. For example, the information that a given person has purchased a boycotted good might lead to discrimination by the neighbourhood; the information that a person has visited a public place might lead to a mistaken arrest in case, by coincidence, a crime took place at the same time. A last example is the collection of several personal data in order to profile an identifiable individual. This might lead to create new information or to "*produce knowledge*"[126] about this individual, information which might be false and in any case which is beyond the control of the respective person. This action is therefore susceptible to impact several fundamental rights such as the right to non-discrimination and the right to due process[127], as well as the freedom of choice, the freedom of assembly and the freedom of expression in case this profile would be used in order to prevent the concerned person to use a particular service of the information society.

Regarding the fundamental rights that are affected by the right to the protection of personal data (therefore the rights that enter in conflict with the right to data protection), they might be exactly the same as those that are protected by the privacy and the data protection sphere, and even more numerous. Indeed, for example, the freedom of expression and the right to information, as well as the freedom to conduct a business or the inquiry on a crime, might legitimately require the release of

[126] Antoinette Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", *op. cit.*, p. 13 of the electronic version.
[127] Mireille Hildebrandt, and Bert-Jaap Koops, "The challenges of Ambient Law and legal protection in the profiling era", May 2010, Modern Law Review 73 (3), p. 428-460.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the personal information relating to a third party. The right to the protection of private life of an individual might also itself require that another person is prevented from attending certain places in order to not disturb its quietness, which will require memorising such prohibition and the events that led to decide it. The balance to be made between the right to the protection of personal data and these other rights follows the same rule used in the area of the protection of private life: this balance is proposed by the mechanism for privacy and personal data protection (respectively under the ECHR, and both the EUCFR and the EU data protection legislation, as we will see later) itself, which requires *inter alia* that any limitation to the right to the protection of personal data has a legal basis, pursues a legitimate aim, and is necessary and proportionate to the aim pursued. These tests take into account the precise context of the exercise of privacy and the value and the legitimacy of the other right at stake[128].

[128] Indeed, the necessity and the proportionality tests under the ECHR and the EUCFR, which are also applicable under the GDPR, take account of the importance of the opposed right or value. See below our Section 2.3.2.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Summary of Section 2.2

- The notion of privacy receives many definitions but the more relevant one[129] seems to be a definition of privacy that include the whole sphere of information and freedoms that surround an individual, the protected privacy being defined in relation to third parties' rights. Under this approach, the right to private life includes the rights to the freedom and to the secrecy of all that relates to the behaviour of the concerned person in his or her private sphere, in addition to provide refuge for the exercise of a series of other fundamental rights where a full enjoyment of these rights implies either a secret exercise (actual or future - which might lead to the right to be forgotten), or an exercise that is particularly protected from external influences or interferences[130]. The effective protection of these elements of life against disclosure and interference of third parties will depend on the legitimacy of these third parties to access information or to prevent the exercise by someone else of one of his or her freedom, which drives to apply the very clear ECHR and EUCFR methodology that enables to find out, in each individual case, what relates to the protected private life and what is excluded from this sphere (non-protected elements remaining private in nature). This methodology consists schematically of analysing if one given third party' intrusion into private life has a legal basis, pursues a legitimate aim, and is necessary and proportionate to the aim pursued. This also means that the definition of the protected private life is definitely contextual, and depends on the third parties who take part in the related context, in addition to the morals of a time[131] and to the value and

[129] Since it does not contradict the other approaches, while it enables to give a practical content to privacy as it is protected by legal instruments through the application of the ECHR and EUCFR fundamental rights protection mechanisms.

[130] Without prejudice to the question of whether the way the right is exercised, or the purposes and impacts of such exercise, are legitimate - which might have to be assessed independently, possibly on another legal basis such as the right to freedom and expression and its limits.

[131] Without explicit authorisation (from law or the concerned person) to interfere with the sphere of privacy of another person, third parties legitimacy will depend on what belongs to their own sphere of "freedom", subject to (generally civil) liability in case of fault or abuse of right. The latter are generally assessed in the light of what it is common to do or to not do in certain circumstances and of what it is admitted in terms of being at a certain place at a certain moment, or of behaving in a certain manner in certain circumstances, or even of what should or not contribute to a debate of public interest. On this discussion see Estelle De Marco *in* Estelle De Marco *et al.*, MANDOLA Deliverable D2.2 -

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the legitimacy of the other right at stake.

- The sphere of personal data might be considered as an integral part of the privacy sphere, under the latter definition of privacy, or as a sphere that overlap the privacy sphere without being exactly the same, in the light of more restrictive conceptions of privacy, where some personal data are not considered to be related to private life, such as elements of the public or social life[132].

- However, in both cases, by the rule of protection mechanisms, both the protection of private life and the protection of personal data also protect the same series of other rights and freedoms, which include (non-exhaustively) the right to image and voice, the right to correspond and of personal communications, the right to establish and develop private relationships and more generally relationships with other human beings, the right of everyone to take decisions at his or her own discretion into his or her zone of private life, the right to the integrity of the person and the prohibition of degrading ill-treatment, the right to liberty and security, the right to conduct a business, the freedom of thought, conscience and religion, the freedom of movement, the freedom of assembly and association, the right to self-determination and personal autonomy, the right to be assessed in the proper light and the right to a fair trial, and the right to personal action and to shape one's own life with minimal outside interference which is protected through different stand-alone rights (such as the freedom of the arts and science, the freedom of expression, the right to education and other cultural rights, the freedom to choose an occupation and the right to property) or through the protection of the general principle of freedom.

- The exercise of the right to private life and to personal data protection might on the opposite affect a series of fundamental rights that might be exactly the same as those that are protected

Identification and analysis of the legal and ethical framework, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 4.1.2.5.2.

[132] Such an approach appearing however questionable in the light of the ECtHR court cases.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

by the privacy sphere, and even more numerous. The balance to be made between the right to the protection of private life and/or the right to the protection of personal data on the one hand, and these other rights (which might include the right to private life as well) on the other hand, is proposed by the mechanism for privacy protection itself under the ECHR and the EUCFR, which requires - as already analysed - that any privacy limitation has a legal basis, pursues a legitimate aim, and is necessary and proportionate to the aim pursued. These tests take indeed into account the precise context of the exercise of privacy and the value and the legitimacy of the other right at stake[133].

2.3 - Nature and extent of the protection granted to private life and the personal data sphere

The philosophy that underlies Directive 95/46/EC and the GDPR cannot be precisely apprehended without shedding light on the content of the mechanism that is used at the ECHR and the EUCFR levels in order to protect the private and the personal data spheres, for reasons already exposed, which will be summarised beforehand.

2.3.1 - The interest of analysing the nature and extent of the protection granted to the private and the personal data spheres

We have analysed that the definition of protected privacy understood in relation to third parties' rights, as well as the extent of the protection of personal data, are directly dependent from the conditions in which the right to private life on the one hand and the right to the protection of personal data on the other hand can be limited, since these conditions enable to identify if a given third party is or is not legitimate to access information relating to the life of a natural person, or to

[133] See below our Section 2.3.2.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

interfere with the exercise of a right that is particularly protected by the secrecy of the personal life. The understanding of this mechanism of protection therefore enables to compare the protection granted to the private and to the personal data spheres by fundamental texts, with the protections granted by Directive 95/46/EC and the GDPR.

We have also suggested[134] that both Article 8 of the ECHR and Article 7 and 8 of the EUCFR - which do coexist today, their provisions being mandatory for EU Member States[135] - offer to privacy and to personal data an equal protection mechanism. Indeed, the rights laid down in the EUCFR have the same scope and meaning than the ECHR where they do not offer a stronger protection[136], and the details provided in addition in Article 8 of the EUCFR are already an integral part of the protection offered by the European Court of Human Rights (ECtHR)[137]. It is the reason why the CJEU explained *inter alia* in 2003 that "*the provisions of Directive 95/46, insofar as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must be interpreted in light of that right, which forms an integral part of the general principles of EU law*", referring to "*Article 8 ECHR*"[138]. It is also the reason why the opinions of the Article 29 Data Protection Working Party, which becomes

[134] See above, the Section 2.1 of the current report.
[135] All the EU Member States have ratified or accessed the ECHR, and the EUCFR has the same value as the treaties since the entry into force of the Treaty of Lisbon (Article 6 of the Treaty on European Union).
[136] EU Charter of Fundamental Rights, article 52, 3. For further reading, see especially French Cour de cassation, "Dossier : la charte des droits fondamentaux - historique et enjeux juridiques", in veille bimestrielle de droit européen, October 2010, n° 34, http://www.courdecassation.fr/publications_26/publications_observatoire_droit_europeen_2185/veilles_bimestrielles_droit_europeen_3556/2010_3865/octobre_2010_3810/droits_fondamentaux_18630.html (last accessed on 24 January 2018).
[137] On the fairness of the processing see *Handbook on European data protection law*, European Union Agency for Fundamental rights and Council of Europe, 2014, 3.4 p. 73, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, and the ECtHR court cases referred to in this Section (*Haralambie v. Romania*; 3rd Sect., appl. n°21737/03, 27/10/2009 (final: 27/01/2010; *K.H. and Others v. Slovakia*, 4th Sect., appl. n°32881/04, 28/04/2009 (final: 06/11/2009)*;* on the consent as a basis of the processing see for ex. *Perry v. RU*, 17 July 2003; Peck v. R.U, 29 January 2003; ; on the right to access see for ex. *Haralambie v. Romania*, *op. cit.*; on the right to rectification see for ex. ECtHR, Cemalettin Canli v. Turkey, No. 22427/04, 18 November 2008 and *Handbook on European data protection law*, *op. cit.*, Section 5 p. 103.
[138] CJEU, C-465/00 and C-138/01, *Rechnungshof v. Osterreichischer Rundfunk,* 20 May 2003, §§70-71; see Laraine Laudati, *Summaries of EU court decisions relating to data protection 2000-2015*, 28 January 2016, 10th European data protection day, n° 1.2 p. 5 and n°10 p. 58.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the European data protection board under the GDPR[139], apply extensively the ECHR privacy protection principles in order to interpret the data protection legislation[140].

As a result, it is important to note that, since the right to private life on the one hand and the right to the protection of personal data on the other hand enjoy the same protection mechanism (as well as other conditional rights[141], such as, for example, the right to the freedom of expression and the right to freedom of assembly), the theoretical discussion relating to the exact perimeter of privacy does not have any practical implication outside the identification of the other fundamental rights and freedoms that might be at stake and protected by these spheres, which is an information to be taken into account when comparing the differences of wording that may exist between Directive 95/46/EC and the GDPR.

We have finally analysed that the protection mechanism of both the right to private life and the right to the protection of personal data contains in itself the rule that enables to balance the other rights that might be opposed. Indeed, the conditions that must be respected in this regard, and primarily the conditions of necessity and proportionality, will enable to evaluate the extent of the interference and the legitimacy of the third party to cause such interference on the one hand, and the legitimacy of the data subject in relation to his or her expectation of confidentiality and non-intrusion on the other hand. In this sense, the rules for protecting personal data are also rules for limiting the protection of personal data in case this protection is opposed to the exercise of other rights and values such as the freedom of speech, the freedom of scientific research or the preservation of one

---

139 GDPR, Articles 68 *et seq*.

140 Opinions of the Article 29 Working Party can be found on http://ec.europa.eu/newsroom/article29/news.cfm?tpa_id=6936 (URL last accessed on 24 January 2018). See for example *Opinion 15/2011 on the definition of consent* of 13 July 2011 (WP187) updated in the *Guidelines on Consent under Regulation 2016/679* of 28 November 2017 (WP 259), and in the *Opinion 03/2013 on purpose limitation*, 2 Avril 2013 (WP203).

141 As already explained in our executive summary, some of the rights identified in the European Convention on Human rights are called "absolute", such as the right to life or to not be subjected to torture, while others are called "conditional" because they can be subjected to dispensations and/or limitations, as the right to respect for private life and the right to freedom of expression: Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", *in Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, pp.44-45).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

person's life. This observation will also be of importance during the analysis of balancing mechanisms proposed by both Directive 95/46/EC and the GDPR.

The need is therefore, at this stage of the analysis, to clarify the conditions under which a limitation of the right to privacy and to personal data is possible[142].

2.3.2 - The conditions for limiting the right to private life and the right to personal data protection

According to Article 8 para. 2 of the ECHR as interpreted by the ECtHR, and which are to be interpreted narrowly[143], the conditions for limiting the right to private life and/or the right to personal data protection are the following: any interference or limitation of these rights must have a specific, clear, accessible and foreseeable legal basis, must be in conformity with one of the legitimate aims listed in the Convention, must be necessary and must be proportionate (the two latter principles being contained in the formula "*necessary in a democratic society for the aforesaid aim*"[144], which implies according to the ECtHR that the interference, "*in a society that means to remain democratic*"[145], correspond to a "*pressing social need*"[146], and is "*proportionate to the legitimate aim pursued*"[147]).[148]

---

[142] Certain legal authors refer to these requirements as a "*general public order clause*": Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", *op.cit.*, pp. 44-45.

[143] See for instance ECtHR, ch., 25 February 1993, *Crémieux v. France*, appl. n° 11471/85, §38; Steven Greer, *The exceptions to Article 8 to 11 of the European Convention on Human Rights,* Human Rights files n°15, Council of Europe publishing, 1997, especially p. 8, http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf; Steven Greer, *The margin of appreciation: interpretation and discretion under the European Convention on Human Rights,* Human Rights files n°17, Council of Europe publishing, 2000, especially p. 20 (proportionality); p. 26 (public interest exceptions), http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf; Toby Mendel, A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights, Council of Europe, especially p. 3 (strict interpretation of the test for freedom of expression restrictions), https://rm.coe.int/16806f5bb3; Ivana Roagna, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe human rights handbooks, Council of Europe, 2012, especially p. 37 (strict interpretation of the test for private life restrictions), www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf (URLs last accessed on 21 February 2018).

[144] See for instance ECtHR, plen., 26 April 1979, *Sunday Times v. The United Kingdom*, appl. n° 6538/74, § 45, Series A, n° 30.

[145] Joint dissenting opinion of judges Wiarda, Cremona, Thór Vilhjálmsson, Ryssdal, Ganshof van der Meersch, Sir Gerald Fitzmaurice, Bindschedler-Robert, Liesch and Matscher, §8, available under the Sunday Times court case, *op cit.*

[146] ECtHR, *Sunday Times v. The United Kingdom, op cit*, § 59.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

As regards the definition of "interference" or "limitation", it is constituted as soon as a personal data is accessed or used (or a freedom protected by the wall of private life prevented to be exercised), "*no matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way*"[149], and no matter whether this data is publicly available or not[150].

2.3.2.1 - A specific, clear, accessible, stable and foreseeable legal basis

Any interference with the right to private life and the right to personal data must be lawful, that is to say it must be "*prescribed by law*" according to the ECtHR, expression that must be understood as pursuing the same aim as the expressions "*in accordance with the law*"[151], "*in accordance with law*", or "*provided for by law*", within the convention and its protocols[152]. Indeed, all these expressions, which are "*equally authentic but not exactly the same*", are translated by the French expression "*prévues par la loi*", and the ECtHR must "*interpret them in a way that reconciles them as far as possible and is most appropriate in order to realise the aim and achieve the object of the treaty*"[153].

These expressions mean firstly "*that any interference must have some basis in the law of the country concerned*"[154]. However, the notion of "Law" is understood by the ECtHR "*in its substantive sense, not its formal one*". In consequence, it does not only refer to legislative texts, but it also includes *"non-written law*", "*enactments of lower rank than statutes*", and case law. "*In a sphere covered by the written law, the "law"*" is

---

147 ECtHR, *Sunday Times v. The United Kingdom, op cit,* § 63. See also Frédéric Sudre, « La dimension internationale et européenne des libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, under the dir. of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, p. 43; Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 86.

148 The current Section 2.3.2 is largely issued from Estelle De Marco previous research, lastly presented in Estelle De Marco *et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework*, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 4.1.3

149 CJEU, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, *op. cit.*, §33.

150 See for instance Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, WP203, III.2.5, p.35.

151 This is the terminology used by the ECHR. The EUCFR mentions "*provided for by law*": Article 52.1.

152 See ECtHR, plen., 26 April 1979, *Sunday Times v. The United Kingdom*, appl. n° 6538/74, § 48.

153 See ECtHR, *Sunday Times v. The United Kingdom*, *op. cit.* § 48.

154 ECtHR, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), p. 19, referring to ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, §§66 *et seq.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

therefore "*the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments*"[155].

These expressions mean secondly that, *"over and above compliance with domestic law, it* [is required] [...] *that domestic law itself* [is] [...] *compatible with the rule of law*"[156]. The principle of legal basis "*thus implies that there must be a measure of legal protection in domestic law*", including "*against arbitrary interferences* [...] *with the right to private life*"[157].

In order to prevent such arbitrary interferences, the ECtHR developed three main requirements which all contribute to a fourth one which is the requirement of predictability: the law that organises the limitation of the right to privacy must be sufficiently clear and precise. It must be accessible, and it must be stable.

2.3.2.1.1. Clear and precise

Law must notably be "*formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail*"[158].

The requirement of clear and precise[159] legal basis is therefore a principle of transparency, which will enable citizens to be aware of the interferences they might suffer in relation to the exercise of their

---

155 All quotations are coming from ECtHR, ch., 24 April 1990, *Kruslin v. France*, appl. nº11801/85, §29. On this issue see also Frédéric Sudre, op cit, page 43; R. Koering-Joulin, D. 90, chron. p. 187. See Estelle De Marco *in* Cormac Callanan, Marco Gercke, Estelle De Marco and Hein Dries-Ziekenheiner, *Internet blocking - balancing cybercrime responses in democratic societies*, October 2009, p 182, available at http://www.aconite.com/blocking/study; French version available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/ (URLs last accessed on 26 January 2018).

156 On this fundamental principle, see also ECtHR, 3rd Sect., 12 May 2000, *Khan v. The United Kingdom*, appl. nº 35394/97, §26.

157 ECtHR, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), p. 19, referring to ECtHR, plen., 2 August 1984, *Malone v. The United Kingdom*, appl. n°8691/79, §§66 *et seq.* (violation of Article 8 of the Convention - Interception of postal and telephone communications and release of information obtained from "metering" of telephones, both effected by or on behalf of the police within the general context of criminal investigation).

158 All quotations are coming from the European Court of Human Rights case *Sunday Times v. The United Kingdom*, *op cit*, § 49. See also Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, page 43; Steve Foster, *Human Rights and Civil Liberties*, 2nd ed., 2008, p. 464.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

fundamental rights, in addition to be a safeguard ensuring through transparency that what is foreseen will be effective, since it can therefore be controlled - the principle of legal basis participating that way in the proportionality of the interference[160] in addition to be an imperative to ensure legal certainty[161].

This principle of transparency is named fairness in the EUCFR[162], this requirement going also beyond the principle of legal basis as we will analyse it with the proportionality principle.

As a result, the requirement is to provide "*the entire relevant and adequate information*"[163], excluding that way "*obscurity and uncertainty as to the state of the law*"[164], in relation to both the nature and extent of the interference and the "*adequate and effective guarantees against abuse*" that are implemented[165]. Among the information to be provided lie the "*kind of information that may be recorded, the categories of people against whom* [...] [the] *measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed* [...] [, the] *limits on the age of information held or the length of time for which it may be kept*"[166].

---

159 ECtHR, ch., 24 April 1990, *Huvig v. France*, appl. no 11105/84, §32 ("*clear, detailed rules*"). For an example at the domestic level, the French Constitutional Council considers more globally that the principles of clarity, accessibility and intelligibility of the law impose on the law-maker to "adopt disposals of sufficient precision and non-equivocal formula in order to prevent subjects of the law from an interpretation that would be in opposition with the Constitution or from the risk of arbitrary": French Constitutional Court, decision n° 2004-503 of 12 August 2004, § 29, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2004/2004-503-dc/decision-n-2004-503-dc-du-12-aout-2004.908.html (last accessed on 18 January 2018).

160 See below our Section 2.3.2.4.2.

161 ECtHR, 28 March 2000, ch., *Baranowski v. Poland*, appl.n°28358/95, §52 ; Conseil d'État, *op. cit.* (n°29), p. 281.

162 EUCFR, Article 8 .

163 Translated from French, ECtHR, 3rd Sect., *Haralambie v. Romania*; 27 October 2009, appl. n°21737/03, §86 (juged in relation to the access to information). See also *Handbook on European data protection law*, European Union Agency for Fundamental rights and Council of Europe, 2014, 3.4 p. 73, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

164 . ECtHR, plen., 2 August 1984, *Malone v. the United Kingdom*, appl. n°8691/79*,* §79; French Constitutional Council, Decision n° 2004-503 DC of 12 August 2004, *op.cit.,* § 29.

165 ECtHR, plen., 6 September 1978, *Klass and other v. Germany*, appl. n°5029/71, §50; French Constitutional Council, Decision n° 2013-357 QPC of 29 November 2013, *Société Wesgate Charters Ltd*, cons. 8, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2013/2013-357-qpc/decision-n-2013-357-qpc-du-29-novembre-2013.138841.html (last accessed on 28 January 2018).

166 ECtHR, gr. ch., 4 May 2000, *Rotaru v. Romania*, appl. n°28341/95, §57.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

The level of detail that is required "*depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed*"[167]. As a result, in the context of the collection of personal data by public authorities, the ECtHR considers that this requirement of foreseeability "*cannot be exactly the same (…) where the object of the relevant law is to place restrictions on the conduct of individuals*"[168]. However, in such case, the law must still be "*sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to* [a] [...] *potentially dangerous interference with the right to respect for private life and correspondence*"[169]. Law must further *"indicate the scope* [...] *and the manner of* [...] *exercise"*[170] of the power conferred to competent authorities, "*with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference*"[171]. This notably implies to include an indication of the "*grounds required for ordering*" the measures that constitute the interference[172], and a series of information ensuring the fairness of the processing such as the cases in which the measure can take place[173], the length of the measure[174], the extent of LEAs' powers[175], and the way the respect of these restrictions will be enforced and controlled.

The principle of clarity is therefore applicable in any case and particularly in the area of communications intercept by the judicial authority[176] and by intelligence services[177], as well as more widely to "*both the storing by a public authority of information relating to an individual's private life and the use of it*

[167] ECtHR, gr. ch., 26 October 2000, *Hasan and Chaush v. Bulgaria*, appl. n° 30985/96, §84.
[168] ECtHR, *Malone v. The United Kingdom*, §67, *op. cit.*; Council of Europe, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), *op. cit.*, p. 19; In the same line see ECtHR, 2nd Sect., 22 October 2002, *Taylor-Sabori v. the United Kingdom*, appl. n°47114/99, §18, related to covert surveillance by public authorities.
[169] ECtHR, *Malone v. The United Kingdom*, *op. cit.* §67; See also all the references in footnote n°147.
[170] ECtHR, *Malone v. the United Kingdom*, *op. cit.* §68; ECtHR, 4th Sect., 12 January 2016, *Szabó and Vissy v. Hungary,* appl. no37138/14, §65; ECtHR, gr. ch., 4 December 2008, *S and Marper v. the United Kingdom*, appl. n° 30562/04 and 30566/04, §95; Council of Europe, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), *op. cit.*, p. 19.
[171] *Ibid.*
[172] See for example ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 50.
[173] See for example ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 51.
[174] See for example ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 50.
[175] See for example ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 56.
[176] See for ex. ECtHR, 12 May 2000, *Khan v. The United Kingdom*, appl. no 35394/97, §22s.
[177] See for ex. ECtHR, plen., 2 August 1984, *Malone v. the United Kingdom, appl.* 8691/79, §67.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

and the refusal to allow an opportunity for it to be refuted"[178], in particular within the context of "*the development of surveillance methods resulting in masses of data collected*"[179] (which must be accompanied by a "*simultaneous development of legal safeguards securing respect for citizens' Convention rights*"[180]).

2.3.2.1.2. Adequately accessible

Domestic law must also "*be adequately accessible*", which means that "*the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case*"[181]. This implies firstly that the legal basis is easily accessible to concerned citizens[182]. This implies secondly that the provisions which base the limitation of freedom are intelligible "*in the light of the legal corpus in which they are intended to be part of*" [183]. Therefore, the whole of this corpus must be consistent[184], in order to fully meet the requirement of predictability[185]. In other words, the "*physical*"[186] access to the legal basis must be accompanied by an "*intellectual*" [187] access to this legal basis.

2.3.2.1.3. Stable

A law that can "*reasonably*"[188] be foreseen must be stable[189], this principle being also linked to the requirement of legal certainty[190]. In addition, the principle of stability favours the general public's

---

178 ECtHR, gr.ch., 4 May 2000, *Rotaru v. Romania*, appl. nº28341/95, §45s.
179 ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary*, appl. nº37138/14, §68.
180 *Ibid.*
181 ECtHR, plen., 26 April 1979, *Sunday Times v. The United Kingdom*, appl. n° 6538/74, § 49. On this question, see also Pascale Deumier, « La publication de la loi et le mythe de sa connaissance », Les petites affiches, 6th March 2000, n° 46.
182 Ex. ECtHR, ch., 24 April 1990, *Huvig v. France*, appl. nº 11105/84, §33.
183 Translated from French. French Conseil d'État, « Sécurité juridique et complexité du droit », public report 2006, http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Securite-juridique-et-complexite-du-droit-Rapport-public-2006, p. 282.
184 *Idem*, pp. 282 et 288. Principles of consistency and intelligibility of legal texts as a whole are most of the time implicit in the ECtHR jurisprudence (see for ex. ECtHR, plen., 2 August 1984, *Malone v. the United Kingdom*, appl. n°8691/79, §66). However see ECtHR, ch., 16 December 1992, *de Geouffre de la Pradelle v. France*, appl. nº12964/87, §34; ECtHR, gr.ch., 15 October 2015, *Perinçek v. Switzerland*, appl. nº 27510/08, §134.
185 ECtHR, *Huvig v. France*, *op. cit.* §26.
186 Translated from French. Pascal BEAUVAIS, « Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes », *in* ERPC, *Archives de politique criminelle*, éd. A. Pédone, 2007/1 (nº29), p.4, https://www.cairn.info/revue-archives-de-politique-criminelle-2007-1-page-3.htm (last accessed on 28 January 2018).
187 *Idem.*
188 See for ex. ECtHR, gr. ch., 15 October 2015, *Perinçek v. Switzerland*, appl. n°27510/08, §134.
189 See for ex. ECtHR, 1st sect., 30 July 2015 (final: 30/10/2015), *Ferreira Santos Pardal v. Portugal*, appl. nº30123/10, §42, f.
190 *Idem*; French Conseil d'État, « Sécurité juridique et complexité du droit », *op. cit.*, p. 281.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

confidence in the legal system, such confidence being "*one of the essential components of a State based on the rule of law*"[191]. The principle of stability especially means no unpredictable variations[192] and, potentially, not too frequent variations[193].

2.3.2.2 - A legitimate aim

Article 8 para. 2 of the ECHR lists exhaustively the legitimate aims for which an interference with the right to privacy, including the right to the protection of personal data, may be legitimate. These aims are the interests of national security, public safety or the economic well-being of the country; the prevention of disorder or crime; the protection of health or morals, and the protection of the rights and freedoms of others.

This notion of legitimate aim is also considered by the Court of Justice of the European Union[194], the EUCFR requiring that limitations to the rights it enshrines must "*genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*"[195].

2.3.2.3 - The necessity of the interference

This principle of "necessity" of the interference consists in the **demonstration that this interference is actually appropriate to satisfy a specific societal need**.

Indeed, according to the ECtHR, any limitation of private life, in order to be legitimate, must be a need, and this need must be established convincingly[196]. The latter term "need" refers to two

---

191 See for ex. ECtHR, 3rd Sect., 1st December 2005, *Păduraru v. Romania*, appl. n°63252/00, §98; ECtHR, *Ferreira Santos Pardal v. Portugal, op. cit.* §42, f.

192 ECtHR, 30 July 2015, *Ferreira Santos Pardal v. Portugal*, *op. cit.* §43-49; French Conseil d'État, « Sécurité juridique et complexité du droit », *op. cit.* p. 281.

193 French Conseil d'État, « Sécurité juridique et complexité du droit », *op. cit.* p. 281. See ECtHR, ch., 16 December 1992, *de Geouffre de la Pradelle v. France*, appl. n°12964/87, §33; Pascal BEAUVAIS, « Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes », *in* ERPC, *Archives de politique criminelle*, éd. A. Pédone, 2007/1 (n°29), pp. 13 and seq., https://www.cairn.info/revue-archives-de-politique-criminelle-2007-1-page-3.htm; Dominique J. M. SOÛLAS de RUSSEL, Philippe RAIMBAULT, « Nature et racines du principe de sécurité juridique : une mise au point », RIDC, 2003, vol. 55, n°1, p. 90, referring to ECtHR, plen., 13 June 1979, *Marckx v. Belgium*, appl. n°6833/74 (URLs last accessed on 28 January 2018).

194 See for example CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, §46.

195 Article 52.1 of the Charter.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

different kind of needs: a "pressing social need" (in other words a societal issue that needs to be addressed[197]), and a need for the specific proposed interference (which must be appropriate to satisfy the identified social need[198]). These two needs constitute the requirements of the principle of necessity.

2.3.2.3.1. The demonstration of a specific societal need

The interference must be "*necessary having regard to the facts and circumstances prevailing in the specific case*"[199], which implies firstly identifying "*the specific societal need to be addressed*", "*within the broader sphere of the legitimate aim pursued",* with a view to protecting this particular aim[200].

This need must be "pressing", in other words it must have a certain "*level of severity, urgency or immediacy"*[201]. Harm may result on society if the need is not addressed, taking into account the views of society and potentially divergent opinions regarding this particular "need"[202].

Moreover, the existence of this severe or urgent need has to be proven. For instance, in a case where the applicant had been prevented by the national courts to make certain statements relating to the dangers of microwave ovens, on the base of infringing the right to fair competition, the ECtHR

---

196 ECtHR, ch., 25 February 1993, *Crémieux v. France*, appl. n° 11471/85, §38: "*the need for an interference* (...) *in a given case must be convincingly established*". In the same spirit, see the Opinion of the European Data Protection Supervisor, on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, 26 September 2005, § 10, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2005/05-09-26_data_retention_EN.pdf (last accessed on 28 January 2018).

197 Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, 3.13.

198 Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.17, 3.19.

199 ECtHR, *Sunday Times v. The United Kingdom*, *op. cit*, § 65.

200 Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.13.

201 Article 29 Data Protection Working Party, Opinion 01/2014 (WP 211), *op. cit.*, 3.14.

202 Article 29 Data Protection Working Party, Opinion 01/2014 (WP 211), *op. cit.*, 3.17 - 3.19.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

concluded that "*there was no evidence that the sale of microwave ovens had been affected by the applicant's remarks*"[203].

2.3.2.3.2. The demonstration that the interference is suited to satisfy that need

Establishing the need for interference, in a given case, also means establishing that this interference is appropriate to reach the aim pursued, in other words that it effectively may mitigate the harm caused to society[204].

This identification of the necessity of the interference may imply reviewing "*the effectiveness of existing measures*" aiming at addressing the targeted pressing social need, "*over and above the proposed measure*", and explaining "*why these existing measures are no longer sufficient*" and how the proposed measure will bring remedies[205].

For instance, the European Data Protection Supervisor recalled that "*statements of Member States on whether they consider data retention a necessary tool for law enforcement purposes*" do not "*as such establish the need for data retention as a law enforcement measure*", and that "*the statements on the necessity should be supported by sufficient evidence*"[206].

---

[203] Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 *et se*q., quotation p. 25, in relation with ECtHR, ch., 25 August 1998, *Hertel v. Switzerland*, appl. n° 25181/94. Jeremy McBride considers this requirement (consisting in determining "*whether there was a sufficient basis for believing that a particular interest was in peril*") as being a "proportionality" requirement. However, together with the Article 29 Data Protection Working Party (see footnotes above), we rather believe that this requirement is a condition of the "necessity" of an interference, not a condition of its proportionality. However, this discordance of opinions has no practical impact, since it is in any cases a requirement which will base the assessment of the Court. On this issue see below our Section 2.3.2.5.

[204] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.19. In the same sense see also CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, §49, available at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12 (last accessed on 14 February 2018), which verifies whether the interference "*is appropriate for attaining the objective pursued*".

[205] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, 3.26.

[206] Opinion of the European Data Protection Supervisor, on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31 May 2011, § 41, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf (last accessed on 24 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

In the same line, the Article 29 Data Protection Working Party noticed, in 2004, that the framework decision on data retention which proposed a "*comprehensive storage of all traffic data, user and participant data*", did not provide "*any persuasive arguments that retention of traffic data to such a large-scale extent is the only feasible option for combating crime or protecting national security*". The Working Party also noticed that "*representatives of the law enforcement community have failed to provide any evidence as to the need for such far reaching measures*"[207].

More recently, the CJEU recalled that "*the principle of proportionality*[208] *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*"[209]. However, unlike the two authorities quoted above, the CJEU considered that the retention of traffic data "*may be considered to be appropriate for attaining the objective pursued*" by the Data Retention Directive[210]. The CJEU challenged the validity of the Data Retention Directive in the light of Article 7 of the EUCFR, not on the basis of the principle of necessity, but on the basis of the principle of proportionality that we will analyse below, the interference being not limited to what is strictly necessary to achieve its objectives.

2.3.2.4 - The proportionality of the interference to the aim pursued

The principle of proportionality[211] is "*recognised as one of the central principles governing the application of the rights and freedoms*" contained in the ECHR and its additional Protocols.[212] Allowing "*some evaluation of*

---

[207] Article 29 Data Protection 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 or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism, adopted on 9 November 2004, WP99, quotations page 4.

[208] This principle includes, in this formula, the principle of necessity (Advocate General Poiares Maduro for instance considers that "*the concept of necessity [...] is well established as part of the proportionality test*" (Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 5.7). For further analysis of discordances of classification, see the introduction of our Section 4.1.3.

[209] CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, *op. cit.*, §46.

[210] CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, *op. cit.*, §49.

[211] On the entire subsection see Estelle De Marco *in* Cormac Callanan, Marco Gercke, Estelle De Marco and Hein Dries-Ziekenheiner, *Internet blocking - balancing cybercrime responses in democratic societies*", October 2009, Section 7.5.2,

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

how much of a contribution a particular restriction can make towards securing a given objective"[213], the principle of proportionality satisfies "*the need for balancing entailed when giving effect to the rights*" that are concerned by the ECHR requirements. Indeed, without this requirement, "*the formulation of Convention provisions would be open to restrictions depriving the rights and freedoms of all content so long as they were prescribed by law and for a legitimate purpose*"[214], in addition to answering a pressing social need.

In the light of the ECtHR court cases, the proportionality of a measure that limits freedoms implies that this measure or interference does not go "*further than needed to fulfil the legitimate aim being pursued*"[215], and is surrounded by appropriate safeguards.

2.3.2.4.1. The interference must be strictly necessary

The limitation of a conditional fundamental right must be strictly necessary to the aim pursued, and, for example, in relation with the monitoring of communications by public authorities, it must be "*strictly necessary, as a general consideration, for the safeguarding of the democratic institutions and, moreover, (...) strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation*"[216].

This principle implies an effective assessment of the strict necessity of the measure in relation with its context, scope and nature:

---

http://www.aconite.com/blocking/study; French version available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/ (URLs last accessed on 26 January 2018).

[212] Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 *et seq*., quotation p. 23.

[213] Jeremy McBride, *op cit, p. 24*.

[214] Jeremy McBride, *op cit,* p. 24.

[215] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.20.

[216] ECtHR, 4th Sect., 12 January 2016, *Szabó and Vissy v. Hungary,* appl. nº37138/14, §73. For an application of this principle by the CJEU, see for example CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, §§ 46, 56 and 65.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- **Context**[217]**:** adapting the interference to its context means inter alia taking into account several elements such as the severity of the social need and the "*proportionality of the very behaviour which is being restricted*"[218].

  - **The severity of the social need:**

    Depending on the seriousness of the issue to be addressed, whatever measures will not be considered as appropriate. As it has been highlighted by the Article 29 Data Protection Working Party"[219], "*the more severe the issue and/or the greater or more severe or substantial the harm or detriment which society may be exposed to, the more an interference may be justified*". When the aim of the interference is public security, and more specifically prevention and detection of crime, the severity of the social need must be assessed having regards to the specific crime the measure is intended to address[220], and to the harm that crime would cause to society if not addressed.

  - **The proportionality of the restricted behaviour (and legitimacy of the opposed fundamental right)**

    Whatever the severity of the societal issue to be addressed, the proposed measure may cause harm to individuals to a lesser or greater extent, and the more this extent is, the less the interference is appropriate[221]. The "*nature of the activity being affected*" (sensitivity, high expectation of privacy[222], value of the possibly opposed fundamental right…) needs

[217] See for ex. ECtHR, ch., 24 February 1997, *De Haes et Gijsels v. Belgium,* appl. n°19983/92.
[218] Jeremy McBride, *op cit*, pp. 25.
[219] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, 3.26.
[220] The ECtHR noted for instance in a court case the lack of consideration of "*the nature or gravity of the offence*": Article 29 Data protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), op. cit., 3.24, referring to ECtHR, gr.ch., 4 December 2008, *S & Marper v. United Kingdom*, appl. n° 30562/04 and 30566/04.
[221] The Article 29 Data Protection Working Party covers this issue under the formula "*nature of the interference*": Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.26.
[222] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211*), op. cit.*, 3.26.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

therefore to be taken into account.

For example, "*the privacy considerations in terms of context are very different when installing CCTV cameras on a public street as opposed to installing them in toilets or hospital wards*"[223]. In the same spirit in relation to freedom of expression, the ECtHR considered that the "*remarks made by journalists about the conduct of views of judges and politicians*" were appropriate and could not be punished, considering *"they had sufficient factual basis to fall within the protection extended to the expression of value judgments under Article 10*"[224].

The proportionality of the very behaviour that is being restricted may also depend on the characteristics of the individuals whose rights are limited. Such a characteristic may be the age (for example, the age "*of the suspected offender*" when the aim of the interference is public security[225]), and the capacity of a given individual to adapt his or her behaviour to a given context[226].

- **Scope[227]:** the scope of the interference must not exceed what is necessary to reach the aim pursued[228]. This means, *inter alia*, to limit to the greatest extent the volume of the intrusions into privacy (and, for example, of collected personal information), the number of places and

[223] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.26.
[224] Jeremy McBride, *op. cit.*, pp. 25 and 26, referring to ECtHR, ch., 24 February 1997, *De Haes and Gijsels v. Belgium*, appl. n° 19983/92, and ECtHR, ch., 1 July 1997, *Oberschlick v. Austria* (n°2), appl. n° 20834/92.
[225] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.,* 3.24, referring to ECtHR, gr.ch., 4 December 2008, *S & Marper v. United Kingdom*, appl. n° 30562/04 and 30566/04.
[226] In relation to an obligation to secure one's computer in order to prevent counterfeiting (knowing that computer security can never be ensured for sure), see Estelle De Marco, *Analyse du nouveau mécanisme de prevention de la contrefaçon à la lumière des droits et libertés fondamentaux*, 4 June 2009, Juriscom.net, http://juriscom.net/2009/06/hadopi-analyse-du-nouveau-mecanisme-de-prevention-de-la-contrefacon-a-la-lumiere-des-droits-et-libertes-fondamentaux/ (last accessed on 28 January 2018).
[227] See for ex. ECtHR, 5e sect., 19 May 2016, *D.L. v. Bulgaria*, appl. no7472/14, §105.
[228] See for example ECtHR, 5th Sect., 19 May 2016, *DL v. Bulgaria, op. cit.*, §105. See also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, 3.26.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

people affected[229], the cases of exercise of the measure (LEAs' powers of decision and action must notably be limited to what is necessary), and the time during which the measure will be effective[230].

In relation to the cases of exercise of the measure, interferences that consist in processing personal data must in particular be based on the consent of the person concerned or on some other legitimate ground laid down by law[231] (these legitimate grounds being actually authorised situations of exercise of the measure, motivated by listed purposes that are more specific than the "legitimate aim" required by the ECHR and the EUCFR, but broader than the specific need to be identified during the necessity test, and which may be bypassed in case the data subject gives his or her consent). Other situations of exercise might be imposed by fundamental legal instruments depending on the exact nature of the interference: for instance, certain methods of people surveillance must be limited to serious crimes[232] or to "very serious crimes"[233].

Where the interference aims to the prevention or repression of penal infringements, it must be adapted to the severity of the infringement at stake, as well as to the impact this infringement may have on society[234]. The latter impact might at least partly be assessed in the light of the importance granted to the combat against this particular infringement on a value scale, at a given national level: it might for example be considered that physical violations of human

[229] ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary,* appl. n°37138/14, *op.cit.* §§73 and 75-77. On this issue and the previous one see also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.26.
[230] On this issue and the previous one see for example ECtHR, ch., 25 February 1993, *Crémieux v. France*, appl. n° 11471/85, §40.
[231] EUCFR, Article 8 ; At the CEDH level see for ex. ECtHR, 3rd Sect., *Perry v. the United Kingdom*, 17 July 2003, appl. n° 63737/00, §46; ECtHR, 4th Sect., *Peck v. the United Kingdom*, 29 January 2003, appl. n° 44647/98, §78.
[232] See for ex. ECtHR, 3rd Sect., 8 November 2016, *Figueiredo Teixeira v. Andorra*, appl. n° 72384/14, §43. See also Council of Europe, Committee of Ministers, Recommendation n° Rec (2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism, 20 April 2005.
[233] See for ex. ECtHR, 5th Sect., *Uzun v. Germany*, 2 September 2010, appl. n° 35623/07, §80.
[234] The ECtHR did for example noticed the lack of consideration of "*the nature or gravity of the offence*": Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.24, referring to the case ECtHR, gr. ch., *S and Marper v. the United Kingdom*, 4 December 2008, appl. n° 30562/04 and 30566/04, §35.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

integrity are more severe than theft[235]. However, a certain amount of attention should be devoted to the consistency of this value-scale, which could itself be challenged at the ECtHR level[236].

In addition, the "*overall effect*" of the interference must not lead to "*actually extinguish*"[237] a protected right:[238] for instance, it "*was found to be unacceptable*" to prevent a person making statements in a situation where such a measure effectively prevented this individual "*making his contribution to the public debate*": this was affecting "*the very substance of his view*"[239]. Another example could be to prevent someone from exercising his or her private life on a particular well-used social network[240].

---

235 Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, *op. cit.*, 3.18.

236 For example, under French law, gradations in certain penalties do not seem to reflect the importance of values to be protected. Indeed, if sanctions were showing a hierarchy of value, counterfeiting (3 years of imprisonment and fine of 300 000 € - Articles L. 335-2 *et seq.* of the Intellectual property Code) would be considered as undermining society more seriously than provocation to hatred (1 year of imprisonment and/or a fine of 45 000 € - Article 24 of Law of 29 July 1881 on Press freedom), and the non-denunciation of provocation to hatred by hosting providers (1 year of imprisonment and a fine of 75 000 €, in addition to the prohibition to exercise for 5 years or more this professional activity - Article 6, I, 7, 5° and 6, VI, 1 of Law n°2004-575 of 21 June 2004) would be considered as undermining Society more seriously than the provocation to hatred itself. On this issue see Estelle De Marco, *Analyse du nouveau mécanisme de prevention de la contrefaçon à la lumière des droits et libertés fondamentaux*, 4 June 2009, Juriscom.net, http://juriscom.net/2009/06/hadopi-analyse-du-nouveau-mecanisme-de-prevention-de-la-contrefacon-a-la-lumiere-des-droits-et-libertes-fondamentaux, especially the conclusion; Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 818.

237 Jeremy McBride, *op cit*, p. 24.

238 In the same line, the CJEU verifies whether the interference may "*adversely affect the essence of the fundamental right*": CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, §40, available at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12 (last accessed on 14 February 2018).

239 Jeremy McBride, op cit, p. 25, referring to the court case Hertel v. Switzerland, judgment of the Court, 25 August 1998.

240 See for example the practice of Facebook which consists in closing the accounts of persons who use a pseudonym and who refuse to produce their identity card, without seriously justifying their need for such personal information (outside an argument of combatting identity usurpation, which does not seem acceptable since the production of an identity card does not prove the identity of the account's owner, and since the service provider seems here to illegitimately assume a prerogative of public power, in a context where the use of pseudonyms is a security recommendation: see for ex. Nadia Drake, *Help, I'm Trapped in Facebook's Absurd Pseudonym Purgatory*, 19 June 2015, https://www.wired.com/2015/06/facebook-real-name-policy-problems/; The Berlin District Court has furthermore considered that this obligation to mention a true identity was illegal under German law: see for ex. Gericht rüffelt Facebook für Voreinstellungen, 12 February 2018, Spiegel Online, http://www.spiegel.de/netzwelt/web/facebook-voreinstellungen-landgericht-berlin-sieht-verbraucherschutz-verstoesse-a-1193024.html, and (with the German decision

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- **Nature**[241]**:** the ECtHR also verifies if the interference's aim "*can be satisfactorily addressed in some other, less restrictive way*"[242]. For instance, "*an order requiring a journalist to disclose his source for a leak about the financial affairs of a company was considered to be unjustified* […] *insofar as the objective was to prevent dissemination of confidential information since this legitimate concern was already being secured by an injunction restraining publication of the information that had been disclosed*"[243]. Therefore, "*an explanation of what other measures were considered and whether or not these were found to be more or less privacy intrusive should be presented. If any were rejected which were found to be less privacy intrusive, then the strong justifying reasons as to why this measure was not the one that was selected to be implemented should be given*"[244].

2.3.2.4.2. The interference must be limited by appropriate safeguards

Appropriate safeguards, in other words "*adequate and effective*"[245] safeguards, must firstly be implemented in order to palliate potential weaknesses of the necessity and proportionality tests[246], in particular where technology used does not itself enable to limit the scope of this interference as it would be necessary. These safeguards must secondly be implemented in order to "*render possible*"[247] the actual respect of the limitation of the interference extent as it has been scheduled - which means in order to ensure the effectiveness of limitations as they have been determined, through the determination of enforcement and control measures which might especially be of an organisational or of a technical nature.

---

in Annex) Etienne Wery, *Facebook condamnée : ses conditions générales posent problème*, 15 February 2018, https://www.droit-technologie.org/actualites/facebook-condamnee-conditions-generales-posent-probleme/ (URLs last accessed on 16 February 2018).

241 See for ex. ECtHR, gr.ch., 27 March 1996, *Goodwin v. United Kingdom,* appl. nº17488/90, §42.

242 Jeremy McBride, op cit, p. 26. For an application of this principle at the EU level see for example a judgment of the European Union civil service tribunal (first chamber), *V. v. European Parliament*, 5 July 2011, case F-46/09, § 139, available at http://curia.europa.eu/juris/liste.jsf?language=en&num=F-46/09 (last accessed on 14 February 2018).

243 Jeremy McBride, op cit, p. 26, referring to ECtHR, gr.ch., 27 March 1996, *Goodwin v. United Kingdom,* appl. nº17488/90.

244 Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 3.26.

245 ECtHR, *Klass and others v. Germany*, *op. cit.* §§ 50 *et seq.*

246 ECtHR, plen., 6 September 1978, *Klass and others v. Germany*, appl. n°5029/71, §55, referring to "*adequate and equivalent guarantees*" to be implemented in order to palliate the absence of effective remedy.

247 Ex. ECtHR, plen., 13 June 1979, *Marckx v. Belgium*, appl. nº6833/74, §31.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Enforcement measures will include at the first place the clear identification and transparent[248] information - in other words fair[249] information - relating to the nature, extent and limits of the interference, as well as relating to the safeguards that will ensure that these limits are respected. This should be primarily done in the legal basis that authorises the interference, as analysed previously in this report[250]. As we already evoked it, this identification and correlative information must relate to the "*kind of information that may be recorded, the categories of people against whom* [...] [the] *measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed*"[251], as well as to "*minimum safeguards concerning, inter alia, duration* ['*age of information held or the length of time for which it may be kept*'[252]], storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness"[253].

We already analysed that the level of detail that is required "*depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed*"[254], but similar information will be required in any case, including where processing activities are carried out by public authorities[255], in order to "*give the individual adequate protection against arbitrary interference*" through sufficient clarity[256], including *"the scope* [...] *and the manner of* [...] *exercise"*[257] of the power conferred to competent authorities, the cases in which the measure can take place[258], the

[248] See above the Section 2.3.2.1.1 of the current report.
[249] EUCFR, Article 8.
[250] See above the Section 2.3.2.1.1 of the current report.
[251] ECtHR, gr. ch., 4 May 2000, *Rotaru v. Romania*, appl. n°28341/95, §57.
[252] Ibid, §57.
[253] ECtHR, gr. ch., 4 December 2008, *S and Marper v. the United Kingdom*, appl. n° 30562/04 and 30566/04, §99.
[254] ECtHR, gr. ch., 26 October 2000, *Hasan and Chaush v. Bulgaria*, appl. n° 30985/96, §84.
[255] See for ex. ECtHR, plen., 2 August 1984, *Malone v. the United Kingdom*, appl. n°8691/79, §67; ECtHR, 2nd Sect., 22 October 2002, *Taylor-Sabori v. the United Kingdom*, appl. n°47114/99, §18, related to covert surveillance by public authorities.
[256] *Ibid.*
[257] ECtHR, *Malone v. the United Kingdom*, *op. cit.* §68; ECtHR, 4th Sect., 12 January 2016, *Szabó and Vissy v. Hungary,* appl. n°37138/14, §65; ECtHR, gr. ch., 4 December 2008, *S and Marper v. the United Kingdom*, appl. n° 30562/04 and 30566/04, §95; ECtHR, plen., 6 September 1978, *Klass and others v. Germany*, appl. n°5029/71, §56; Council of Europe, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), *op. cit.*, p. 19.
[258] See for example ECtHR, plen., 6 September 1978, *Klass and others v. Germany*, appl. n°5029/71, §. 51.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

length of the measure[259], as well as the "*grounds required for ordering*" the measures that constitute the interference[260].

Transparency or fairness is however not limited to the legal basis and must also be ensured throughout the life of the interference through the provision of "*the entire relevant and adequate information*"[261] relating to processing operations, especially in case the concerned person requests an access to information relating to this interference and potentially communication of data concerning him or her[262]. Among the information to be provided lie the one which is supposed to be included in the legal basis authorising the interference, in addition to potential specificities of the data processing - in the extent that proportionality requires this information - compared to what this legal basis foresees, which might be relating to the specific context of processing operations, including if the latter evolves, for example information on risks resulting from environmental pollution[263].

Such transparency or fairness must be ensured with regards to specified purposes[264], which means that should only be hidden the information which secrecy is imposed by the pursuit of these purposes[265] the notion of "specified purposes" corresponding to the need that must be identified during the course of the necessity test[266]

---

[259] See for example ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 50.
[260] See for example ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 50.
[261] Translated from French, ECtHR, 3rd Sect., *Haralambie v. Romania*; 27 October 2009, appl. n°21737/03, §86 (judged in relation to the access to information). See also *Handbook on European data protection law*, European Union Agency for Fundamental rights and Council of Europe, 2014, 3.4 p. 73, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (last accessed on 21 February 2018).
[262] ECtHR, 3rd Sect., *Haralambie v. Romania*; 27 October 2009, appl. n°21737/03, §86 ; ECtHR, 4th Sect., *K.H. and Others v. Slovakia*, 28 April 2009 (final: 06/11/2009), appl. n°32881/04, esp. §46.
[263] ECtHR, 4th Sect., 28 April 2009, *K.H. and Others v. Slovakia,* appl. n° 32881/04; §46.
[264] EUCFR, Article 8 ; ECtHR court cases already mentioned in relation to transparency, for example ECtHR, 3rd Sect., *Haralambie v. Romania*, 27 October 2009 (final: 27/01/2010), appl. n°21737/03, §86; ECtHR, 4th Sect., *K.H. and Others v. Slovakia*, 28 April 2009 (final: 06/11/2009), appl. n°32881/04.
[265] In this sense see Council of Europe, Recommendation R(87)15 of the Committee of Ministers to Member States regulating the use of personal data in the Police sector, 6.4: "*Exercise of the rights of access, rectification and erasure should only be restricted insofar as a restriction is indispensable for the performance of a legal task of the police or is necessary for the protection of the data subject or the rights and freedoms of others*".
[266] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), op. cit., 3.13; See above the Section 2.3.2.3.1 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Enforcement measures may also imply the implementation of internal procedures that enable to identify if a given data processing operation is performed in compliance with authorised situations of exercise, one of which being to obtain the consent of concerned individuals[267]. Technical measures must also be implemented where possible, for example ensuring data deletion after a certain period of time[268].

Control measures include the authorisation and/or supervision of an independent authority[269], which will ensure that the legal conditions for the interference are respected and will prevent any freedom of interpretation in relation to general terms potentially provided for by law. In principle, such independent control should be made by the judicial authority before the measure takes place, and a supervision of another nature is only permitted if the authority in charge of it provides the same guarantee of independence and expertise[270], posterior supervision being not permitted in all matters[271] since confidentiality cannot be restored once destroyed[272]. In addition, a judge from the judiciary should be involved "*at least in the last resort*"[273] in fields "*where abuse is potentially so easy in individual cases and would have (…) harmful consequences for democratic society as a whole*"[274], which is generally the case when the interference is organised for police purposes.

Control measures also include a right of access[275] to "*all relevant and appropriate information*"[276], a right of rectification of data[277] and a right to obtain copy of these data without needing to "*specifically justify a*

[267] See above, Section 2.3.2.4.1, "Scope".
[268] See for example ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 52.
[269] EUCFR, Article 8; Article 29 Data Protection Working Party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (WP 211), 27 February 2014, 3.24, referring to ECtHR, gr.ch., 4 December 2008, *S & Marper v. United Kingdom*, appl. n° 30562/04 and 30566/04; ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 55.
[270] ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary,* appl. n°37138/14, *op.cit.* §§73 and 75-77 (media surveillance); ECtHR, ch., 25 March 1998, *Kopp v. Switzerland*, appl. n°23224/94, §73.
[271] *Ibid.*
[272] ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary,* appl. n°37138/14, *op.cit.* §§77.
[273] See for example ECtHR, *Klass and others v. Germany*, *op. cit.*, § 55.
[274] See for example ECtHR, *Klass and others v. Germany*, *op. cit.*, § 56.
[275] EUCFR, Article 8; ECtHR, *Haralambie v. Romania*, *op. cit.*; ECtHR, *K.H. and Others v. Slovakia*, *op. cit.* §46; Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.,* 3.24.
[276] ECtHR, *K.H. and Others v. Slovakia*, *op. cit.* §46.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

request to be provided with [such] *a copy*"[278], granted to concerned individuals. An "*effective and accessible*"[279] procedure to be followed to exercise these rights must be available[280] and a right of appeal must be available, in particular where the right of access is denied[281]…).

Finally, means must be provided to ensure safeguards effectiveness, such as a judicial organisation and an adequate allocation of resources in order to ensure the practical implementation and the efficiency of judicial controls.

2.3.2.5. Note on the discordance of classification of the necessity and proportionality requirements

The principles of necessity and of proportionality are both contained in the ECHR formula: "*necessary in a democratic society*"[282], and therefore might both be covered by the term "necessary"[283] where this word is used by reference to this previous formula. However, the most cited and perhaps most important principle (considered as a "*one of the general principles of European Union law*"[284]) is proportionality, which might therefore be used in turn, by abuse of terms, as a principle covering the principle of necessity, especially since one of its requirements is to ensure that an interference does not exceed what is "necessary" to reach the aim pursued[285], such a term having a different meaning than the notion of "necessity" but being likely to create confusion.

---

277 EUCFR, Article 8; ECtHR, 2nd Sect., 18 November 2008, *Cemalettin Canli v. Turkey*, appl. n° 22427/04, §§20-27; *Handbook on European data protection law*, European Union Agency for Fundamental rights and Council of Europe, 2014, 3.4 p. 73, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (last accessed on 21 February 2018), Section 5 p. 103.
278 ECtHR, *K.H. and Others v. Slovakia*, *op. cit.* §§47-48.
279 ECtHR, *K.H. and Others v. Slovakia*, *op. cit.* §46.
280 See for example ECtHR, 2nd Sect., 24 September 2002, *MG v. the United Kingdom*, appl. n° 39393/98, and Council of Europe, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), p. 91; ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 55.
281 ECtHR, *MG v. the United Kingdom*, appl. n° 39393/98, *op. cit.*; ECtHR, *Klass and others v. Germany*, *op. cit.*, §. 56.
282 See above the introduction of our Section 2.2.3.
283 See for example ECtHR, 5th Sect., 19 May 2016, *DL v. Bulgaria*, appl. n° 7472/14, §105.
284 See for ex. CJEU, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, joint cases C-92/09 and C-93/09, § 74.
285 See above, our Section 2.3.2.4.1.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

In the current Section 2.3, the principles of necessity and proportionality and their respective requirements were analysed on the basis of a deep analysis of the ECtHR court cases, taking also into account the etymology of these words. But as a result of the observation made in our first paragraph above, it is to be noted that it is not rare that the doctrine or court cases name one of what we consider as being a proportionality requirement as being a necessity requirement[286], and vice versa[287].

This being said, these discordances of classification have very small or no practical consequences since, usually, the respect of both these principles is required where one of them must be applied, and both courts and legal analysts recognise that necessity and proportionality imply together a certain number of obligations, which are the ones we have analysed in this Section, whatever they are classified as obligations ensuring necessity or obligations ensuring proportionality. In that line, the Article 29 Data Protection Working Party[288] has emphasised that the European Union Court of Justice (CJEU) has an approach which is "*largely consistent*" with the ECtHR's one[289], and has made recent efforts to apply the principles of necessity and proportionality, as they were developed by the ECtHR, to Article 7 and 8 of the EUCFR[290].

---

[286] See for example CJEU, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, *op. cit.*, §§ 76 *et seq.* ; CJEU, *Schwarz v. Stadt Bochum*, C-291/12, 17 October 2013, §46: "*in assessing whether such processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage measures which will interfere less with the rights recognised by Articles 7 and 8 of the Charter but will still contribute effectively to the objectives of the European Union rules in question*" (the research for less intrusive measures being a proportionality requirement, see below our Section 2.2.3.4). On this latter decision, see also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), n° 3.31.

[287] See for ex. CJEU, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, *op. cit.* § 74: "*the principle of proportionality* (...), *requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued*"; Advocate General Poiares Maduro considers for example that "*the concept of necessity [...] is well established as part of the proportionality test*": see Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), n° 5.7.

[288] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.30.

[289] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 4.2.

[290] For an example of such application, see CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, 8 April 2014, available at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12 (last accessed on 14 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Summary of Section 2.3

General considerations:

- The protection mechanism of both the right to private life and the right to personal data protection is the same. Indeed, both Article 8 of the ECHR and Article 7 and 8 of the EUCFR - which do coexist today, their provisions being mandatory for EU Member States[291] - offer to privacy and to personal data an equal protection: the rights laid down in Articles 7 and 8 of the EUCFR have the same scope and meaning than Article 8 of the ECHR where they do not offer a stronger protection[292], and the details provided in addition in Article 8 of the EUCFR are already an integral part of the protection offered by the European Court of Human Rights (ECtHR)[293].
- Since the protection mechanism of both the right to private life and the right to personal data protection is the same, the theoretical debate relating to the interrelations between the sphere of private life and the sphere of personal data has no practical incidences, outside the interest of identifying the other freedoms that are at stake.
- This protection mechanism determines both the content of the protected privacy and the extent of the personal data protection. Its knowledge is therefore an important asset within the framework of a

[291] All the EU Member States have ratified or accessed the ECHR, and the EUCFR has the same value as the treaties since the entry into force of the Treaty of Lisbon (Article 6 of the Treaty on European Union).
[292] EU Charter of Fundamental Rights, article 52, 3. For further reading, see especially French Cour de cassation, "Dossier : la charte des droits fondamentaux - historique et enjeux juridiques", *in* veille bimestrielle de droit européen, October 2010, n° 34, http://www.courdecassation.fr/publications_26/publications_observatoire_droit_europeen_2185/veilles_bimestrielles_droit_europeen_3556/2010_3865/octobre_2010_3810/droits_fondamentaux_18630.html (last accessed on 24 January 2018).
[293] On the fairness of the processing see *Handbook on European data protection law*, European Union Agency for Fundamental rights and Council of Europe, 2014, 3.4 p. 73, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, and the ECtHR court cases referred to in this Section such as ECtHR, 3rd Sect., *Haralambie v. Romania*, 27 October 2009 (final: 27/01/2010), appl. n°21737/03, §86; ECtHR, 4th Sect., *K.H. and Others v. Slovakia*, 8 April 2009 (final: 06/11/2009), appl. n°32881/04; on the consent as a basis of the processing see for ex. ECtHR, 3rd Sect., *Perry v. the United Kingdom*, 17 July 2003, appl. n° 63737/00, §46; ECtHR, 4th Sect., *Peck v. the United Kingdom*, 29 January 2003, appl. n° 44647/98, §78; on the right to access see for ex. *Haralambie v. Romania*, *op. cit.*; on the right to rectification see for ex. ECtHR, *Cemalettin Canli v. Turkey*, No. 22427/04, 18 November 2008 and *Handbook on European data protection law*, *op. cit.*, Section 5 p. 103.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

comparison between the GDPR and Directive 95/46/EC, in two respects. Firstly, understanding this mechanism enables to compare the protection granted to the private and to the personal data spheres by fundamental texts, with the protections granted by Directive 95/46/EC and the GDPR, and therefore enables to analyse the differences between the two latter instruments in this respect. Secondly, this mechanism contains in itself the rule that enables to balance the other rights that might be opposed to the protection of private life and/or to the protection of personal data. Indeed, the conditions that must be respected in this regard, and primarily the conditions of necessity and proportionality, will enable to evaluate the extent of the interference and the legitimacy of the third party to cause such interference on the one hand, and the legitimacy of the data subject in relation to his or her expectation of confidentiality and non-intrusion on the other hand. In this sense, the rules for protecting personal data are also rules for limiting the protection of personal data in case this protection is opposed to the exercise of other rights and values such as the freedom of speech, the freedom of scientific research or the preservation of one person's life.

- According to Article 8 para. 2 of the ECHR as interpreted by the ECtHR, and which are to be interpreted narrowly[294], the conditions for limiting the right to private life and/or the right to personal data protection are the following: any interference or limitation of these rights must have a specific, clear, accessible and foreseeable legal basis, must be in conformity with one of the legitimate aims listed in the Convention, must be necessary and must be proportionate to the afore-said aim. The two latter principles of necessity and proportionality are contained in the formula "*necessary in a democratic society for the aforesaid aim*"[295], which implies that the interference, "*in a society that means to remain democratic*"[296], must correspond to a "*pressing social need*"[297], and must be "*proportionate to the legitimate aim*

[294] See for instance ECtHR, ch., 25 February 1993, *Crémieux v. France*, appl. n° 11471/85, §38.
[295] See for instance ECtHR, plen., 26 April 1979, *Sunday Times v. The United Kingdom*, appl. n° 6538/74, § 45, Series A, n° 30.
[296] Joint dissenting opinion of judges Wiarda, Cremona, Thór Vilhjálmsson, Ryssdal, Ganshof van der Meersch, Sir Gerald Fitzmaurice, Bindschedler-Robert, Liesch and Matscher, §8, available under the Sunday Times court case, *op cit.*
[297] ECtHR, *Sunday Times v. The United Kingdom, op cit*, § 59.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

pursued"[298]).

- As regards the definition of "interference" or "limitation", it is constituted as soon as a personal data is accessed or used (or a freedom protected by the wall of private life prevented to be exercised), "*no matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way*"[299], and no matter whether this data is publicly available or not[300].

Legal basis, legitimate aim, necessity and proportionality tests (in other words questions to be answered in order to assess the compliance with the ECHR and the EUCFR requirements of an interference with the right to private life and/or the right to the protection of personal data):

- Is there a clear and precise, adequately accessible, stable and foreseeable legal basis justifying the interference?
  - Clarity and precision must ensure the exclusion of "*obscurity and uncertainty as to the state of the law*"[301], in relation to both the nature and extent of the interference and the "*adequate and effective guarantees against abuse*" that are implemented[302]. These principles therefore ensure the transparency and fairness of the information, which will in turn enable citizens "*to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail*"[303].

[298] ECtHR, *Sunday Times v. The United Kingdom, op cit,* § 63. See also Frédéric Sudre, « La dimension internationale et européenne des libertés et droits fondamentaux », *in Libertés et droits fondamentaux*, under the dir. of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, p. 43; Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 86.

[299] CJEU, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, *op. cit.*, §33.

[300] See for instance Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, WP203, III.2.5, p.35.

[301] . ECtHR, plen., 2 August 1984, *Malone v. the United Kingdom*, appl. n°8691/79, §79; French Constitutional Council, Decision n° 2004-503 DC of 12 August 2004, *op.cit.,* § 29.

[302] ECtHR, plen., 6 September 1978, *Klass and other v. Germany*, appl. n°5029/71, §50; French Constitutional Council, Decision n° 2013-357 QPC of 29 November 2013, *Société Wesgate Charters Ltd*, cons. 8, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2013/2013-357-qpc/decision-n-2013-357-qpc-du-29-novembre-2013.138841.html (last accessed on 28 January 2018).

[303] All quotations are coming from the European Court of Human Rights case *Sunday Times v. The United Kingdom*, *op cit*, § 49. See also Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, page 43; Steve Foster, *Human Rights and Civil Liberties*, 2nd ed., 2008, p. 464.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- "*Physical*"[304] access to the legal basis must be accompanied by an "*intellectual*" [305] access to this legal basis.
- Stability implies no unpredictable[306] and too frequent[307] variations.
- Foreseeability must be ensured through the three previous conditions.

- Does the interference pursue one legitimate aim covered by the ECHR or the EUCFR?
- Is the measure necessary?
  - Is this measure *"seeking to address an issue which, if left unaddressed, may result in harm to or have some detrimental effect on society or a section of society?"* [308]
  - What is this issue or "need", specifically, within the broader sphere of the legitimate aim pursued? (it must be precisely specified)
  - Is there *"any evidence that the measure may mitigate such harm?"*[309]
  - What are the existing measures in place? Why are they no longer sufficient and what will be the added value of the proposed measure?
  - *"What are the broader views (societal, historic or political, etc.) of society on the issue in question?"*[310] and on

[304] Translated from French. Pascal BEAUVAIS, « Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes », *in* ERPC, *Archives de politique criminelle*, éd. A. Pédone, 2007/1 (nº29), p.4, https://www.cairn.info/revue-archives-de-politique-criminelle-2007-1-page-3.htm (last accessed on 28 January 2018).
[305] *Idem.*
[306] ECtHR, 30 July 2015, *Ferreira Santos Pardal v. Portugal*, *op. cit.* §43-49; French Conseil d'État, « Sécurité juridique et complexité du droit », *op. cit.* p. 281.
[307] French Conseil d'État, « Sécurité juridique et complexité du droit », *op. cit.* p. 281. See ECtHR, ch., 16 December 1992, *de Geouffre de la Pradelle v. France*, appl. nº12964/87, §33; Pascal BEAUVAIS, « Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes », *in* ERPC, *Archives de politique criminelle*, éd. A. Pédone, 2007/1 (nº29), pp. 13 and seq., https://www.cairn.info/revue-archives-de-politique-criminelle-2007-1-page-3.htm; Dominique J. M. SOÛLAS de RUSSEL, Philippe RAIMBAULT, « Nature et racines du principe de sécurité juridique : une mise au point », RIDC, 2003, vol. 55, nº1, p. 90, referring to ECtHR, plen., 13 June 1979, *Marckx v. Belgium*, appl. nº6833/74 (URLs last accessed on 28 January 2018).
[308] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.19.
[309] *Ibid.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the proposed measure?

- *Have "any specific views/opposition to"* this issue or measure *"expressed by society been sufficiently taken into account?"*[311]

- Is the measure proportionate?
  - Is the proposed measure strictly necessary to achieve the pursued aim?
    - ✓ Is it appropriate to its context?
      - ❖ Adapted to the severity of the social need, taking into account the specific issue the measure is intended to address and the harm that this issue would cause to society if not addressed;
      - ❖ Adapted to the nature of the behaviour which is being restricted (sensitivity, high expectation of privacy, ability of individuals to adapt their behaviour depending on their age or other particular characteristics...);
    - ✓ Is the scope of the interference sufficiently limited to reach the aim pursued?
      - ❖ Is the scope limited to the strict necessary in terms of severity compared to the severity of the need at stake, of volume of intrusions, of number of people affected, of situations in which the measure can take place, of time during which the measure will be effective…?
      - ❖ Are there exhaustively listed authorised situations of exercise of the interference taking into account its specificities, and in case of positive answer are they respected? For example, certain methods of people surveillance must be limited to serious crimes or to very serious crimes, and personal data processing must be based on the consent of the person concerned or on some other legitimate ground laid

310 *Ibid.*
311 *Ibid.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

down by law.

- ❖ Does the overall effect of the proposed measure leave some scope for the limited freedom?

- ✓ Is the interference, in its nature, the less freedoms-restrictive one? What other measures could be considered, and why are they rejected?

- o Is the measure limited by adequate and effective safeguards?

  - ✓ Which precise safeguards have been scheduled (1) in order to palliate potential weaknesses of findings during the examination of these other steps, and (2) in order to render possible the restrictions decided in the previous steps of the necessity and proportionality tests, including technical (in order for ex. to ensure data deletion after a certain period of time)?

  - ✓ Are these safeguards clearly detailed in a legal basis and in a legal documentation accessible to people whose rights are limited, where information has not been provided individually? Does this information include "*the entire relevant and adequate information*"[312] that will enable to ensure the fairness of the processing, including where relevant the grounds or reasons required for ordering or deciding it, the situations where the measure can take place, the length of the measure, the possible extent of the intrusion in the private life and/or personal data spheres (nature of data collected, number of people concerned, etc.)? Is there any existing internal policy regulating the answer to be provided to persons granting access to this information and to their processed personal data?

  - ✓ Do these safeguards provide for measures that will enable the control of the scheduled

[312] Translated from French, ECtHR, 3rd Sect., *Haralambie v. Romania*; 27 October 2009, appl. n°21737/03, §86 (juged in relation to the access to information). See also *Handbook on European data protection law*, European Union Agency for Fundamental rights and Council of Europe, 2014, 3.4 p. 73, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (last accessed on 21 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

interference limitations, and which ones? (objective authorisation / supervision by a judge or, if relevant, another independent authority; rights of access, of rectification of data granted to concerned individuals; right of these individuals to obtain a copy of their data without having to justify their request; clarification of the procedure to be followed to exercise these rights; right of appeal afforded to individuals; etc.).

- ✓ Do these safeguards include organisational and financial measures aiming at ensuring their practical effectiveness?

- Are the necessity and the proportionality of the proposed measure sufficiently justified?

  In addition, the information substantiating compliance with the principles of necessity and proportionality must be sufficient to convincingly establish the legitimacy of the interference. This principle is so important that the Article 29 Data Protection Working Party considers this question to be a test in itself, in addition to the necessity test and to the proportionality test.[313] Therefore, it may be important to analyse this question independently, to review the quality and relevance of evidences that have been produced (such as "*research, surveys or other information*"[314]).

2.4 - The transcription, in Directive 95/46/EC and in the GDPR, of the interrelations and protection of fundamental rights

The interrelations between rights that have been studied previously in this report as well as the mechanism that ensures their protection has been properly taken into account in the GDPR and in Directive 95/46/EC. As a result, these legal instruments both protect the same sphere of private life

[313] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.27.
[314] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit.*, 3.27. The working party refers to the ECtHR formula: the "*interference must be supported by relevant and sufficient reasons*". See for example ECtHR, 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. n° 62332/00, § 88.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

and other fundamental rights through the protection of processed personal data, and both constitute practical applications of the ECHR and EUCFR requirements.

2.4.1 - The GDPR and Directive 95/46/EC both protect private life and other fundamental rights through the protection of processed personal data

Directive 95/46/EC announces protecting "*the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*"[315], whereas the GDPR outlines that the "*Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*"[316]. As a result, even though the GDPR disconnects the privacy protection and the protection of personal data, the latter statements show that both legal instruments announce to protect (all) "*fundamental rights and freedoms of natural persons*" that might be limited by the processing of personal data.

This has two consequences: the protection of an important number of other fundamental rights beside the right to private life and to the protection of personal data, and the necessity to include both these fundamental rights and the right to personal data protection as assets in data protection impact assessments (DPIA).

2.4.1.1 - The protection of an important number of other fundamental rights beside the right to private life and to the protection of personal data

Fundamental rights and freedoms that might be limited by the processing of personal data are also the fundamental rights that are impacted by an interference with the private data sphere in the most extensive conception of privacy defined as the whole sphere of information and freedoms that surround an individual within the boundaries set up by the ECHR and the EUCFR in order to

[315] Article 1, §1 of Directive 95/46/EC. See also recital n°2 which states that "*data-processing systems are designed to serve man* [and] (...) *must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals*".
[316] Article 1, §2 of the GDPR. See also recital n° 2.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

balance conflicts of fundamental rights (the protected privacy sphere being therefore defined in relation to third parties' rights)[317].

Fundamental rights that might be protected therefore include all the rights of which the full enjoyment implies either a secret exercise (actual or future - which might lead to the right to be forgotten), or an exercise that is particularly protected from external influences or interferences[318].[319] These rights are non-exhaustively the right to image and voice, the right to correspond and of personal communications, the right to establish and develop private relationships and more generally relationships with other human beings, the right of everyone to take decisions at his or her own discretion into his or her zone of private life, the right to the integrity of the person and the prohibition of degrading ill-treatment, the right to liberty and security, the right to conduct a business, the freedom of thought, conscience and religion, the freedom of movement, the freedom of assembly and association, the right to self-determination and personal autonomy, the right to be assessed in the proper light and the right to a fair trial, and the right to personal action and to shape one's own life with minimal outside interference which is protected through different stand-alone rights (such as the freedom of the arts and science, the freedom of expression, the right to education and other cultural rights, the freedom to choose an occupation and the right to property) or through the protection of the general principle of freedom[320].

However, this protection is limited to interferences due to the "*processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*"[321], whereas the ECtHR protects under Article 8 of the ECHR any use of personal data where it impacts private life in its extensive definition, even though

[317] See above the Section 2.2.1.1.5 of the current report.
[318] Without prejudice to the question of whether the way the right is exercised, or the purposes and impacts of such exercise, are legitimate - which might have to be assessed independently, possibly on another legal basis such as the right to freedom and expression and its limits.
[319] See above the Section 2.2.1.2. of the current report.
[320] See above the Section 2.2.2.2 of the current report.
[321] Article 2, 1 of the GDPR; Article 3, 1 of Directive 95/46/EC using a very close wording.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

"*the need for* [...] *safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned*"[322].

2.4.1.2 - The necessity to include both all these fundamental rights and the right to personal data protection as "primary assets" in data protection impact assessments (DPIA)

As a first consequence of the above, data protection impact assessments must include all the fundamental rights that are protected by the personal data sphere as "primary assets", this latter notion corresponding to the elements that need to be protected against risk, in risk management methodologies that are supposed to be used in a DPIA[323]).

This appears to be obvious but is not as clear as it should be when reading the guidelines that are increasingly provided in relation to the carrying out of DPIA, and which reduce either the scope of the protection of personal data, or the scope of the protection of other fundamental rights.

2.4.1.2.1. DPIA are supposed to assess the future impact of an initiative on the right to personal data protection and other fundamental rights

A privacy impact assessment (PIA)[324] has been defined in the PIAF EU project as "*a process for assessing the impacts on privacy of a project (…) or other initiative (...) and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts*"[325]. Roger Clarke defines a PIA as "*a systematic process that identifies and evaluates, from the perspectives of all stakeholders, the potential effects*

[322] ECtHR, gr.ch., 4 December 2008, *S & Marper v. United Kingdom*, appl. n° 30562/04 and 30566/04, §103.
[323] See Estelle De Marco, *Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2 of 11 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications (last accessed on 21 February 2018), Section 4.3.2.
[324] Elements of the current discussion are issued from Estelle De Marco previous research, lastly published in Estelle De Marco, *Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, *op. cit.*, Section 3.1.1.
[325] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.5, available at http://www.piafproject.eu/Deliverables.html (last accessed on 16 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

on privacy of a project, initiative or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts"[326].

A PIA is therefore a tool that targets less the respect of a specific legislation than the respect of general requirements for protecting human rights and freedoms[327], through the assessment and mitigation of the impacts that an initiative can cause on these rights and freedoms. As a consequence, the assessment of these impacts may lead to determine safeguards that are not provided for by law, and even safeguards that aim to palliate the breach of a legal requirement that is difficult to apply in particular circumstances[328].

In these definitions and in most of the other, very close, that have been provided by publications on this subject[329], the notion of "privacy" is largely understood as referring to all the fundamental rights and freedoms that might be impacted by the aforesaid project or initiative, either without particular restriction or reducing the number of the targeted freedoms to those that might be impacted by a privacy and / or a data protection limitation[330].

Since a PIA is supposed to be the assessment of the impacts of an initiative on privacy, understood as covering impacts on all fundamental rights (at least those exercised behind the wall of the private sphere), a DPIA is supposed to consist as well in "*the identification of future consequences of a current or*

---

326 Roger Clarke, *An Evaluation of Privacy Impact Assessment Guidance Documents*, International Data Privacy Law 1, 2 (March 2011) 111-120, available at http://www.rogerclarke.com/DV/PIAG-Eval.html (last accessed on 16 February 2018).

327 See for instance Roger Clarke, *Privacy Impact Assessments*, 19 April 1999, last update on 26 May 2003, available at http://www.rogerclarke.com/DV/PIA.html (last accessed on 16 February 2018): "*A PIA (…) considers the impacts of a proposed action, and is not constrained by questions of whether the action is already authorised by law. Moreover, to the extent that relevant codes or standards exist, it does not merely accept them, but considers whether they address the public's needs*".

328 Which might for example be the case of the principle of data minimisation, within the framework of a project aiming at performing big data analysis.

329 See for ex. David Wright and Paul De Hert, "Introduction to Privacy Impact Assessment*", in* David Wright and Paul De Hert, *Privacy Impact Assessment*, Law, Governance and Technology Series volume 6, Springer, 2012, pp. 3 *et seq.*, in particular pp. 5 *et seq.*

330 See for example Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, *op. cit.*, p. 14; Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", *in* David Wright and Paul De Hert, *Privacy Impact Assessment*, Law, Governance and Technology Series volume 6, Springer, 2012, pp. 33 *et seq.*; Colin Bennett's, *In Defence of Privacy*, Surveillance & Society, Vol. 8, No. 4, 2011, pp. 485–496, mentioned by Gary T. Marx, *Privacy Is Not Quite Like the Weather*, *in* David Wright and Paul De Hert, *Privacy Impact Assessment*, *op. cit.*, foreword p. vi.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

proposed action"[331] on the right to personal data protection, understood as covering all fundamental rights (at least those exercised on the basis of a processing of personal data and those being likely to be limited because of such a processing[332] - and more widely, since we have analysed that the personal data sphere is perfectly included in the private sphere in the most extensive definition of privacy[333] - at least those exercised in the private sphere).

2.4.1.2.2. Reduction of the scope of the protection of personal data

However, most of the definitions that have been given of a DPIA reduce the analysis to the impacts of the data processing operations at stake, without taking into account the whole initiative that includes this processing, and without considering the necessity to assess initiatives that do not consist in a personal data processing but that could have an impact on the right to personal data protection.

Indeed, a data protection impact assessment (DPIA) has been defined by the European Commission as "*a systematic process for evaluating the potential impact of risks where processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*"[334]. More recently, the Article 29 working party defined a DPIA as "*a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to*

[331] This formula corresponds to the definition given to an impact assessment by the International Association for Impact Assessment (IAIA): see Roger Clarke, *Privacy Impact Assessments*, 19 April 1999, last update on 26 May 2003, available at http://www.rogerclarke.com/DV/PIA.html (last accessed on 16 February 2018), "Origins and definition".

[332] Such as, for example, the right to freedom of movement, the right to liberty and security, the right to presumption of innocence and to a fair trial, the right to freedom of expression, the right to freedom of assembly and the right to non-discrimination. See the MANDOLA deliverable D2.2 - *Identification and analysis of the legal and ethical framework*, *op. cit.*

[333] See above, the Section 2.2.2.1 of the current report.

[334] EC recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU), §I, 3 (c), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF (last accessed on 22 February 2018). The Article 29 Data Protection Working Party supports this definition: see Article 29 Data Protection Working Party, *Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205)*, adopted on 22 April 2013, p. 7.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

address them)"[335]. Once again, in these definitions the notion of "risks" is understood as risks for privacy and personal data protection, covering other fundamental rights[336].

It seems that this interpretation is not the most appropriate one, since it harms the protection of personal data themselves, by ignoring the initiatives that could lead to an interference with the right to the protection of personal data without being themselves personal data processing[337]. Even though it would be impractical to request from any individual to assess the impacts or their day-to-day initiatives on the protection of third parties' fundamental rights (keeping in mind that the essence of privacy impact assessments is precisely to enable such assessment on a voluntary basis, any impact being likely to be sanctioned under the general civil liability regime in most countries[338]), it seems that it would be wise to include at least, in a DPIA, the assessment of risks posed by the context of the assessed personal data processing operation, in order both to remain committed to the notion of PIA and to protect adequately citizens' fundamental rights.

The GDPR does not necessarily contradict such an approach, since even though it considers in its Article 35 that a DPIA is the assessment of the "*impact of the envisaged processing operations*", this must be done taking into account "*the nature, scope, context and purposes of the processing*" - which means that the

---

[335] Article 29 Data Protection working party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248, 4 April 2017, p. 4, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 21 February 2018).

[336] See for example CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, p. 3, https://www.cnil.fr/fr/node/15798 (last accessed on 21 February 2018): "*the term "privacy" is used as shorthand to refer to all fundamental rights and freedoms (including those mentioned in Articles 7 and 8 of the [EUCharter], Article 1 of the [Directive-95-46] and the Article 1 of the [DP-Act]: "human identity, human rights, privacy, or individual or public liberties*"); Article 35 of the GDPR evokes the "risk to the rights and freedoms of natural persons".

[337] For example, the processing of simulated data, therefore of non-personal data, may lead to the creation of false information that might be linked to a real existing person, by coincidence; as another example, the initiative to develop a data processing that enables citizens to report penal infringements online through a smartphone application, accompanied by information on statistics relating to online illegal behaviours and on how to behave where facing an online illegal content, would be assessed under this definition in relation to the risks posed by the processing of personal data. However, the accompanying information itself might impact the right to the protection of personal data and other rights, since it might for example mislead on the way to behave where a potentially illegal content is found, and therefore lead the user to write information online or to report information to the system or elsewhere, in other words to create information that will be processed but that would not have been processed in case he or she would not have been misled.

[338] Estelle De Marco *et. al.*, *Deliverable D2.2 – Identification and analysis of the legal and ethical framework*, MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n° JUST/2014/RRAC/AG/HATE/6652, version 2.2.4 of July 2017, http://mandola-project.eu/publications/ (last accessed on 21 February 2018), Section 4.3.3.2, footnote n°349.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

GDPR commands to assess the impacts of the processing operations having regards to its whole context, which might for example lead to process data that were not intended to be processed, due to a project misuse. This leads to extend the scope of the assessment to the impacts on fundamental rights of any project, system or initiative that includes a personal data processing (and even a non-personal data processing where personal data are likely to be included in it), as soon as assessed elements are likely to influence the nature, the content or the scope of this data processing.

In the same line, some legal authors consider a DPIA as being "*an instrument to identify and analyse risks for individuals, which exist due to the use of a certain technology or system by an organization in their various roles (as citizens, customers, patients, etc.). On the basis of the outcome of the analysis, the appropriate measures to remedy the risks should be chosen and implemented*"[339].

In the latter an approach, a PIA and a DPIA can be considered as equivalent terms, but their meaning go beyond the definitions provided by the European Commission and the Article 29 data protection working party. However, this does not seem to be decisive criteria, in the light of the confusion that exists in relation to the notion of DPIA. Indeed, some data protection authorities consider themselves that the terms of PIA and DPIA are interchangeable[340], while they - at the same time - further reduce the scope of the assessment (and therefore of the protection) to the risks posed to processed personal data (and not to the right to the protection of personal data more generally, including or not including other fundamental rights).

---

339 Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost, "A Process for Data Protection Impact Assessment under the European General Data Protection Regulation", *in* K. Rannenberg and D. Ikonomou, *Privacy Technologies and Policy*, Fourth Annual Privacy Forum, APF 2016 Frankfurt. Heidelberg, New York, Dordrecht, London, available at http://www.springer.com/cda/content/document/cda_downloaddocument/9783319447599-c2.pdf?SGWID=0-0-45-1587701-p180200777 (last accessed on 21 February 2018).

340 See for ex. CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, p. 3, https://www.cnil.fr/fr/node/15798 (last accessed on 21 February 2018): "*the acronym "PIA" is used interchangeably to refer to Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA)*"; Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), 4 April 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 21 February 2018), p. 4: "*Note: the term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept*".

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2.4.1.2.3. Cumulative reduction of the scope of the protection of other fundamental rights

Some DPIA methods limit the risk analysis to the risks posed to the personal data that are processed, in practice, considering that the impacts on fundamental rights will only be due to an impact first suffered by one of the personal data that are processed[341]. This approach reduces drastically the scope of the DPIA, and prevents the identification of risks for freedoms that will be due to a correct use (as scheduled in compliance with the GDPR) of the processed data. This approach seems therefore to not comply with the GDPR requirements.

2.4.1.2.4. Conclusion on the primary assets to be included in a DPIA

As a result of the above, primary assets - in other words the elements to be prevented from risks - to be taken into account in a DPIA are the personal data that are processed and the citizens' fundamental rights that might be impacted by the data processing taking into account all its elements of context that can influence this processing. Since among these fundamental rights lies the right to personal data protection itself, the analysis would not be comprehensive without also analysing the risks that might be posed to compliance with the GDPR itself.

Compliance points with the GDPR must therefore also be included in the primary assets. This is confirmed by Article 35 of the GDPR which states that a DPIA must contain at least[342] "*the measures envisaged to address the risks, including safeguards, security measures and mechanisms* ***to ensure the protection of personal data and to demonstrate compliance with this Regulation*** *taking into account the rights and legitimate interests of data subjects and other persons concerned"*. This is also confirmed in recital n°84[343] and in Article 5 para. 2[344] of the GDPR. Addressing the risks to freedoms with measures that include the demonstration of the compliance with the GDPR implies that this compliance is ensured, and

---

341 See CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, *op. cit.* p. 6.

342 In relation to the content of a DPIA, see below our Section 3.7.3.5.

343 Recital n°84 states "*The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation*".

344 Article 5, 2 of the GDPR states that the controller is responsible for, and must be able to demonstrate compliance with, the fundamental principles for processing personal data recalled in Annex of the current report (principle of accountability).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

therefore that the risks of non-compliance are under control, which cannot take place without a proper assessment of risks targeting precisely such compliance, not only in terms of data unlawful destruction, alteration and access, but also in relation to the other data controllers' obligations.

2.4.2 - The GDPR and Directive 95/46/EC both constitute practical applications of the ECHR and EUCFR requirements

In addition to protect the same fundamental rights, both the GDPR and Directive 95/46/EC apply the same mechanism of protection, which is the one that has been adopted at the ECHR level in order to protect private life, and which has been reaffirmed in the EUCFR.

Indeed, Directive 95/46/EC and the GPDR, in their respective first recital, refer primarily to and apply the fundamental rights protection mechanisms proposed in the ECHR (as regards Directive 95/46/EC[345]) and in the EUCFR (as regards the GDPR[346]). This could appear as an important difference whereas it is not, since we have already analysed[347] that both the ECHR and the EUCFR offer to privacy and to personal data an equal protection.

As a result, the provisions of both legal instruments (1) are the result of the application of the ECHR and EUCFR requirements; (2) refer to the need to apply the ECHR and EUCFR requirements where processing operations are going beyond a certain number of precise expectations, and (3) refer to the need to apply the ECHR and EUCFR requirements where the right to the protection of personal data must be balanced with opposed rights and interests.

[345] Directive 95/46/EC, Recital n° 1.
[346] GDPR, Recital n° 1. However, Recital n° 41 does also refer to the ECtHR court cases and Recital n° 73 calls to carry out an evaluation of certain notions in the light of the ECHR.
[347] See above the Section 2.3.1. of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2.4.2.1 - The provisions of both legal instruments are the result of the application of the ECHR and EUCFR requirements

The provisions of the GDPR and of the Directive constitute practical applications of the ECHR and EUCFR principles. Indeed:

- Both legal instruments constitute a legal basis that authorises most processing operations: this legal basis (which appears more detailed and therefore clearer within the framework of the EU reform) aims to ensure foreseeability of processing operations for data subjects and to detail the safeguards that must be implemented in relation to data processing operations.

  This legal basis emphasises the responsibility of the data controller to further ensure the fairness of processing operations[348], which - as we analysed it previously - contributes both to the existence of a foreseeable legal basis[349] and to the proportionality[350] of processing operations. Fairness is moreover explicitly defined in Directive 95/46/EC as the prohibition of secrecy and the requirement of comprehensive information[351], and the meaning of the principle doesn't seem to have changed in the GDPR.

- Both legal instruments require the pursuit of a legitimate aim, which is crystallised in the notion of "legitimate" purposes[352], referring to a specific social need[353] that must be more largely included in one of the legitimate aims[354] authorised by the ECHR and the EUCFR.

- Both legal instruments authorise only processing operations that are necessary: the pressing social need required in the ECHR and the EUCFR[355] is required under the term "purposes" under the

[348] Article 5, 1, a of the GDPR; Article 6, 1, a of Directive 95/46/EC.
[349] See above, Section 2.3.2.1.1 of the current report.
[350] See above, Section 2.3.2.4.2 of the current report.
[351] See Recital 38 to Directive 95/46/EC and the last § of Article 10 of the Directive. See also Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), §34. For further developments on the principle of fairness, see the Annex of the current report, Section 1.2.
[352] Article 5, 1, b of the GDPR; Article 6, 1, b of Directive 95/46/EC.
[353] See above, Section 2.3.2.3.1 of the current report.
[354] See above, Section 2.3.2.2 of the current report.
[355] See above, Section 2.3.2.3.1 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

GDPR and Directive 95/46/EC[356]. These purposes must be "specified", "explicit" and compatible with previous processing operations. Only processing operations that enable to reach these purposes (as required by the ECHR and the EUCFR[357]) are authorised, through a series of requirements whose exact content must be determined in the light of these purposes, such as the requirement of adequation and relevance of processed data[358], and the requirement of accuracy and up-to-datedness of data[359].

- Both legal instruments endeavour to enforce the proportionality of processing operations. Indeed, a large number of provisions intend to confine processing operations to the strict necessary to the pursuit of specified purposes, both by commanding such limitation and by organising the implementation of a series of safeguards that aim to enforce these restrictions.
    - In relation to limitations, main ones are the conditions surrounding data subjects' consent[360], the principles of data minimisation[361] and of time limitation[362], the prohibition to process special categories of data[363], the rights of the data subjects[364], the obligation of confidentiality and security[365],

      In addition, the GDPR and the Directive 95/46/EC list restrictively a series of situations in which processing operations are authorised. These situations, named "legitimate grounds" under the Directive 95/46/EC[366] and "legal grounds" under the GDPR[367] are actually a list of purposes that are more specific than the "legitimate aim" required by the ECHR and the

356 Article 5, 1, b of the GDPR; Article 6, 1, b of Directive 95/46/EC.
357 See above, Section 2.3.2.3.2 of the current report.
358 Article 5, 1, c of the GDPR; Article 6, 1, c of Directive 95/46/EC.
359 Article 5, 1, d of the GDPR; Article 6, 1, d of Directive 95/46/EC.
360 Articles 4, 11 and 7 of the GDPR and Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 28 November 2017 (WP259); Article 2, h of Directive 95/46/EC and Article 29 data protection Working Party, *Opinion 15/2011 on the definition of consent*, 13 July 2011 (WP187).
361 Article 5, 1, c of the GDPR; Article 6, 1, c of Directive 95/46/EC.
362 Article 5, 1, e of the GDPR; Article 6, 1, e of Directive 95/46/EC.
363 Articles 9 and 10 of the GDPR; Article 8 of Directive 95/46/EC.
364 Articles 12 to 22 of the GDPR; Articles 10 to 12, 14, 15 of Directive 95/46/EC.
365 Articles 32 to 34 of the GDPR; Articles 16 and 17 of Directive 95/46/EC.
366 "Legitimate" being a word used in the title of Section II of Directive 95/46/EC.
367 "Lawfulness of processing" being the title of Article 6 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

EUCFR[368], but that are broader than the specific need to be identified during the necessity test (which corresponds to the specific purpose of the processing under the GDPR and Directive 95/46/EC)[369], and which may be bypassed in case the data subject gives his or her consent.

- In relation to safeguards, main ones are the obligation of the data controller to either notify the processing to the data protection Authority[370] or to pre-establish evidences of his or her respect of the legislation[371], the power of supervisions granted more generally to data protection authorities[372], the requirement of existing remedies and sanctions[373], the designation of a data protection officer[374], the safeguards to be implemented in certain cases of data transfers[375] and the support of codes of conduct[376] and of certification mechanisms[377].

2.4.2.2 - The provisions of both legal instruments refer to the need for a new legal basis or for additional necessity and proportionality tests where processing operations are going beyond a certain number of precise expectations

Beside their specific requirements, both the GDPR and Directive 95/46/EC regulate the situations where data processing operations cannot be framed by typical safeguards and therefore pose a higher level of risks for the rights and freedoms of individuals than data processing that can stay within the boundaries of these typical safeguards. In these situations, the GDPR commands the adoption of a new legal basis, and/or the carrying out of specific necessity and proportionality tests in order to identify the alternative or complementary safeguards that are specifically needed.

368 See above, the Section 2.3.2.2 of the current report.
369 See above, the Section 2.3.2.3.1 of the current report.
370 Articles 18 to 20 of Directive 95/46/EC.
371 Articles 24, 30 of the GDPR.
372 Articles 31, 36 and 51 *et seq.* of the GDPR; Articles 20, 21 and 28 of Directive 95/46/EC.
373 Articles 77 to 82 of the GDPR; Articles 22 to 24 of Directive 95/46/EC.
374 Article 37 to 39 of the GDPR; Articles 25 *et seq.* of Directive 95/46/EC.
375 Articles 44 *et seq.* of the GDPR; Articles 25 and 26 of Directive 95/46/EC.
376 Article 41 of the GDPR; Article 27 of Directive 95/46/EC.
377 Articles 42 and 43 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

In that respect, the compatibility test that is required in case personal data are further processed for the same purpose or another one implies the carrying out of a proportionality test[378]. The test of legitimate interest, which must be carried out by data controllers who do not obtain the consent of data subjects and who do not justify one of the other legitimate grounds set out in Article 6 of the GDPR[379], contains a necessity test and a proportionality test, along with a risk analysis targeting the impact of the data processing on the rights and freedoms[380]. Privacy impact assessments that become mandatory under the GDPR also include explicitly a necessity and a proportionality test[381].

In the same line, the situations in which processing operations are authorised under the GDPR and Directive 95/46/EC (which are actually a list of purposes that are more specific than the "legitimate aim" required by the ECHR and the EUCFR, but broader than the specific need to be identified during the necessity test which is the processing specific purpose[382], and which may be bypassed in case the data subject gives his or her consent) can only serve as legal grounds[383] or legitimate grounds[384] for processing operations if these operations are "necessary" to achieve them, this term of "necessity" referring once again to the necessity and proportionality tests proposed by the ECtHR[385].

---

[378] See below the Annex to the current report, Section 2.4.2, and Article 6, 4 of the GDPR; See also Estelle De Marco *et. al.*, *Deliverable D2.2 – Identification and analysis of the legal and ethical framework*, MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n° JUST/2014/RRAC/AG/HATE/6652, version 2.2.4 of July 2017, http://mandola-project.eu/publications/ (last accessed on 21 February 2018), Section 4.2.3.3.2.

[379] Article 7 of Directive 95/45/EC.

[380] See Estelle De Marco *et. al.*, *Deliverable D2.2 – Identification and analysis of the legal and ethical framework*, *op. cit.,* Section 4.2.3.3.6; Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217)*, 9 April 2014; recital n°47 of the GDPR.

[381] Article 35 of the GDPR. These tests were already included in privacy impact assessments (which were an ethical action): see Estelle De Marco, *MANDOLA Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2 of 11 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 3.1 (last accessed on 24 January 2018).

[382] See above, Section 2.4.2.1 of the current report.

[383] Under the GDPR, "lawfulness of processing" being the title of Article 6.

[384] "Legitimate" being a word used in the title of Section II of Directive 95/46/EC.

[385] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), 9 April 2014, Section II, 1 (to be read in conjunction with Section III.1.1): "*Article 8 ECHR focuses on the protection of private life, and requires justification for any interference with privacy. This approach is based on a general prohibition of interference with the right of privacy and allows exceptions only under strictly defined conditions. In cases where there is 'interference with privacy' a legal basis is required, as well as the specification of a legitimate purpose as a precondition to assess the necessity of the interference* [editor note: the Article 29 Working Party evoking here both the principles of necessity

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Indeed, where one of these grounds are used, the processing operations do not respect the principle of data subject's consent, and therefore present higher risks for the rights and freedoms of natural persons than those that are authorised by people concerned. Moreover, some of these grounds must themselves be the result of a specific legal basis that organise them in the respect of the principles of necessity and proportionality[386].

In addition, the GDPR[387] and Directive 95/46/EC[388] require that the information provided to data subjects by data controllers is adapted to the particularities of the processing operations[389], with the aim of providing the "necessary" information that will ensure "fair" processing.

2.4.2.3 - The provisions of both legal instruments refer to the application of the ECHR and EUCFR protection mechanism where the right to the protection of personal data must be balanced with opposed rights and interests

Finally, the GDPR and Directive 95/46/EC authorise a series of exceptions to the data protection they organise, with the aim of protecting opposed interests such as State security or the preservation of life, or with the aim of protecting opposed fundamental rights such as the freedom of expression and the freedom of the press.

- Processing operations that are necessary to safeguard a list of interests including national security and the protection of rights and freedoms of individuals may not be subject to some data protection requirements under the conditions that they are authorised by a specific legal basis ensuring necessity and a proportionality, according to Article 23 of the GDPR and Article

---

and proportionality, see on this issue our Section 2.3.2.5]. *This approach explains that the ECHR does not provide for a list of possible legal grounds but concentrates on the necessity of a legal basis, and on the conditions this legal basis should meet*".

386 See article 6, 3 of the GDPR referring to processing necessary for compliance with a legal obligation to which the controller is subject or necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This clarification does not appear in Directive 95/46/EC but is inherent to the respect, by Member States, of their obligations under the ECHR and the EUCFR.

387 Articles 13 and 14 of the GDPR.

388 Articles 10 and 11 of Directive 95/45/EC.

389 The GDPR creates however a literal limitation of the information to be provided to data subjects (which should be bypassed by a reading in the light of the ECHR transparency principle), since the wording of Article 13 and 14 does not refer anymore to the possibility to provide not-listed information: see below the Section 3.8 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

13 of Directive 95/46/EC. Article 23 of the GDPR adds that "*the essence of the fundamental rights and freedoms*" must be respected, which emphasises the importance of a strict respect of the steps of the lawfulness, necessity and proportionality tests[390].

- One of these interests regulated in Article 13 of the Directive is in the GDPR the subject of a separate provision, Article 89. Based on these two latter provisions, processing operations that are necessary for "*scientific or historical research purposes or statistical purposes*"[391], in addition to "*archiving purposes in the public interest*"[392] which is added by the GDPR, may not be subject to the respect of a series of data protection requirements under the same conditions of performing a necessity and a proportionality test including the implementation of appropriate safeguards[393], and of being authorised by a specific legal basis[394].

- More precisely in relation to the rights and freedoms that might be opposed to the right to the protection of personal data, some provisions of the GDPR and of the Directive identify explicitly a list of rights which exercise may exclude the application of a series of data protection requirements, such as freedom of expression[395], public access to official documents[396], employment[397], freedom of thought and religion[398] (the GDPR regulating specifically, in addition, the processing of the national identification number[399]). Here again, these derogations must be provided for by law and respect the essence of the necessity and proportionality principles, even though all these provisions do not name all these requirements (since these are general requirements developed in Articles 23 and 13 mentioned in our first point above), each of them emphasising on those of these requirements that need to be particularly secured within

390 See above the Section 2.3 of the current report and the summary of this Section 2.3.
391 Article 13 of Directive 95/45/EC. See also Articles 6§1, b and e and 11 of this Directive.
392 Article 89 of the GDPR. See also Articles 5; 9; 14§5 and 17§3 of the GDPR.
393 See the two preceding footnotes.
394 Article 89 of the GDPR; Article 13, 2 of Directive 95/46/EC; implicit in Article 6, 1, e of the same Directive (Member States having the obligation to "lay down" appropriate safeguards).
395 Article 85 of the GDPR; Article 9 of Directive 95/45/EC.
396 Article 86 of the GDPR; Articles 18§3; 21§3al.2, 26§1(f) of Directive 95/45/EC.
397 Article 88 of the GDPR; Article 8§2, b) of Directive 95/45/EC.
398 Article 91 of the GDPR; Article 8§2, d) of Directive 95/45/EC.
399 Article 87 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the framework of the opposed right they regulate.

- Finally, opposed interests and rights are not all explicitly included in the above-mentioned provisions, and might be named only in the list of possible exceptions that are specific to each data protection obligation. For example, the prohibition of the processing of special categories of data may only be bypassed where the processing is "necessary" to pursue several important listed objectives which have already been mentioned such as the carrying out of obligations in the field of employment law, some case of exercise of the freedom of thought or of assembly, and the right to information or to defend one's own case in justice, but they may also be subject to exceptions where there is a need to preserve the vital interests of the data subject or to exercise preventive medicine[400]. The notion of "necessity" refers here also to the principles of necessity and proportionality[401], including the identification of appropriate safeguards (which are in some cases explicitly required by the GDPR and Directive 95/46/EC) in an appropriate legal basis.

Since Article 23 of the GDPR and Article 13 of Directive 95/46/EC evoke the possibility to establish derogations in the large context of the protection of rights of others, all these apparent differences of treatment between rights on the one hand and between the GDPR and Directive 95/46/EC on the second hand are not of utmost importance (and such a complexity was perhaps not necessary) since, at the end, each situation requires the application of a very simple rule which is to respect in details the principles of legal basis, of legitimate aim, of necessity and of proportionality as we analysed it previously in the current report[402].

2.4.3 - Conclusion of Section 2.4

The previous analyses suggest that there are only few substantive differences between the GDPR and Directive 95/46/EC, most of the variations consisting actually in the GDPR of clarifications that

[400] Article 9 of the GDPR; Article 8 of Directive 95/45/EC.
[401] See especially the Sections 2.4.2.1 and 2.3.2.5 of the current report.
[402] See above the Section 2.3.2 of the current report. See also recital 4 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

leave less flexibility as to how the rule must be interpreted (preventing some literal interpretations that would not take into account the ECHR and the EUCFR requirements) or that leave less flexibility as to how the rule must be applied (in relation to choices that are available in order to enforce the principles of necessity and of proportionality in given situations). Most of the latter differences, which become substantive differences in their details where the options that enable to ensure proportionality are reduced, might however be circumvented in case a given specific rule of the GDPR cannot be applied, which might for example occur in the big data area[403], through the carrying out of novel necessity and proportionality tests, possibly under the supervision of the relevant data protection authority as Article 35 para. 11 of the GDPR foresees it in a DPIA context.

This conclusion therefore shows that compliance with the GDPR is not supposed to be a difficult step for data controllers who previously complied with Directive 95/46/EC understood as a practical application of the ECHR and EUCFR principles, in other words who had already an "ethical" approach (in the sense of legal ethics[404]) of this data protection legislation, at the exception of the obligation to constitute "prima facie" evidences of the respect of the legislation (other than the performance of a necessity and proportionality test), which replaces in the GDPR the previous obligation to notify data processing to the data protection authority. This will be analysed in more details in the following Section.

[403] Big data techniques might indeed be very difficult to reconcile with some data protection principles such as data minimisation and even collection for determined and specific purposes.

[404] Legal ethics might be defined as "*the ethical principles underlying laws*" (translated from French: Leslie Sheinman, "Ethique juridique et déontologie", Droit et Société N°36-37/1997, pp. 265-275, available at http://www.persee.fr/doc/dreso_0769-3362_1997_num_36_1_1408 - last accessed on 24 February 2018): the intention is to refer to the legislator's spirit, even further to the value system and to the philosophy underlying the legal system (Jean-Claude Rocher, *Aux sources de l'éthique juridique - Les présocratiques*, June 2001, ed. Fac 2000, coll. Reflechir, especially pp. 11-13), and not only to the letter of the legal text. In this sense, ethics "*establishes itself as the natural complement of the conceptualisation of law*" (ibid p.12). This leads to interpret the concept of respect for fundamental rights in a protective manner for the individual, taking into account the ECtHR requirements, which must be interpreted in a restrictive way (on this last requirement see above the Section 2.3.2 of the current report).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

3. Comparative analysis between the GDPR and Directive 95/46/EC

The comparative analysis between the provisions of the GDPR and Directive 95/46/EC shows small differences of substance, which might however be important in terms of impact. They especially relate to the territorial scope of the protection, to the scope of the security to be ensured, and to data controllers liability and accountability. The other modifications consist mainly of clarifications with a view to enforcing the ECHR and EUCFR principles of necessity and proportionality[405], such clarification being already accessible through an ethical approach[406] of the Directive 95/46/EC including the applications of the Article 29 working party's opinion in that field[407].

3.1 Definitions

In relation to definitions, The GDPR follows the definitions laid down in Directive 95/46/EC, clarifying and detailing them, and adds new ones.

The definitions of personal data, of data subject, of processing, of filing system, of controller, of processor, of third party, of recipient and of data subjects' consent are indeed the same, most of the time a bit more detailed without bringing changes to their meaning or scope.

In particular, the definition of data subject consent receives the clarification that the consent must be "*unambiguous*" and indicated through a "*statement*" or a "*clear affirmative action*", which were however

[405] See above, the Section 2.4.3 of the current report.
[406] See above, the Sections 2.3.2.3 and 2.3.2.4 of the current report.
[407] See for example Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, (WP 203); *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (WP 211); *Opinion 15/2011 on the definition of consent* (WP187); *Opinion on the use of location data with a view to providing value-added services*, November 2005, WP 115; *Opinion 2/2010 on online behavioural advertising*, 22 June 2010, WP 171; *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217); *Opinion 13/2011 on Geolocation services on smart mobile devices* (WP 185), 16 May 2011; *Opinion 1/2010 on the concepts of "controller" and "processor"*, 16 February 2010.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

already principles to be applied within the framework of Directive 95/46/EC[408]. In addition, the GDPR details the form of the consent in order to ensure that it valid and *inter alia* freely given, in its Articles 7 and 8[409].

Finally, the GDPR adds several definitions that were not existing in Directive 95/46/EC, those of restriction of processing, of profiling, of pseudonymisation, of personal data breach, of biometric data, of genetic data, of data concerning health, of main establishment, of representative, of enterprise, of "group of undertakings", of binding corporate rules, of supervisory authority, of supervisory authority concerned, of cross-border processing, of relevant and reasoned objection, of information society service and of international organisation.

3.2 Material and territorial scopes of the protection

The material scope of the protection does not differ between the GDPR and Directive 95/46/EC, at least literally, while the territorial scope of the protection has been modified.

3.2.1 Material scope of the protection

Literally, the material scope of the protection does not differ between the GDPR and Directive 95/46/EC, apart a difference of pure form in writing the exceptions. In practice, a difference lies in the fact that Directive was often applying to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties while, under the EU reform, these files will be subject to the respect of Directive 2016/680.

[408] The word "unambiguous" was mentioned in Article 7a and it was agreed that consent could be expressed in different ways but through a positive act: see Article 29 Working Party, *Opinion 15/2011 on the definition of consent* (WP187), II.3 p. 10.
[409] See below the Section 3.4 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Literally, the material scope of the protection does not differ since both legal instruments apply to "*the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*"[410]. Both instruments exclude from their scope the processing of personal data "*by a natural person in the course of a purely personal or household activity*"[411] and "*in the course of an activity which falls outside the scope of Union law*"[412]. One difference between texts, which appears to be of pure form, is that Directive 95/46/EC gives examples of these latter activities[413] while the GDPR excludes in addition, expressly, some of the same activities[414].

In practice, however, the exclusion from the GDPR of processing of personal data "*by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*" will be effective since these very activities will be regulated by Directive 2016/680, whereas it is relative under Directive 95/46/EC. Indeed, the only instrument targeting police and judiciary processing at the EU level is currently the Council Framework Decision 2008/977/JHA of 27 November 2008, which material scope is restricted to transborder data processing for the purposes of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty. Since these files are supposed to respect the ECHR and EUCFR principles together with recommendation R. (87)15 of the Committee of Ministers of the Council of Europe[415], it has been noticed that "*in most*

410 Article 2§1 of the GDPR; Article 3§1 of Directive 95/46/EC states the same with a very thin difference of wording, of pure form.
411 Article 2§2, c) of the GDPR; Article 3§2 point 2 of Directive 95/46/EC.
412 Article 2§2, a) of the GDPR; Article 3§2 point 1 of Directive 95/46/EC which refer to the scope of "Community law which has the same meaning..
413 Article 3§2 point 1 of Directive 95/46/EC: activities "provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law".
414 Article 2§2, b) and d) of the GDPR, which excludes expressly data processing "by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU" and "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".
415 This recommendation is not formally binding for the countries that are parties to the ECHR. However, the Committee of Ministers recommendations are related to actions required to further the aim of the Council of Europe

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Member States the scope of the implementing legislation is wider than the directive (95/46/EC) itself requires and does not exclude data processing for the purpose of law enforcement"[416]. This is for example the case in France[417].

For the rest, the GDPR recalls that the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data are regulated by Regulation (EC) 45/2001, and states that the latter regulation, as well as other Union legal acts applicable to such processing of personal data, "*shall be adapted to the principles and rules*" of the GDPR[418], while evoking a possible future reform of these rules in order to ensure "*uniform and consistent protection of natural persons*"[419]. The GDPR also recalls that it does not "*prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive*"[420].

3.2.1 Territorial scope of the protection

Directive 95/46/EC and the relevant domestic law that implements it only apply where the data controller is established on the territory of the concerned Member State, where the controller is established in a country where the law of the concerned State applies by virtue of international law, and where this controller is not established on the EU territory but processes personal data using an equipment located on the territory of the afore-mentioned Member State[421], which is the case where

---

and the European Convention on Human Right. In this sense, Member States that took the commitment to respect the ECHR should follow the Committee of Ministers recommendations. See the statute of the Council of Europe (available at http://conventions.coe.int/Treaty/EN/Treaties/Html/001.htm - last accessed on 21 February 2018), and Alexandre-Charles Kiss, *Annuaire français du droit international*, Year 1960, Volume 6, pp. 755-773, notably pp. 765 and 766.

[416] Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005) 475 final, 19 December 2005, §4, available at http://www.statewatch.org/news/2006/sep/eu-com-dp-edps-opinion.pdf (last accessed on 21 February 2018).

[417] Law n° 78-17 of 6 January 1978 (modified) also applies to law enforcement activities.

[418] Article 2§3 of the GDPR.

[419] Article 98 of the GDPR.

[420] Article 2§4 of the GDPR.

[421] Article 4 of Directive 95/46/EC.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

this controller uses calculating facilities, java scripts, or cookies on the user's terminal located in the concerned Member State to store and retrieve personal data[422].

This territorial scope of the protection is modified in the GDPR[423]. The latter still applies to data controllers who are established in the EU (regardless of whether the processing takes place in the EU or not) and to those who are not established in the EU but in a place where Member State law applies by virtue of public international law, but in relation to data controllers who are not established in the EU it abandons the criteria of the "place of processing", which has no incidence anymore, and replaces it - within the framework of the pursuit of certain purposes - with the criteria of data origins. As a result, the Regulation applies "*to the processing of personal data of data subjects who are in the Union*", where "*the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union*".

This latter criterion of application of the GDPR appears to be a good protective measure for citizens within the EU, and it seems more appropriate that the "processing" criteria which did not have necessarily logical links with the origin of processed data. However, we can regret its restriction to goods, services and monitoring activities, since the other activities will in the future not be subject to the application of the GDPR, even though processing operations take place in the EU.

3.3 Data, purpose and data processing qualities

Both in the GDPR and the Directive 95/46/EC, the requirement of data and data processing qualities is divided into three main principles: the principle of quality of data processing, the principle of specified, explicit and legitimate purpose and the principle of data quality. The GDPR does not bring substantive changes on this field taking into account previous requirements that had to be read

[422] Data Protection Working Party, Opinion 8/2010 on applicable law, 16 December 2010, WP179.
[423] Article 3 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

in the light of the ECHR and EUCFR principles[424], but only clarifies some of them, such as the need to ensure data processing transparency.

3.3.1 Qualities of data processing

The GDPR[425] embodies the principles of fairness and lawfulness of the processing of personal data that was already lying in Directive 95/46/EC[426], without modifying their meaning[427]. The GDPR adds a principle of transparency, which complements the principle of fairness (which requires the provision of complete information), with a requirement of clarity of this information (it must be easily accessible, easy to understand, clear and in plain language[428], which enables inter alia to reinforce the obligation of the data controllers to clearly indicate to data subjects which data are required and which are not in the light of the purposes that are pursued, among the data that are requested[429]). However, this principle of transparency was already latent in Directive 95/46/EC, both on the basis of the ECHR and EUCFR principles[430] than on the basis of the analysis of the Article 29 Working party[431], along with the concept of predictability[432] (which has for its part not been included in the GDPR even though foreseeability is evoked in Recital n°41 of the latter).

[424] See above the Sections 2.3.2.1.1, 2.3.2.4.2 and 2.4.2 of the current report.
[425] Article 5 (a) of the GDPR.
[426] Article 6 (a) of Directive 95/46/EC.
[427] See the Annex of the current report, Sections 1.1 and 1.2.
[428] See the Annex of the current report, Section 1.3, Article 12 of the GDPR and Recitals 39 and 58 of the GDPR.
[429] See Recital n°43 of the GDPR: « Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance". See also Recital n° 60 of the GDPR and its Article 7 that regulates the conditions for data subject's consent.
[430] See above the Sections 2.3.2.1.1 and 2.3.2.4.2 of the current report.
[431] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203, II.3 p. 13; II.1.2 p. 18
[432] *Ibid.*, II.3 p.13.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

3.3.2 Qualities of processing purposes

The GDPR[433] embodies the principle of specified, explicit and legitimate purpose of Directive 95/46/EC[434] (such purposes corresponding to the need that must be identified during the course of a ECHR and EUCFR necessity test[435]), as well as the principle that "*once data are collected, they must not be further processed in a way incompatible with those purposes*"[436]. Indeed, these principles are "*a prerequisite for applying other data quality requirements* [...] [since they] *contribute to transparency, legal certainty and predictability in the exact same way*"[437]. The compatibility test proposed by the Article 29 working party[438] is in addition still valid since the GDPR evokes explicitly its steps in its Article 6 para. 4 as well as its conclusions on the conditions under which further processing for historical, statistical or scientific purposes is not considered as incompatible[439], such an exception being also embodied by the GDPR (which adds the purposes of archiving in the public interest and which regulates this exception in more details - following partly the Article 29 working group - in its Article 89).

3.3.3 Data qualities

The GDPR[440] embodies the principle of adequacy, relevance and not excessiveness of data enshrined in Directive 95/46/EC[441], classifying these principles under the concept of "data minimisation" and replacing the principle of "non-excessiveness" with the principle that data must be "*limited to what is necessary*" to reach the purposes of the data processing operations, which appears more appropriate

433 Article 5 (b) of the GDPR.
434 Article 6 (b) of Directive 95/46/EC.
435 *Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211)*, 3.13; See above the Section 2.3.2.3.1. of the current report.
436 Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203, p. 4.
437 *Ibid.*, II.2 p.11.
438 *Ibid.*, III.2 pp. 20 *et seq.*
439 *Ibid.*, III.2.3 p. 28.
440 Article 5 (c) of the GDPR.
441 Article 6 (c) of Directive 95/46/EC.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

since it is closer to the ECHR and EUCFR requirement[442] which was also supposed to be applied within the framework of Directive 95/46/EC[443].

The GDPR[444] also embodies the obligations of data accuracy and of keeping these data up-to-date, as well as the obligation to take every reasonable step to ensure that inaccurate data are erased or rectified (adding that this must be done "*without delay*").

The GDPR[445] finally embodies the principle of time limitation and the possible processing for longer periods for historical, statistical or scientific purposes, as well as (which is new compared with the Directive) for archiving purposes in the public interest, with thin modifications of pure form. Indeed, the GDPR clarifies that the appropriate safeguards to be implemented at this occasion must be of an organisational and technical nature (which is also clarified in other provisions in relation to safeguards more generally[446]), which is not a substantive modification compared with Directive 95/46/EC in the light of ECHR and EUCFR requirements[447]. The GDPR also states that data may be "stored" for longer periods in order to be solely processed for the latter statistical, historical, scientific and achieving purposes, rather than stating that data may be "processed" for longer period for these same purposes, but this cannot mean that the first storage can be done for other purposes, since storage is an action belonging itself to the "processing" categories[448].

3.4 Legal ground for processing

In the same line as Directive 95/46/EC[449], the GDPR[450] embodies the principle that processing of personal data must be either based on the consent of the data subject (conditions for consent being

[442] See above the Section 2.3.2.4.1 of the current report.
[443] See above the Section 2.4.2 of the current report.
[444] Article 5 (d) of the GDPR; Article 6 (d) of Directive 95/46/EC.
[445] Article 5 (e) of the GDPR; Article 6 (e) of Directive 95/46/EC.
[446] See especially the Section 3.6 of the current report.
[447] See the Section 2.3.2.4.2 of the current report.
[448] Article 4 §2 of the GDPR.
[449] Article 7 of Directive 95/46/EC.
[450] Article 6 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

newly regulated in Articles 7 and 8 of the GDPR), or "necessary" (this term referring to the need to perform a ECHR necessity and a proportionality test[451]) to pursue some strictly listed aims (which are actually a list of purposes that are more specific than the "legitimate aim" required by the ECHR and the EUCFR, but that are broader than the specific need to be identified during the necessity test - which corresponds for its part to the specific purpose of the processing under the GDPR and Directive 95/46/EC[452]).

The thin differences between the GDPR and Directive 95/46/EC appear to be of pure form at the following exceptions:

- The purpose of performing a task carried out in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed is reduced to the controller (such an authority vested only in third parties to whom the data are disclosed is not a legal ground for processing anymore).
- The legal ground consisting of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed is also alleviate from the notion of third parties to whom the data are disclosed. The GDPR also clarifies that this legal ground cannot base processing carried out by public authorities in the performance of their tasks, and emphasises the necessity to take care of the particular protection due to children in relation to information society services.
- The GDPR restricts the Member States latitude to maintain or introduce more specific provisions in relation to processing operations that are necessary for compliance with a legal obligation to which the controller is subject and that are necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[453].
- At the exception of the paragraph above and in the same line as Directive 95/46/EC, the

[451] See above the Section 2.4.2.2 of the current report.
[452] See above the Section 2.4.2.1 of the current report.
[453] Article 6 §2 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

GDPR authorises derogations to the obligation to legally base data processing and to the list of acceptable grounds in order to preserve the freedom of expression and the press[454]. However, while the Directive did not provide for other possible exceptions, the GDPR also authorises Member States to determine other specific conditions (targeting all the GDPR provisions) in listed areas which are processing and public access to official documents[455], processing of the national identification number[456] and processing in the context of employment[457].

3.5 Special categories of data

In the same line as Directive 95/46/EC, the GDPR prohibits the principle of two special categories of data which are data commonly named "sensitive data" and data relating to penal infringements. If the second prohibition remains unchanged in substance, the first one is reinforced.

3.5.1 Sensitive data

The list of sensitive data provided by Directive 95/46/EC[458] is supplemented in the GDPR[459] with a series of new data: genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning a natural person's sexual orientation.

Situations were exceptions may take place are also the same, with very minor differences (such as the possibility for bodies with a philosophical aim to process data concerning former members in addition to members, while Directive was only mentioning members).

The GDPR adds however three possible exceptions, listed in Article 9 para. 2 (i) and (j) and in Article 9 para. 4. They are respectively related (1) to reasons of public interest in the area of public health, (2) to archiving purposes in the public interest, scientific or historical research purposes or

[454] Article 85 of the GDPR, Article 9 of Directive 95/46/EC.
[455] Article 86 of the GDPR.
[456] Article 87 of the GDPR.
[457] Article 87 of the GDPR.
[458] Article 8 of Directive 95/46/EC.
[459] Article 9 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

statistical purposes (subject to conditions detailed in Article 89 of the GDPR) and (3) to genetic data, biometric data or data concerning health, which may be subject to conditions including limitations at the initiative of Member States.

3.5.2 Data relating to penal infringements

The GDPR[460] prohibits the processing of personal data relating to criminal convictions and offences the same way as Directive 95/46/EC[461], with very minor differences of wording (the GDPR excluding especially, by reference to Article 6 para. 1, processing based on Directive 2016/680).

3.6 Security

The principle of security of processing, which is stated in Article 17 para. 1 of Directive 95/46/EC, is in the GDPR[462] embodied in addition to be detailed and extended in terms of scope.

In relation to the method to be used, both texts impose to carry on a risk analysis, several clarifications brought in the GDPR being taken from risk management methodologies[463].

In relation to the scope of the analysis, Directive 95/46/EC imposes to protect personal data against a series of undue processing operations, which means to analyse the risks posed to personal data, while the GDPR commands to assess the risks posed to citizens' rights and freedom, in addition to the risks posed to processed data. Assessing the risks posed to rights and freedoms imposes to adapt traditional risk assessment methodologies to such investigations' perimeter[464] and to include, in the

[460] Article 8 §5 of Directive 95/46/EC.
[461] Article 10 of the GDPR.
[462] Article 5, §1 (f) and Article 32 of the GDPR.
[463] Such as the « likelihood » and « severity » of risks, the necessity to take technical and organisational measures in order to mitigate risks, the necessity to ensure the confidentiality, integrity and availability of processing systems, of data and more generally of any element (called "primary asset" in risk management methodologies) that need to be protected against risks. See also below the Section 3.7.3.5 of the current report.
[464] On a method built on the state of the art, taking into account both PIA and risk management guidelines and correcting inconsistencies due to the merging of all these methods (that target different needs), see Estelle De Marco, MANDOLA Deliverable D2.4a (Intermediate) - *Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2 of 11

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

list of the "primary assets" to be protected (which correspond to the elements that need to be protected against risk), both (1) the citizens' fundamental rights that might be impacted by the data processing (taking into account the context of this processing) and (2) compliance with the GDPR itself. Indeed, among the fundamental rights to be protected lies the right to personal data protection itself, the respect of the GDPR being a condition to achieve such protection[465]. In addition, data controllers have a general obligation to implement appropriate technical and organisational measures in order both to ensure that legislation is respected and to demonstrate such compliance, taking into account the risks and their likelihood and severity[466]. The latter obligation imposes to all data controllers to perform an analysis of the risks posed to the respect of the legislation, in order to find the appropriate measures that are likely to mitigate or eliminate those risks.

This change might appear as being a logical implementation of the ECHR principles, imposing that risk analyses take inspiration from privacy impact assessment guidelines in order to determine their scope of investigation[467]. This is true within the framework of the obligation to carry out a data protection impact assessment[468], but it constitutes a real change in the area of risk management, where traditional methodologies apply to information systems and to the data they contain[469], while Directive 95/46/EC did not command to particularly adapt these methodologies.

In addition, the GDPR provides for examples of measures that might be appropriate in order to ensure security, which may be useful, and states that adherence to an approved code of conduct or

July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 3.2.2 (last accessed on 24 January 2018). For an application of this method to the outputs of an EU part-funded project, see Estelle De Marco *et al.*, MANDOLA Deliverable D2.4b (final) - *Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4b.4 of 30 September 2017, same project, available at the same address.

[465] See above the Section 2.4.1.2. of the current report.

[466] Articles 24 and 5§2 of the GDPR. See below the Section 3.7.3.1 of the current report.

[467] See below the Section 3.7.3.5 of the current report.

[468] *Idem.*

[469] See for ex. Estelle De Marco, MANDOLA Deliverable D2.4a (Intermediate) - *Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2 of 11 July 2017, *op. cit.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

an approved certification mechanism as they are regulated in the GDPR "*may be used as an element by which to demonstrate compliance*" [470] with the security requirement.

Finally, the GDPR obliges data controllers to notify personal data breaches to the supervisory authority no later than 72 hours[471] and to the data subjects[472], regulating *inter alia* the content of the notifications. These obligations are subject to exceptions (more numerous in relation to the notification of the data subject)[473].

3.7 Liability and accountability of the data controllers and processors

Liability and accountability of the data controllers and processors is the main modification of substance brought by the GDPR compared with Directive 95/46/EC, in addition to the modification of the territorial scope and to the scope of the obligation of security. Even though the responsibility of the controllers to enforce the data protection legislation is only partly reinforced compared with Directive 95/46/EC (in addition to the establishment of a welcome exception), as well as the controllers' responsibility in relation to the other persons involved in the processing of personal data and as processors' responsibility, provisions relating to the data controller's accountability and relating to sanctions are the object of important modifications.

3.7.1 Responsibility to enforce the data protection legislation

The GDPR regulates three aspects of the responsibility of the data controller to enforce the data protection legislation.

[470] Article 32, §3 of the GDPR.
[471] Article 33 of the GDPR.
[472] Article 34 of the GDPR.
[473] Articles 33 and 34 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

3.7.1.1 Explicit obligation to enforce the legislation's provisions

In the same line of Directive 95/46/EC, the GDPR imposes to data controllers to ensure the respect of the data protection legislation, multiplying however the provisions where this obligation is reminded. Such as Directive 95/46/EC, the GDPR states this principle in the provisions relating to purposes, data and data processing qualities[474], in the provisions relating to data subjects' rights (which are much more numerous)[475] and in relation to confidentiality and security of processing[476], in addition to the new provisions relating to transparency[477] and relating to the conditions applicable to child's consent in relation to information society services[478].

3.7.1.2 Exception of processing which does not require identification

On the opposite, the GDPR also establishes in its Article 11 an exception to the controller's responsibility, where the purpose of the processing does not require the identification of a data subject. In such case, the controller is "*not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with*" the GDPR, and he or she is authorised to both (1) inform the data subject that he or she is not in a position to identify him or her (in case it can demonstrate it) and (2) to not apply a certain number of data subjects' rights (unless the data subject provides additional information enabling his or her identification). Such exception is not provided for in Directive 95/46/EC, but was already latent since Article 15 of the Directive imposes to organise a right of access of the data subject, which implies in turn being able to identify him or her as the subject of the processed information, in order to answer his or her request. However, the novel Article 11 of the GDPR ensures data controllers' legal security in a more appropriate manner.

474 Article 5§2 of the GDPR, Article 6§2 of Directive 95/46/EC.
475 Articles 13 to 21 of the GDPR, Articles 10 to 12 of Directive 95/46/EC.
476 Articles 32 to 34 of the GDPR, Articles 16 and 17 of Directive 95/46/EC.
477 Article 12 of the GDPR.
478 Article 8 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

3.7.1.3 Codes of conduct and certification

In order to contribute to the proper implementation of the data protection legislation, including the respect of all the controllers' obligations, Directive 95/46/EC encourages the drawing up of codes of conduct, establishing some process enabling the control of their content by legitimate authorities[479]. The GDPR embodies the rule, reinforces its formalism as well as the control and monitoring of the codes of conduct, and clarifies the content of the latter, extending their application to data controllers who are not subject to the Regulation[480].

In addition, the GDPR encourages the "*establishment of data protection* [voluntary] *certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors*", and organises the procedure to issue them[481]. It also regulates also certification bodies[482].

3.7.2 Responsibility of the data controller in relation to the other persons involved in the processing of personal data

Both in Directive 95/46/EC (as interpreted by the Article 29 Working party) and in the GDPR, joint controllers may share the responsibility to comply with the data protection legislation, based on a contract distributing responsibilities (unless law regulates their responsibilities otherwise)[483]. In both cases, the data controller alone is entitled to give instructions, in relation to processing operations, to processors and more generally to any person acting under his or her responsibility[484] (and, under the GDPR, data controllers must "take steps to ensure" that this is respected, as part of the obligation of

[479] Article 27 of Directive 95/46/EC.
[480] Articles 40 and 41 of the GDPR.
[481] Article 42 of the GDPR.
[482] Article 43 of the GDPR.
[483] Article 26 of the GDPR; Implicit in Article 2 d) of Directive 95/46/EC, interpreted by the Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 16 February 2010, p. 20.
[484] Article 29 of the GDPR; Article 16 of Directive 95/46/EC.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

security[485]). The data controller not established in the Union must in addition designate ("*in writing*", in the GDPR) a representative in the Union[486].

For the rest, the GDPR embodies the principles that processors must provide a certain number of guarantees and must act on the basis of a contract or other legal act[487], and reinforces the processors' obligations, notably in relation to the content of their contract to be established with the controllers (and their correlative obligations) and in relation to possible sub-processors.

3.7.3 Data controllers' (and processors') accountability: evidences pre-establishment vs notification

Under Directive 95/46/EC, data controllers have the duty to notify processing operations to the relevant supervisory authority[488], which might take the form of a request for authorisation[489]. Member States laws may provide for simplified notification in relation to a list of processing operations that are unlikely to affect adversely the rights and freedoms of data subjects, and may even exempt whole or a part of processing operations from the obligation of notification where data controllers appoints a personal data protection official, who will be in charge, in particular, to ensure "*that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations*" through "*ensuring in an independent manner*" that these operations comply with law and through keeping a register of processing operations carried out by the controller[490], which must include at least some listed information[491]. In addition, Member States are supposed to ensure that processing operations

485 Article 32 §4 of the GDPR.
486 Article 27 of the GDPR; Article 4 § 2 of Directive 95/46/EC (referring to a representative in the concerned Member State).
487 Article 28 of the GDPR; Article 17 §2, §3 and §4 of Directive 95/46/EC.
488 Article 18 of Directive 95/46/EC.
489 Such as in France, for example.
490 Article 18 of Directive 95/46/EC.
491 Article 18 of Directive 95/46/EC which refers to Article 21§2, which refers itself to the information listed in Article 19 a) to e).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

that are likely to present specific risks to the rights and freedoms of data subjects are examined before they start by the relevant data protection authority[492].

The GDPR brings important changes to these rules: the obligation to notify data protection Authorities disappears, and is replaced by an obligation to pre-establish evidences of compliance with law from the start of processing operations, and even before this start since privacy by design and by default also becomes an explicit obligation. This principle includes several distinct obligations which are the following.

3.7.3.1 Implementation of measures that enable to demonstrate compliance with the GDPR

Data controllers must, as a general rule, implement appropriate (technical and organisational) measures in order both to ensure that each step of the data protection legislation is respected at the time it has to be respected, and to demonstrate such compliance.

- This principle is firstly the subject of an independent article that regulates "the responsibility of the controller"[493]. This article clarifies that these measures must be reviewed and updated where necessary, that they must include "*appropriate data protection policies*" where proportionality requires it, and that adherence to approved codes of conduct or certification mechanisms[494] may be used as an element by which compliance can be demonstrated.
- This principle is also recalled in several other articles of the GDPR, which command the data controller to "*be able to demonstrate compliance*" with their provisions[495].

Data processors must also implement in practice the necessary measures that enable them to demonstrate compliance with their obligations in terms of respect of the GDPR and of controllers' instructions, which are listed in Article 28 para. 3. Indeed, according to the latter (point h),

[492] Article 20 of Directive 95/46/EC.
[493] Article 24 of the GDPR.
[494] See above, the Section 3.7.1.3 of the current report.
[495] Article 5§2 relating to the principles relating to processing of personal data (data, data processing and purposes quality, in addition to security - named integrity and confidentiality - of processing operations); Article 7 relating to conditions for data subjects' consent; Article 11 relating to processing which does not require identification;

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

processors make available to the controller "*all information necessary to demonstrate compliance*" with their obligations; they must also allow for and contribute to audits.

3.7.3.2 Obligations of documentation

In addition to their obligation to demonstrate compliance with the GDPR, certain data controllers must "*maintain a record of processing activities under their responsibility*", which must contain a series of information listed in Article 30 of the GDPR and which must be made available to the supervisory authority on request[496]. This obligation applies (1) to organisations employing more than 250 persons, and (2) to organisations employing less than 250 persons that carry out processing operations *that are "likely to result in a risk to the rights and freedoms of data subjects"*[497] or that either are not occasional or include special categories of data[498].

In addition, data controllers must "*document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken*"[499], so that the supervisory authority is enabled to verify compliance with their obligation to notify personal data breaches[500].

3.7.3.3 Obligation in certain cases to designate a data protection officer

In addition to the obligations to demonstrate compliance with the GDPR and to document their processing activities, data controllers have the obligation to designate a data protection officer in certain situations[501], namely where "*the processing is carried out by a public authority or body*" (except for courts acting in their judicial capacity); where "*the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale*"; or where "*the core activities of the controller or the processor consist of*

[496] Article 30, §4 of the GDPR.
[497] Article 30, §5 of the GDPR.
[498] See above the Section 3.5 of the current report.
[499] Article 33, §5 of the GDPR.
[500] See above the Section 3.6 of the current report.
[501] Article 37 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

processing on a large scale of special categories of data [...]"[502]. In other situations, the designation of a data protection officer is optional (unless law states otherwise)[503]. The GDPR moreover regulates certain possibilities to appoint one data protection officer for several organisations or administrations[504], the criteria to be used to designate a data protection officer[505], and the data protection officer position[506] and tasks[507]. Finally, the data controller or the processor must "*publish the contact details of the data protection officer and communicate them to the supervisory authority*"[508].

3.7.3.4 Protection by design and by default

Data protection must explicitly be ensured by design and by default[509].

These principles are already implicit in Directive 95/46/EC, if read in the light of the ECHR and EUCFR principles[510]. Indeed, in relation to privacy by design, the legislation is supposed to be respected at the time processing operations begin, and it seems very difficult, in relation to numerous processing activities, to be able to respect a certain number of principles such as data and processing qualities and data security, or to provide answers to data subjects' requests where the latter exercise their rights of access and rectification, if processes are not in place in order to ensure that appropriate action is taken in an efficient manner, under reasonable delays and without undermining associated business activities. In relation to privacy by default, the data protection principles already include *inter alia* data minimisation, time limitation and data subjects' consent as a legitimate basis for processing. As a result, the respect of the current legislation should lead to apply a reinforced protection by default, which might be alleviated in particular cases where a legitimate ground or reason enables a stronger interference with the right to the protection of personal data.

---

[502] See above the Section 3.5 of the current report.
[503] Article 37, §4 of the GDPR.
[504] Article 37 §2 and §3 of the GDPR.
[505] Article 37 §5 and §6 of the GDPR.
[506] Article 38 of the GDPR.
[507] Article 39 of the GDPR.
[508] Article 37 §7 of the GDPR.
[509] Article 25 of the GDPR.
[510] See above, the Section 2.4 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

It is the reason why the concept of privacy by design has been developed in the 1990's by Dr. Ann Cavoukian, former Information and Privacy Commissioner of Ontario[511], and afterward increasingly considered[512]. Indeed, this concept has been referred to as being the "*next generation of privacy protection*"[513] (and is basically today the "new" one), to respond to new challenges posed by technology. Its objective is both to achieve a deep and meaningful respect of privacy (which is threatened in the context of the use of new technologies[514]) and to serve data controllers' interests (*inter alia* through the improvement of customers' or citizens' confidence, through costs reduction and through the reduction of risk of liability associated with privacy breaches[515]). Privacy by design is therefore seen as a "*win-win, positive-sum approach*"[516] where the protection of privacy (or, at least, compliance with legal rules protecting privacy) must not be seen any more as a burden that threatens business and innovation. The privacy by design method is basically to embed privacy requirements "*into the design specifications of information technologies, business practices, and networked infrastructures as a core functionality*", while "*preserving a commitment to full functionality*"[517]. This method, divided into seven principles[518], already includes the concept of privacy by default since ensuring an automatic protection of personal data means *inter alia* that "*no action is required on the part of the individual to protect their privacy*"[519], or, in other words, that the protection must be the strongest possible in case the data

[511] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *A White Paper for Regulators, Decision-makers and Policy-makers*, August 2011, p. 3 (Introduction), available at https://gpsbydesign.org/resources-item/privacy-by-design-in-law-policy-and-practice-a-white-paper-for-regulators-decision-makers-and-policy-makers/ (last accessed on 23 February 2018). The current developments relating to privacy by design are partly based on Estelle De Marco previous research in that field, lastly published in Estelle De Marco, MANDOLA Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes, version 2.4a.2 of 11 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 3.2.2 (last accessed on 24 January 2018).

[512] See Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit.*, especially pp. 3-5; see also Article 29 working party, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 1st December 2009 (WP 168), esp. pp.2-3 and pp. 12 *et seq.*

[513] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit.*, p. 10.

[514] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit.*, p. 6.

[515] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit.*, p. 11.

[516] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit.*, p. 10.

[517] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit.*, p. 10.

[518] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit.*, pp. 28 *et seq.*

[519] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit.*, p. 28, n°2.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

subject "*does nothing*"[520].

The GDPR incorporates these principles, requiring that organisational and technical measures are implemented in order to ensure in an effective manner the application of both the "*data-protection principles*" and "*the necessary safeguards*"[521] that will enable to meet these requirements, taking into account the context[522] and the severity and likelihood of risks (which implies to perform a risk analysis[523]). Data protection principles must in addition be implemented - through these same organisational and technical measures -"by default"[524], in order to ensure that "*only personal data which are necessary for each specific purpose of the processing are processed*" in terms of "*amount of personal data collected,* [...] *extent of their processing*"[525], period of storage and accessibility (which must in particular prevent accessibility "*without the individual's intervention, to an indefinite number of natural persons*"[526]). Here again[527], an "*approved certification mechanism* [...] *may be used as an element to demonstrate compliance*" with these requirements[528].

3.7.3.5 Data protection impact assessment

In addition to the obligations evoked previously, the GDPR commands to carry out, prior to the processing, a data protection impact assessment (DPIA) where this processing is of a type that "*is likely to result in a high risk to the rights and freedoms of natural persons*"[529], which will be in particular the case where it uses "*new technologies*"[530], and especially in case of (a) "*systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural*

[520] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit.*, p. 28, n°2.
[521] Article 25 of the GDPR.
[522] Namely the state of the art, the cost of implementation and the nature, scope, context and purposes of processing.
[523] See below the Section 3.7.3.5 of the current report.
[524] Article 25, §2 of the GDPR.
[525] *Idem.*
[526] *Idem.*
[527] See above the Section 3.7.1.3 of the current report; see also for example Sections 3.6 and 3.7.3.1.
[528] Article 25, §3 of the GDPR.
[529] Article 35, §1 of the GDPR.
[530] *Idem.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

person"; (b) "*processing on a large scale of special categories of data*[531]"; or (c) "*systematic monitoring of a publicly accessible area on a large scale*"[532]. A single DPIA is however acceptable "*to address a set of similar processing operations that present similar high risks*"[533].

The extent of this obligation appears therefore to be very large, since it will be very difficult to appreciate at which point the use of new technologies will not pose a high risk for rights and freedoms, considering in addition that the notion of risks for privacy is highly subjective[534], unless the lists of processing requiring and not-requiring the carrying out of a DPIA, to be published by data protection authorities[535], are very clear.

As a consequence, it is likely that a DPIA will have to be undertaken in most situations, in order to ensure legal certainty. This being said, it is striking that the minimum content of a DPIA as it is detailed in the GDPR consists of four elements that are already required in most processing operations.

Indeed, the GDPR states that a DPIA must contain at least the following five steps[536]:

- "*A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller*" [537]. However, the purposes of the processing, the categories of data subjects and of processed data, and their recipients including the data controller, are *inter alia* elements of information that must be recorded[538]. In addition, the risk assessment that is also required by the GDPR, as we will analyse it below, already

[531] See above the Section 3.5 of the current report.
[532] Article 35, §3 of the GDPR.
[533] *Idem.*
[534] The notion of private life being very subjective as well, and a large part of private life being protected or non-protected because the private life's owner him or herself decided to share his or her information of private life with third parties (see above Section 2.2.1.1 of the current report and Section 3.4 highlighting that data subjects' consent is the principle for collecting personal data). As a result, a simple list of clients might be perceived as requiring the performance of a DPIA, depending on the processing context (this answer has been the most important one provided to an examination question proposed by the editor at the issue of a Master course on personal data protection, in November 2017).
[535] Article 35, §§4-6 of the GDPR.
[536] Article 35, §7 of the GDPR.
[537] Article 35, §7 (a) of the GDPR.
[538] See above the Section 3.7.3.2 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

implies, inherently, a systematic description of processing operations[539].

- "*An assessment of the necessity and proportionality of the processing operations in relation to the purposes*"[540]. We have already analysed that the GDPR requires the data controller to ensure both the necessity and the proportionality of processing operations through a set of requirements that impose, most of the time, an evaluation of the necessity and of the proportionality of his or her action (such as the determination of the processing purposes, and the identification of time limits and adequate data minimisation in this regard)[541]. Since the data controller must pre-establish evidences of compliance[542], it appears that the undertaking of formal necessity and proportionality tests is the most appropriate mean to fully ensure and demonstrate compliance with law. In addition, the GDPR provides for several situations where additional necessary and proportionality tests are required, where data processing operations cannot be framed by typical safeguards it provides[543].

- "*An assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1*"[544], taking into account "*the nature, scope, context and purposes of the processing*"[545]. This requirement corresponds to the performance of a risk analysis, following a risk management method[546], with the aim to protect both citizens' rights and freedoms and compliance with the GDPR (which will be

[539] See Estelle De Marco, *MANDOLA Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2 of 11 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 3.4, step n°3 (last accessed on 24 January 2018).
[540] Article 35, §7 (b) of the GDPR.
[541] See above, the Section 2.4.2.1. of the current report.
[542] See above, the Section 3.7.3.1. of the current report.
[543] See above, the Section 2.4.2.2. of the current report.
[544] Article 35, §7 (c) of the GDPR.
[545] Article 35, §1 of the GDPR.
[546] See for ex. Estelle De Marco, *MANDOLA Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2 of 11 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 3.4 (last accessed on 24 January 2018). For an application of this method to the outputs of an EU part-funded project, see Estelle De Marco *et al.*, MANDOLA Deliverable D2.4b (final) - *Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4b.4 of 30 September 2017, same project, available at the same address.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

identified as "primary asset" within the framework of the risk assessment[547]), in addition to personal data that are processed. This requirement implies therefore, in addition, to perform in any way a test of compliance with the GDPR, since the analysis of risks targeting such compliance implies a prior identification of the actual level of compliance and of the steps that have been taken in this regard.

However, the performance of a risk analysis is an obligation in all cases of personal data processing on the basis of Article 32 of the GDPR, which - as we analysed it - also commands the assessment of risks on rights and freedoms and on compliance with the GDPR itself[548]. In addition, tests of compliance with the GDPR will be necessary in all situations of personal data processing, due to the general obligation to implement appropriate technical and organisational measures in order both to ensure the respect of the data protection legislation and to demonstrate such compliance[549].

- "*The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned*"[550]. This requirement is the logical result of any risk analysis that would be applied to processed personal data and to obligations whose respect ensures compliance with the GDPR, taking into account the impacts of these measures on all rights and interests at stake (keeping in mind that a risk analysis always evaluates impacts of risks as well as their severity[551]).

- "*Where necessary,* [...] *a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations*"[552]. This

[547] See above, the Section 2.4.1.2 of the current report.
[548] See above the Section 3.6 of the current report.
[549] Article 24 of the GDPR. See above, the Section 3.7.3.1. of the current report.
[550] Article 35, §7 (d) of the GDPR.
[551] See for ex. Estelle De Marco, MANDOLA Deliverable D2.4a (Intermediate) - *Privacy Impact Assessment of the MANDOLA outcomes*, op. cit., Section 4.4.1.
[552] Article 35, §11 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

requirement is also one of the steps of any risk analysis and any privacy impact assessment[553].

As a result, it is likely that in practice, a DPIA as it is described in the GDPR will be mandatory in all or in most cases, even if it is split into several tasks performed at different occasions.

The five minimum requirements that need to be included in a DPIA according to the GDPR can however be supplemented by two other steps that are usually included in PIA guidelines and even in risk management methodologies (without being mandatory in the latter ones), and which are the determination of the assessment team and the consultation of relevant stakeholders in order to collect their views and take them into account[554].[555] The GDPR evokes the latter one without making it mandatory, stating that "*where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations*"[556].

For the rest, the GDPR clarifies[557] that a DPIA should also be performed prior the adoption of a law that authorises specifically certain processing operations, and that in such cases the processing regulated through this law must be exempted from carrying out other DPIAs, unless such subsequent DPIA are deemed necessary[558] (which should be the case in several situations where the context of the processing is likely to evolve)[559]. The GDPR also states here[560] that "*compliance with approved codes of conduct* [...] *shall be taken into due account in assessing the impact of the processing operations*

[553] See for ex. Estelle De Marco, *MANDOLA Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, *op. cit.*, Section 4.7.
[554] See Estelle De Marco, *MANDOLA Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2, *op. cit.,* Sections 3.4, 4.2 and 4.6.
[555] A test of compliance with the relevant legislation is also required as a PIA and risk management step, but we have analysed that these tests are already included in the GDPR requirements, which impose both a necessity and proportionality test and a test of compliance with the GDPR.
[556] Article 35, §9 of the GDPR.
[557] Any law should ensure that the limitation brought to rights and freedom is necessary and proportionate to the aim pursued, and provide for appropriate safeguards in this regard (see above the Section 2.3.2 of the current report).
[558] Article 35, §10 of the GDPR.
[559] See the fifth DPIA requirement above and our related footnotes.
[560] See above the Section 3.7.1.3 of the current report; see also for example Sections 3.6 and 3.7.3.1.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

performed by such controllers or processors, in particular for the purposes of a data protection impact assessment"[561].

3.7.3.6 Cooperation with the supervisory authority

Under the GDPR, the controller and the processor must firstly "*cooperate, on request, with the supervisory authority in the performance of its tasks*" [562]. This is already the case in practice under Directive 95/46/EC due to the investigative powers dedicated to supervisory authorities[563], but without being declared as a principle. Under the GDPR, the controller must also "*consult the supervisory authority prior to processing*" where a DPIA "*indicates that the processing would result in a high risk in the absence of measures taken* [...] *to mitigate the risk*"[564], and must provide at this occasion several listed information[565]. These provisions should particularly be used in case the nature or the context of processing operations prevent the controller from respecting certain legal provisions, and that alternative safeguards must be found in order to ensure the necessity and proportionality of processing operations[566].

3.7.4 Remedies, liability and sanctions

The GDPR follows the same line as the Directive in relation to remedies and liabilities, adding however details and clarifications, and providing for determined administrative sanctions (which is not the case in the Directive) which might be very high.

3.7.4.1 Right to lodge a complaint

In the same line as Directive 95/46/EC, the GDPR states that every data subject must have the right to lodge a complaint with a supervisory authority[567] (even though the Directive lets more room to Member States in this regard[568]) and must have the right to an effective judicial remedy against a

[561] Article 35, §8 of the GDPR.
[562] Article 31 of the GDPR.
[563] Article 28 of Directive 95/46/EC.
[564] Article 36 §1 of the GDPR.
[565] Article 36 §3 of the GDPR.
[566] See above the Section 2.4.3 of the current report and the Annex, Section 2.1.
[567] Article 77 of the GDPR.
[568] Article 22 of Directive 95/46/EC.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

controller in order to obtain compensation[569]. However, the GDPR adds the right to an effective judicial remedy against a processor[570], as well as against a supervisory authority[571] (providing for the possibility of an effective remedy in case of a three-months silence, while Directive 95/46/EC organises the solely right to lodge a complaint against a decision from this authority[572]). It also regulates the representation of data subjects within the framework of a complaint[573] and the suspension of proceedings where first "*proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State*" [574].

3.7.4.2 Liability

In the same line as Directive 95/46/EC, the GDPR[575] enshrines the right to receive compensation from the controller (adding, however, the possibility to receive compensation also from the processor) where the latter did not comply with the legislation, exempting these stakeholders from liability where they prove they are not responsible "*in any way*"[576] for the event giving rise to the damage. The GDPR regulates in addition situations where more than one controller or processor are involved[577], recourse actions[578], and identifies competent jurisdictions[579]. It also regulates the general conditions for imposing administrative fines[580].

569 Article 79 of the GDPR, Article 23 of Directive 95/46/EC.
570 Article 79 of the GDPR.
571 Article 78 of the GDPR.
572 Article 28 §3 sub§. 4 of Directive 95/46/EC.
573 Article 80 of the GDPR.
574 Article 81 of the GDPR.
575 Article 82 of the GDPR.
576 The wording of Directive 95/46/EC (Article 23) is "*in whole or in part*" which appears a bit more restrictive.
577 Article 82 §4 of the GDPR.
578 Article 82 §5 of the GDPR.
579 Article 82 §6 of the GDPR.
580 Article 83 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

3.7.4.3 Sanctions

While the Directive leaves to Member States the duty to "*adopt suitable measures to ensure the full implementation*" of its provisions, including sanctions in case of infringement[581], the GDPR enables such determination of sanctions by Member States provided that they are "*effective, proportionate and dissuasive*"[582] and imposes a certain level of administrative fines[583]. Indeed, infringements of a list of provisions must be subject to "*administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*"[584]. Another list of infringements must be subject to "*administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*"[585].

3.8 Data subjects' rights

In the same line as Directive 95/46/EC, the GDPR enshrines the rights of data subjects to information[586] (in addition to add a principle of transparency of this information[587]). Globally, the mandatory information is wider in the GDPR than in the Directive, but the latter gives explicitly more room to adapt the information to the processing's specificities (the Directive states that the information it lists must be provided "*at least*", while the GDPR states that "*all the*" information it lists must be provided). This has no consequences if read in conjunction with the principle of fairness, which imposes to provide to data subjects all the necessary information[588], and with the ECHR and EUCFR principle of transparency[589], but this remains very implicit and, as a result, could lead data controllers to provide the information listed in Articles 13 and 14 of the GDPR only

581 Article 24 of Directive 95/46/EC.
582 Article 84 of the GDPR.
583 Article 83 of the GDPR.
584 Article 83 §4 of the GDPR.
585 Article 83 §4 and §6 of the GDPR.
586 Articles 13 and 14 of the GDPR; Articles 10 and 11 of Directive 95/46/EC.
587 Article 12 of the GDPR; see above, the Section 3.3.1 of the current report.
588 See above, the Section 3.3.1 of the current report.
589 See above, the Section 2.3.2.4.2 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

(which will render very difficult an administrative or judicial assessment of their liability in this regard, in case of damage or penal proceedings based on this obligation).

In the same line as Directive 95/46/EC, the GDPR also grants data subjects with a right of access[590], a right to rectification[591], a right to erasure[592], a right to obtain notification of measures taken to other recipients of the personal data concerned[593], a right to object[594], and a right to not be subject to automated decision making[595], which are however reinforced. In particular, the right to erasure includes in the GDPR a right to be forgotten, especially where the controller "*has made the personal data public*"[596], and the right to not be subject to automated decisions includes, in the GDPR, a "*right to obtain human intervention on the part of the controller*"[597], the prohibition to use special categories of data[598] unless strict exceptions[599], and the clarification that profiling might be one of these automated decision making[600].

In addition, the GDPR adds a right to restriction of processing[601] (which replaces the right to obtain the blocking of the processing under Directive 95/46/EC[602]), and a right to data portability[603].

3.9 Supervisory authorities and Commission supervision

The GDPR enshrines the existence of supervisory authorities established in Directive 95/46/EC and their responsibility for monitoring the application of the data protection legislation[604]. However, the

590 Article 15 of the GDPR; Article 12 a) of Directive 95/46/EC.
591 Article 16 of the GDPR; Article 12 b) of Directive 95/46/EC.
592 Article 17 of the GDPR; Article 12 b) of Directive 95/46/EC.
593 Article 19 of the GDPR; Article 12 c) of Directive 95/46/EC.
594 Article 20 of the GDPR; Article 14 of Directive 95/46/EC.
595 Article 22 of the GDPR; Article 15 of Directive 95/46/EC.
596 Article 17 §2 of the GDPR.
597 Article 22 §3 of the GDPR.
598 See above, the Section 3.5 of the current report.
599 Article 22 §4 of the GDPR.
600 Article 22 §1 of the GDPR.
601 Article 18 of the GDPR.
602 Article 12 b) of Directive 95/46/EC.
603 Article 20 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

GDPR states in much more detail the conditions for independence[605], the competence[606], tasks[607] and powers[608] of the authorities, regulating in addition the competence of the lead and of the other supervisory authorities in case the controller has several establishments within the EU[609] and the cooperation between involved authorities in such situation[610]. The GDPR adds requirements relating to the members of supervisory authorities[611] and regulates their mutual assistance[612] and their joint operations[613].

Consistency of the application of the GDPR throughout the EU is also specifically regulated, through cooperation between supervisory authorities[614] and supervision of the European data protection board[615], which replaces the Article 29 data protection working party established by Articles 29 and 30 of Directive 95/46/EC and which powers, composition and tasks are also regulated in far greater detail[616].

The Commission's powers and attributions are also reinforced and extended. The Commission is entitled to adopt delegated acts[617], particularly in relation to the information to be presented by icons and the procedures for providing standardised icons[618], and implementing acts (*inter alia* in order to standardise electronic exchanges between supervisory authorities and the board[619] and to specify the format and procedures for mutual assistance between supervisory authorities[620]), assisted by a

604 Article 51 of the GDPR; Article 28 of Directive 95/46/EC.
605 Article 52 of the GDPR.
606 Article 55 of the GDPR.
607 Article 57, 59 of the GDPR.
608 Article 58 of the GDPR.
609 Article 56 of the GDPR.
610 Article 60 of the GDPR.
611 Articles 53, 54 of the GDPR.
612 Article 61 of the GDPR.
613 Article 62 of the GDPR.
614 Article 63 of the GDPR.
615 Articles 64-66 of the GDPR.
616 Articles 68-76 of the GDPR.
617 See for ex. Articles 92, 12, 43§8 of the GDPR.
618 Article 12 §8 of the GDPR.
619 Article 67 of the GDPR.
620 Article 61 §9 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Committee that is already established in Directive 95/46/EC[621] but which is now more precisely regulated in Regulation n° 182/2011[622]. The Commission receives several other powers in the area of standardisation, for instance in relation to the determination of contractual clauses relating to processors' contracts[623] and the determination of standard protection clauses in the area of data transfers[624]. It participates to the general consistency mechanism[625], and - together with supervisory authorities - receives missions aiming to develop international cooperation for the protection of personal data in relation to third countries and international organisations[626]. Its tasks in the area of encouraging the drawing up of codes of conduct are reinforced[627] and extended to certification mechanisms[628], and its power to issue adequacy decisions in the area of data transfers is clarified and detailed[629]. The Commission receives finally the power to issue reports on the evaluation and review of the GDPR[630] and to submit legislative proposals "*with a view to amending other Union legal acts on the protection of personal data*" [631].

3.10 Data transfers

Such as Directive 95/46/EC[632], the GDPR regulates the transfer of personal data to third countries[633]. The principle that a transfer might only take place where an adequate level of protection is ensured is maintained, but the GDPR is much more detailed in relation to adequacy decisions and

621 Article 93 of the GDPR; Article 31 of Directive 95/46/EC.
622 Article 93 of the GDPR, referring to Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, especially its Article 3.
623 Article 28 §7 of the GDPR.
624 Article 46 of the GDPR.
625 Articles 63-64 of the GDPR.
626 Article 50 of the GDPR.
627 Article 40 of the GDPR; Article 27 of Directive 95/46/EC.
628 Article 42 of the GDPR.
629 Article 45 of the GDPR.
630 Article 97 of the GDPR. Under Directive 95/46/EC (Article 33), this power was limited to the implementation of the Directive.
631 Article 98 of the GDPR.
632 Article 25 of Directive 95/46/EC.
633 Articles 44 to 49 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the way such decisions are taken[634] and on safeguards to be implemented in the absence of such decision[635]. The GDPR also regulates binding corporate rules to which an Article is dedicated[636], transfers or disclosures that are not authorised by Union law[637] and it provides for derogations for specific situations[638].

[634] Article 45 of the GDPR.
[635] Article 46 of the GDPR.
[636] Article 47 of the GDPR.
[637] Article 48 of the GDPR.
[638] Article 49 of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4. Conclusion

The previous analysis confirms that substantive differences between the GDPR and Directive 95/46/EC are not numerous, and are essentially related to the territorial scope of application of the legislation[639], to the liability and accountability of data controllers and processors[640], and to the scope of the obligation of security[641]. The other variations consist actually in the GDPR of clarifications that leave less flexibility as to how the rule must be interpreted (preventing some literal interpretations that would not take into account the ECHR and the EUCFR requirements) or that leave less flexibility as to how the rule must be applied (in relation to choices that are available in order to enforce the principles of necessity and of proportionality in given situations), imposing however in most situations, as a result, actions that are already required within the application of the ECHR and of the EUCFR, and therefore actions that should not constitute a real novelty for data controllers who were already respecting Directive 95/46/EC in light of ECHR and EUCFR requirements[642]. This is for example the case of the content of the information to be provided to data subjects, of the principle of transparency, of the obligation to record processing activities, and of the obligation to carry out and implement the results of necessity and proportionality analyses (which might enable to establish evidence of compliance with these requirements - and further with a large part of the data protection legislation)[643].

This leads to draw a consequence and to express a regret.

The consequence that appears very clearly is that data controllers who cannot respect some of the GDPR requirements seem entitled to carry out a data protection impact assessment in order to highlight weaknesses of their GDPR, necessity and compliance tests, and to determine the

639 See the Section 3.2.1 of the current report.
640 See the Sections 3.7.3 and 3.7.4 of the current report.
641 See the Section 3.6 of the current report.
642 See the Section 2.4 of the current report.
643 See the Section 2.4.2.3.2 of the current report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

safeguards that will both appropriately answer these weaknesses and address the risks identified in this context[644], under the supervision of the relevant supervisory authority[645].

The regret that we can express is that data controllers have not been made more aware and informed, over the last decade, of the understanding of the ECHR and EUCFR requirements, and of the need to read the data protection legislation in the light of these requirements (taking also into account that the necessity and proportionality tests are an efficient approach to business and even personal activities, which enables to prevent to cause damages to others, and therefore to engage one's liability). Such awareness and information would have contributed to enhance practices toward a better understanding of Directive 95/46/EC and of the national provisions implementing it, and therefore toward an application of the data protection legislation that would have been very close to the philosophy that underlies it. This situation would have prevented the fear that surrounds from 2016 the need to implement the GDPR before May 2018[646], since most stakeholders' subject to the respect of Directive 95/46/EC would only have had some smaller adjustments to bring to their practices in order to reach such compliance.

644 Article 35 of the GDPR; see the Section 3.7.3.5 of the current report.
645 Article 36 of the GDPR.
646 See for example Harry Leech, Firms fear negative impact as deadline for GDPR approaches - survey, 30 April 2017, Independent.ie, https://www.independent.ie/business/data-sec/firms-fear-negative-impact-as-deadline-for-gdpr-approaches-survey-35663037.html; *Organisations fear lack of preparedness for GDPR could put them out of business*, 26 April 2017, Out-law.com, https://www.out-law.com/en/articles/2017/april/organisations-fear-lack-of-preparedness-for-gdpr-could-put-them-out-of-business/ (URLs last accessed on 24 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Bibliography

Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 April 2017 (WP248).

Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217).

Article 29 Data Protection Working Party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (WP 211).

Article 29 Data Protection Working Party, *Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force*, 22 April 2013 (WP 205).

Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013 (WP203).

Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent* (WP187).

Article 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices*, 16 May 2011 (WP 185).

Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, 22 June 2010 (WP 171)

Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 16 February 2010.

Article 29 Data Protection Working Party *Opinion on the use of location data with a view to providing value-added services*, November 2005 (WP 115).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Article 29 Data Protection 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 or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism*, adopted on 9 November 2004 (WP99).

Beauvais, Pascal, « Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes », *in* ERPC, Archives de politique criminelle, éd. A. Pédone, 2007/1 (n°29), https://www.cairn.info/revue-archives-de-politique-criminelle-2007-1-page-3.htm (last accessed on 28 January 2018).

Bennett's, Colin, In Defence of Privacy, Surveillance & Society, Vol. 8, No. 4, 2011, pp. 485–496.

Bieker, Felix, Friedewald, Michael, Hansen, Marit, Obersteller, Hannah and Rost, Martin, "A Process for Data Protection Impact Assessment under the European General Data Protection Regulation", *in* K. Rannenberg and D. Ikonomou, *Privacy Technologies and Policy*, Fourth Annual Privacy Forum, APF 2016 Frankfurt. Heidelberg, New York, Dordrecht, London, available at http://www.springer.com/cda/content/document/cda_downloaddocument/9783319447599-c2.pdf?SGWID=0-0-45-1587701-p180200777 (last accessed on 21 February 2018).

Callanan, Cormac, Gercke, Marco, De Marco, Estelle and Dries-Ziekenheiner, Hein, *Internet blocking - balancing cybercrime responses in democratic societies*, October 2009, available at http://www.aconite.com/blocking/study, French version available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/ (last accessed on 26 January 2018).

Cavoukian, Ann, *Privacy by Design in Law, Policy and Practice, A White Paper for Regulators, Decision-makers and Policy-makers*, August 2011, https://gpsbydesign.org/resources-item/privacy-by-design-in-law-policy-and-practice-a-white-paper-for-regulators-decision-makers-and-policy-makers/ (last accessed on 24 January 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, p. 3, https://www.cnil.fr/fr/node/15798 (last accessed on 21 February 2018).

Chupin, Stéphane-Dimitri, *La protection de la vie personnelle délimitée par les frontières des sphères privées et publiques*, thesis, Université Paris I, 2002.

Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *in International Data Privacy Law 1*, 2 (March 2011) pp.111-120, available at http://www.rogerclarke.com/DV/PIAG-Eval.html (last accessed on 16 February 2018).

Clarke, Roger, *What's Privacy'?*, 2006, http://www.rogerclarke.com/DV/Privacy.html (last accessed on 12 February 2018).

Clarke, Roger, *Privacy Impact Assessments*, 19 April 1999, last update on 26 May 2003, available at http://www.rogerclarke.com/DV/PIA.html (last accessed on 16 February 2018).

Council of Europe, Committee of Ministers, *Recommendation n° Rec (2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism*, 20 April 2005.

Conseil d'État, « Sécurité juridique et complexité du droit », public report 2006, http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Securite-juridique-et-complexite-du-droit-Rapport-public-2006.

Cour de cassation, "Dossier : la charte des droits fondamentaux - historique et enjeux juridiques", *in veille bimestrielle de droit européen*, October 2010, n° 34, http://www.courdecassation.fr/publications_26/publications_observatoire_droit_europeen_2185/veilles_bimestrielles_droit_europeen_3556/2010_3865/octobre_2010_3810/droits_fondamentaux_18630.html (last accessed on 24 January 2018).

Deboissy, Florence, "La divulgation d'une information patrimoniale", D. 2000, chron. p. 26.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

DeCew, Judith, "Privacy", *in The Stanford Encyclopedia of Philosophy* (Spring 2015 Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/spr2015/entries/privacy/ (last accessed on 14 February 2017).

De Hert, Paul, Kloza, Dariusz, Wright, David *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, http://www.piafproject.eu/Deliverables.html (last accessed on 24 January 2018).

De Marco, Estelle *et al.*, *MANDOLA Deliverable D2.4b (final) - Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4b.4 of 30 September 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications (last accessed on 24 January 2018).

De Marco, Estelle, *MANDOLA Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2 of 11 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications (last accessed on 24 January 2018).

De Marco, Estelle *et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework*, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications (last accessed on 24 January 2018).

De Marco, Estelle *et al., Deliverable D3.3 - Legal recommendations*, ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), project n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, https://www.epoolice.eu/EPOOLICE/servlet/document.listPublic (last accessed on 12 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

De Marco, Estelle, Analyse du nouveau mécanisme de prevention de la contrefaçon à la lumière des droits et libertés fondamentaux, 4 June 2009, Juriscom.net, http://juriscom.net/2009/06/hadopi-analyse-du-nouveau-mecanisme-de-prevention-de-la-contrefacon-a-la-lumiere-des-droits-et-libertes-fondamentaux/ (last accessed on 28 January 2018).

De Marco, Estelle, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067).

Diamond, Larry, "Defining and Developing Democracy", in Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, *The democracy sourcebook*, Massachusetts Institute of Technology, 2003, p.30.

Dreyer, Emmanuel, "Le respect de la vie privée, objet d'un droit fundamental", Com. com. élec., n° 5, May 2005, I, 18.

Duclos, José, L'opposabilité - Essai d'une théorie générale, Thesis, LGDJ, 1984, n° 177.

European Commission, recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU), §I, 3 (c), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF (last accessed on 22 February 2018).

European Court of Human Rights, *Factsheet, « Protection of personal data »*, Press Unit, April 2017, p. 1, available on the Council of Europe website: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf (last accessed on 12 February 2018).

European Data Protection Supervisor, *Opinion on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, 31 May 2011, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf (last accessed on 24 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

European Data Protection Supervisor, *Opinion on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters* (COM (2005) 475 final, 19 December 2005, http://www.statewatch.org/news/2006/sep/eu-com-dp-edps-opinion.pdf (last accessed on 21 February 2018).

European Union Agency for Fundamental rights and Council of Europe, Handbook on European data protection law, 2014, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (last accessed on 26 January 2018).

Etzioni, Amitai, *The limits of privacy*, Basic Groups, 1999.

Finn, Rachel, Wright David and Friedewald, Michael, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert *et al.*, *European data protection: coming of age?*, Springer, Dordrecht, 2012, pp. 3,-32.

Gavinson, Ruth E., "Privacy and the limits of law", The Yale Law Journal, Vol. 89, n° 3 (Jan. 1980), pp. 421-471, http://www.jstor.org/stable/795891 or http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957 (last accessed on 24 February 2018).

Greer, Steven, *The margin of appreciation: interpretation and discretion under the European Convention on Human Rights*, Human Rights files n°17, Council of Europe publishing, 2000, http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf.

Greer, Steven, *The exceptions to Article 8 to 11 of the European Convention on Human Rights*, Human Rights files n°15, Council of Europe publishing, 1997, http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf.

Gutwirth, Serge, Michael Friedewald, David Wright, Emilio Mordini *et al.*, *Legal, social, economic and ethical conceptualisations of privacy and data protection*, Deliverable D1 of the PRESCIENT project [Privacy and emerging fields of science and technology: Towards a common framework for privacy and

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

ethical assessment], http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf (last accessed on 12 February 2018).

Hansson, Mats G., *The Private Sphere: An Emotional Territory and Its Agent*, Springer, 2008, p. 3.

Hildebrandt, Mireille and Koops, Bert-Jaap, *"The challenges of Ambient Law and legal protection in the profiling era"*, May 2010, Modern Law Review 73 (3), p. 428-460.

Huet, Véronique, "L'autonomie constitutionnelle de l'État : déclin ou renouveau ?", *in* Revue de Droit Constitutionnel 2008/1 (n° 73), pp. 65-87, also available at https://www.cairn.info/revue-francaise-de-droit-constitutionnel-2008-1-page-65.htm (last accessed on 26 January 2018).

Kayser, Pierre, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 329.

Levrat, Nicolas, *The Right to National self-determination within the EU: a legal investigation*, https://ecpr.eu/Filestore/PaperProposal/d0d39dde-15ad-4462-994a-a9e4a2fa24a6.pdf (last accessed on 25 January 2018).

McBride, Jeremy, "Proportionality and the European Convention on Human Rights", *in The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et seq.,

Maitrot de la Motte, Alexandre, "Le droit au respect de la vie privée", *in La protection de la vie privée dans la société d'information*, under the dir. of Pierre Tabatoni, tome 3, 4 et 5, Cahier des sciences morales et politique, PUF, Jan. 2002, p. 271.

Mendel, Toby, *A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights*, Council of Europe, https://rm.coe.int/16806f5bb3.

Peltier, Virginie, *Le secret des correspondances*, PU d'Aix-Marseille, 1999.

Moore, Adam D, *Privacy Rights: Moral and Legal Foundations*, Pennsylvania State University press, 2010.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Reidy, Aisling, *The prohibition of torture, A guide to the implementation of Article 3 of the European Convention on Human Rights*, Human rights handbooks, No. 6, Council of Europe 2002, https://rm.coe.int/168007ff4c (last accessed on 26 January 2018).

Rigaux, François, "Les paradoxes de la protection de la vie privée", *in La protection de la vie privée dans la société d'information*, under the direction of Pierre Tabatoni, tome 1, Cahier des sciences morales et politique, PUF, Oct. 2000.

Roagna, Ivana, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe human rights handbooks, Council of Europe, 2012, www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf (last accessed on 12 February 2018).

Rocher, Jean-Claude, Aux sources de l'éthique juridique - Les présocratiques, June 2001, ed. Fac 2000, coll. Reflechir.

Rössler, Beate, *The Value of Privacy*, Polity Press: Cambridge, 2005.

Rouvroy, Antoinette, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", in *Studies in Ethics, Law and Technology*, Volume 2, Issue 1, 2008, Article 3, p. 25, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 (last accessed on 12 February 2018).

Rudinsky, M., *Civil Human Rights in Russia: Modern Problems of Theory and Practice*, Transaction Publishers, 2008, IBSN 978-0-7658-0391-7.

Saarenpää, Ahti, "Perspectives on privacy", *in* Ahti Saarenpää, *Legal privacy*, LEFIS Series, 5, Prensas Universitarias de Zaragoza, p. 20 (http://puz.unizar.es/detalle/898/Legal+privacy-0.html), available at http://lefis.unizar.es/images/documents/outcomes/lefis_series/lefis_series_5/capitulo1.pdf (last accessed on 12 February 2018).

Sheinman, Leslie, "Ethique juridique et déontologie", Droit et Société N°36-37/1997, pp. 265-275, available at http://www.persee.fr/doc/dreso_0769-3362_1997_num_36_1_1408 - last accessed on 24 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Solove, Daniel J., "A taxonomy of privacy", University of Pennsylvania Law Review, vol. 154, n° 3, Jan.
2006, http://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf (last accessed on 14 February 2018).

Solove, Daniel J., *Understanding privacy*, Harvard University Press, 2008.

Solove, Daniel J., "Conceptualizing Privacy" California Law Review, Vol. 90, 2002, p. 1087.

Soülas de Russel, Dominique J. M., Raimbault, Philippe, « Nature et racines du principe de sécurité juridique : une mise au point », RIDC, 2003, vol. 55, no1, p. 90.

Spiegel Online, *Gericht rüffelt Facebook für Voreinstellungen*, 12 February 2018, http://www.spiegel.de/netzwelt/web/facebook-voreinstellungen-landgericht-berlin-sieht-verbraucherschutz-verstoesse-a-1193024.html (last accessed on 16 February 2018).

Sudre, Frédéric, "La dimension internationale et européenne des libertés et droits fondamentaux", *in Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005.

Tabatoni, Pierre, "Vie privée : une notion et des pratiques complexes", *in La protection de la vie privée dans la société d'information*, under the direction of Pierre Tabatoni, tome 1, Cahier des sciences morales et politique, PUF, Oct. 2000, p. 3.

Terré, François, "La vie privée", *in La protection de la vie privée dans la société d'information*, under the dir. of Pierre Tabatoni, tomes 3, 4 et 5, Cahier des sciences morales et politique, PUF, 1re éd., janv. 2002, p. 138.

Warren, Samuel D. and Brandeis, Louis D., "The right to privacy", Harvard Law Review, vol. IV, 15 Dec. 1890, n°5.

Wery, Etienne, *Facebook condamnée : ses conditions générales posent problème*, 15 February 2018, https://www.droit-technologie.org/actualites/facebook-condamnee-conditions-generales-posent-probleme/ (last accessed on 16 February 2018).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Wright, David and De Hert, Paul, *Privacy Impact Assessment*, Law, Governance and Technology Series volume 6, Springer, 2012.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Annex: Fundamental principles relating to processing of personal data[647]

In Art. 5 of the GDPR the elementary principles for processing of personal data are determined in an abstract manner for the safeguarding of a high level of protection over the entire Regulation. Such a level of protection requires the application of the European Convention on Human Rights (hereinafter ECHR) requirements in terms of limiting "conditional"[648] fundamental rights, keeping in mind that, where the Charter of Fundamental Rights of the European Union (hereinafter EUCFR) does not offer a stronger protection than the ECHR, the meaning and scope of its provisions are the same of those of the latter[649]. As a result, the GDPR and the Police Directive ensure that each personal data processing act is legally based, pursues a legitimate aim, and is necessary and proportionate to the aim pursued.[650] In this way, the GDPR and the Police Directive standards constitute concretisations of the ECHR (including its Article 8 protecting the right to privacy), of the EUCFR (including its Article 8 protecting the right to personal data protection) and of Art. 16 para. 1 of the Treaty on the Functioning of the European Union (hereinafter TFEU).

In contrast to the former EU Data Protection *Directive*[651] (hereinafter DPD), the general principles of the *Regulation* are now directly applicable pursuant to Art. 288 para. 2 of the TFEU. With this change in the type of legislation comes noticeably an increased relevance of the following principles, since they are now **binding in every scenario,** where processing of personal data within the territorial

---

647 This analysis was developed for the INFORM-project by Estelle De Marco (Inthemis, FR) and Matthias Eichfeld (University of Göttingen, DE).

648 Some of the rights identified in the European Convention on Human rights are called "absolute", such as the right to life or to not be subjected to torture, while others are called "conditional" because they can be subjected to dispensations and/or limitations, as the right to respect for private life and the right to freedom of expression: Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', *in Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, pp. 44-45.

649 EU Charter of Fundamental Rights, article 52, 3.

650 For further developments regarding the content of the notions of legal basis, legitimate aim, necessity and proportionality, see Estelle De Marco in Estelle de Marco *et. al.*, Deliverable D2.2 – Identification and analysis of the legal and ethical framework, MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n° JUST/2014/RRAC/AG/HATE/6652, version 2.2.4 of July 2017, Section 4.1.3, available at http://mandola-project.eu/publications/ (last accessed on 6 December 2017).

651 Directive 95/46/EC.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

and material scope of the GDPR takes place.[652] In case of their violation claims for damages and sanctions may immediately follow.[653] Even though in numerous articles of the GDPR a certain concretisation of those principles takes place, it is mandatory to consider the fundamental determination in Art. 5 for each act of data processing.

1 Principles of lawfulness, fairness, transparency

Although the three principles standardised in Art. 5 para. 1 lit. a have reciprocal contexts in relation to each other[654], each notion has its own meaning.

1.1 Lawfulness

A personal data processing constitutes a limitation of a fundamental right. As such, such limitation can only be legitimate if it first has a legal basis which must be clear, precise and predictable in its application[655]. This principle is recalled in the GDPR and in the Police Directive, as well as in Directive 95/46/EC. This principle means that the processing must be authorised by law. This law will be in most case the GDPR itself, where processing operations can fully comply with its provisions. But the GDPR provides for cases where an additional legal basis will be required, in order to, *inter alia*, provide for additional safeguards in particular contexts (for example in case of derogations to the provisions of Article 6 and of derogations allowed under Article 23). Where the GDPR constitutes a sufficient legal basis for a given data processing operation, the latter must in addition be based on the consent of the data subject or on any other legitimate basis provided for by law, as foreseen by both Art. 8 para. 2 of the EUCFR. and Article 6 of the GDPR, which provides

652 See *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 5 para. 1; *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 5, para. 2; *Frenzel*, in: Paal/Pauly, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 5 para. 2.
653 See Art. 82, para. 1 and Art. 83, para. 5 lit. a GDPR.
654 See Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 32 et seq.
655 See for instance Judgement of the CJEU, 20 May 2003, joined cases C-465/00, C-138/01 and C-139/01 (case "Österreichischer Rundfunk"); Judgement of the ECtHR, 4 December 2008, *Marper*, appl. n° 30562/02 and 30556/04.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

more specifically for 6 possible legal foundations, including the data subject's consent and the legitimate interests pursued by the controller or by a third party. In order to use the latter legal basis a "test of legitimate interest" must be performed, and in this regards the Article 29 Working Party (becoming the European Data Protection Board in the GDPR)' and GDPR Recital 47 guidelines must be followed.

In addition, specific requirements from the rules governing the lawfulness of the consent[656] and processing of particularly sensitive data must be considered.[657] If there is a transfer of personal data to third countries or international organisations, the specific conditions in Chapter V of the GDPR must be taken into account.[658]

1.2 Fairness

- The principle of fairness has been defined in Directive 95/46/EC as the prohibition of secrecy and the requirement of comprehensive information[659], and the meaning of the principle doesn't seem to have changed. The GDPR adds that, in particular, natural persons should be made aware of the existence of the processing, of the specific purposes for which personal data are processed and of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing, as well as of any further information necessary to ensure fairness such as the specific context and circumstances of the processing operations, and the question of whether personal data are mandatory and incurred consequences in case of silence.[660]
- Furthermore, the principle of fairness has been seen by an author as an omnibus clause, which primarily covers situations in which the data subject experiences a disadvantage by

[656] Art. 7 and 8 GDPR.
[657] Art. 9 and 10 GDPR.
[658] Art. 44 to Art. 50 GDPR.
[659] See Recital 38 to Directive 95/46/EC. See also Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 34.
[660] See Recital 39. and Recital 60.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

processing their personal data, which is not in line with the overall picture of the balance of power between the data subject and the data controller, without necessarily violating a specific legal prohibition.[661] In other words, it enables to ensure transparency as a proportionality safeguard where an imbalance remains between the controller and the data subject, despite the respect of the other GDPR requirements.

1.3 Transparency

The principle of transparency adds, to the requirement of fairness or in other words of completeness of the information to be provided, a requirement of clarity of this information (it must be easily accessible, easy to understand, clear and in plain language)[662]. This principle applies to all the information that must be provided in order to ensure a fair and transparent processing.[663] The implementation as a new independent principle (that can be therefore seen as an extension of both the principle of fairness and the obligation of data subject's information) emphasises the importance of transparency as a fundamental proportionality safeguard, and therefore as a fundamental condition for the control over the use of one's own data and thus states a precondition for predictability and thereby effective protection.[664]

As a result, the principles of fairness and transparency concern together both the method and the content of the information.[665]

[661] See *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 17; *Frenzel*, in: Paal/Pauly, op. cit., Art. 5 para. 20; *Kramer*, in: Auernhammer, DSGVO – BDSG, *Carl Heymanns Verlag*, Cologne 2017, Art. 5 para. 8-10.
[662] See Recitals 39 and 58 of the GDPR.
[663] See Recital 58 p. 1 and Recital 39 p. 2. See also Art. 12 para. 1 GDPR.
[664] See Art. 29 Data Protection Working Party, Guidelines on transparency under Regulation 679/2016 (WP 260), p. 5, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed 18 December 2017); see also Commission Staff Working Paper SEC (2012)72 final, Annex 2, Section. 2.4, available at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf (last accessed on 18 December 2017).
[665] See Art. 12 para. 1; Art. 13 para. 1 and Art. 14 para. 1; see also *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 11.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2 Principle of purpose limitation[666]

Art. 5 para. 1 lit. b GDPR stipulates that the collection of personal data is only permitted for specific, explicit, legitimate purpose and compatible use.[667]

2.1 Specified purpose

The requirement that the data may only be collected for specified purposes already follows directly from the wording of Article 8 para. 2 EUCFR and from the ECHR principle of necessity (which implies that the rights' limitation - i.e. the processing operations in our context - answers a specific important need -which must be precisely identified and justified-, in addition to be adapted to satisfy this need).

Each purpose must be *"sufficiently defined",* **not later than the time of the data collection**[668], *"to delimit the scope of the processing operation"* and therefore to enable the assessment of the data collection with the law and to enable the *"implementation of any necessary data protection safeguards"*.[669] This specification requires *"an internal assessment"* to identify and detail the kind of processing that *"is and is not included within the specified purpose"*.[670] This means that the controller must not gather data for possible future purposes that are not yet determined at the time of the collection and thus cannot be foreseen by the data subject.

---

666 Some elements of the following discussion are coming from *Estelle de Marco* in: *Estelle de Marco* et. al., Deliverable D2.2 – Identification and analysis of the legal and ethical framework – MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n° JUST/2014/RRAC/AG/HATE/6652, version 2.2.4 of July 2017, Section 4.2, p. 68 et seq.: The right to personal data protection, available at http://mandola-project.eu/publications/ (last accessed on 6 December 2017).

667 Since these notions have already been part of the former DPD, the Article 29 Data Protection Working Party "Opinion 03/2013 on purpose limitation" serves as an adequate reference for further illustration of the principles, as far as no changes are indicated.

668 See Recital 39 p. 6.

669 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203), 2 April 2013, II.2.1, p. 12 and III.1.1, p. 15 et seq., available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (last accessed on 6 December 2017).

670 *Ibid.*, III.1.1, p. 15.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Purposes too vague such as *"improving users' experience"* or *"IT-security purposes"* are usually not specific enough.[671] In the same line, an overall purpose to cover a number of separate purposes is not compliant.[672]

Only in certain situations, when a detailed description is clearly counter-productive because of its complexity, the specification or the purpose can be reduced to key information.[673] Nevertheless, a detailed description of the processing must be accessible via *"layered notice*" such as a link to a corresponding Internet page.[674]

In addition, since the principle of purpose specification is a practical application of the ECHR principle of necessity (of which weaknesses, in the framework of a complete necessity and proportionality tests, must be balanced by proportionality safeguards), it has to be noted that the performance of a necessity and of a proportionality tests can be used in order to find alternative safeguards that could satisfy data protection authorities and judges, in certain circumstances where the principle of purpose specification cannot be respected as written in the GDPR, such as certain kind of data collection performed in a Big data environment, using specific tools, some of the collected data being used as a second step for specific purposes, where the first motive of the collection can be found legitimate in itself even if too general (such as making profit of a EU based technology aimed at feeding innovative services while avoiding recourses to similar technologies produced in countries where the GDPR does not apply).

2.2 Explicit purpose

The purpose must be *"sufficiently unambiguous and clearly expressed"*[675], *"in such a way to as to be understood in the same way"* by the data controller and its staff including third parties processors, the supervisory

[671] See for more examples *Ibid.*, III.1.1., p. 16.
[672] *Ibid.*, III.1.1, p. 16.
[673] *Ibid.*, III.1.1, p. 16.
[674] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.1.1, p. 16.
[675] *Ibid.*, II.2.1, p. 12.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

authority and the data subjects.[676] This principle enables therefore all the parties *"to have a common understanding of how the data can be used"*, and reduces the risk to process data for a purpose that is not expected by the data subject.[677]In this way it enables data subjects to make informed choices.[678] The important thing is *"the quality and consistency of the information provided"*[679], in addition to its accessibility. Clearly there is a close relation between the explicit purpose and the principle of transparency and predictability, as these principles all aim to provide the data subject with complete information about the data processing (and at the end to ensure the proportionality of processing operations).[680] Especially for the accountability of the data processor, which Art. 5 para. 2, Art. 24 para. 1 and Art. 30 para. 1 lit. b GDPR require, the determination of an explicit purpose is mandatory.[681]

2.3 Legitimate purpose

As highlighted by the Article 29 Data Protection Working Party, *"the requirement of legitimacy means that* ***the purposes must be in accordance with the law in the broadest sense****. This includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts".*[682]

2.4 Compatible use

The legal requirement of compatible use responds to the circumstance that it is technically possible to further process data for any purpose, once they have been collected and stored, and thereby interfering repeatedly in the right to protection of personal data. Pursuant to Art. 5 para. 1 lit. b

676 *Ibid.*, III.1.2, p. 17.
677 *Ibid.*, III.1.2, p. 17.
678 *Ibid.*, III.1.2, p. 17.
679 *Ibid.*, III.1.2, p. 18.
680 *Ibid.*, II.3, p. 13.
681 See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 14.
682 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.1.1, p. 20.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

further processing of the collected data is not permitted, if the manner of processing is not compliant with the purpose of the initial collection. It follows from the definition of 'processing' in Article 4 para. 2 GDPR that further processing includes not only the processing of the data for other purposes, but any processing following the collection of the data, which therefore must be compliant with the initial act of collection.[683]

Since the conditions of all principles for the processing of personal data and the requirement of a legal basis for each processing must be fulfilled jointly[684], **two cumulative conditions** must be satisfied: further processing must not be incompatible with the purpose established during the collection of the data and there must be a sufficient legal basis for further processing.[685]

In this context, it is important to note that applying an anonymisation technique constitutes a further processing, which means that such an operation implies on the one hand that the personal data have been first collected in compliance with law, and on the other hand that such an anonymisation needs to be compliant with the fundamental principles (including the need for a legal basis) and the principle of compatible use.[686]

2.4.1 Meaning of recital 50 p. 2 in this context

This interpretation of Art. 5 para. 1 lit. b should also be maintained in the light of Recital 50 p. 2, which, according to its wording, gives the impression that there is no requirement for a separate legal basis in case of a compatible change of purpose. If that were the case, Article 5 para. 1 lit. b in

---

683 This notion of 'further processing' is also established in: Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21: "*any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility*".

684 See for the former DPD: Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 30 et seq.

685 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21; III.2.3., p. 33; See furthermore Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., II.2.1, p. 12, fn. 28: "*Article 8 (2) of the Charter also makes it clear that the requirement of purpose specification is a separate, cumulative requirement that applies in addition to the requirement of an appropriate legal ground.*"; See also *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 19; *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 42.

686 Art. 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques (WP 216), 10 April 2014, 2.2.1, p. 7, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last accessed on 6 December 2017).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

combination with the wide criteria of Art. 6 para. 4 would have the character of a general clause-like extension of all legal bases of Article 6 para. 1.

Against such an understanding of the recital argues that the assessment of the purpose compatibility represents an additional **limiting criterion**, which was already established in similar terms in the former DPD.[687] Since there is no indication in the GDPR except for the wording in recital 50 p. 2 for such a new understanding of the principle of compatible use, the wording can only be understood as meaning that no new legal basis is required if the subsequent processing involves the execution of the initial processing and meets the conditions of the legal basis for the initial processing. A different interpretation of recital 50 p. 2 would be incompatible with the principle of lawfulness of Art. 5 para. 1 lit. a and the overall protective purpose of the GDPR, which is stated in Art. 1 para. 2.[688]

2.4.2 Key factors for purpose compatibility assessment

For further processing, in addition to the existence of a new corresponding legal basis, a detailed examination of the compatibility of the purposes has to be carried out. According to Art. 6 para. 4, the test is mandatory where "the processing for a purpose other than that for which the personal data have been collected is not based on the data subjects consent or on a Union or Member State law[689]".

---

[687] Following the rapporteur of the EU-Parliament involved in the trilogue negotiations *Jan Philipp Albrecht*: *Albrecht*, Das neue EU-Datenschutzrecht – von der Richtlinie zu Verordnung, Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog, in: Computer und Recht 2016, 88 (92); See furthermore the assessment of state council and desk officer of the German Ministry of Justice and Consumer Protection *Peter Schantz*: *Schantz,* Die neue Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, in: Neue Juristische Wochenschrift 2016, 1841 (1844); See also *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 49; *Buchner/Petri* in: Kühling/Buchner, op. cit., Art. 6, para. 182 et seq.; *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 20.

[688] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 20; *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 49.

[689] Such a law must protect the important public interests referred to in Article 23 para. 1 of the GDPR, the data subject or the rights and freedoms of other persons and must comply with the proportionality test required by Article 52 para. 1 of the EUCFR and Article 8 of the ECHR. See Judgement of the CJEU, 6 October 2015, C-362/14 (case "Schrems"); Judgement of the CJEU, 8 August 2014, C-293/12 (case "Digital Rights Ireland").

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

This determination is followed by a non-exhaustive list of criteria for such a process, which is essentially based on the factors developed by the Art. 29 Data Protection Working Party.[690]

- *Any link between the purposes for which the data have been collected and the purposes of further processing, Art. 6 para. 4 lit. a:*

  The issue is to analyse the 'substance' of this relationship, to notably determine if the further processing was "*already more or less implied in the initial purposes, or assumed as a logical next step in the processing according to those purposes*", or if there is only a "*partial or even non-existent link with the original purposes*".[691]

  Although the compatibility requirement is usually missing between the processing for a purpose of a contract and the notice of potential criminal offenses or any potential public security threat given by the data controller to the competent authorities, in such a case there is a legitimate interest of the data controller (Art. 6 para. 1 lit. f) for the display and transmission of personal data.[692] Of course, this does not apply if the data controller is subject to a confidentiality obligation.[693]

- *The context in which the data have been collected, Art. 6 para. 4 lit. b:*

  This assessment should be based, above all, on the 'reasonable expectations' of the data subject resulting from the relationship with the data controller.[694] The more surprising and unpredictable further processing is for the data subject, the more indicates to an incompatibility with the original purpose.[695] For instance, it is incompatible to use security monitoring to control workers, a breathalyser to check working hours or to collect fingerprints of asylum seekers for the initial purpose of prevention from filling multiple

[690] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21; III.2.2, p. 23 et seq.; The GDPR lists five principles but two of them are handled under the same one by the Article 29 Data Protection Working Party.
[691] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 23 et seq.
[692] Recital 50 p. 9.
[693] Recital 50 p. 10.
[694] Recital 50 p. 6.
[695] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 24.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

asylum applications in different Member States simultaneously but using them for law enforcement purposes later on.[696]

- *The nature of the personal data, Art. 6 para. 4:*
  This criterion refers especially to the further processing of special categories of personal data (Art. 9) or personal data related to criminal convictions and offences (Art. 10), but also communication data, location data or whether the data subject is a child or belongs to a more vulnerable segment of the population requiring special protection.[697] As a result, a particularly careful examination is necessary.[698] As well, the general principles and the special requirements for the protection of sensitive data must be considered in such a further processing.[699]

- *The possible consequences of the intended further processing for the data subject, Art. 6 para. 1 lit. d:*
  Both positive and negative consequences must be taken into account for the assessment.[700] According to the risk-based approach of the GDPR (Art. 24 para. 1), potential risks must be included such as the publication of the data or other making accessible to a larger group of people, the processing by third parties or whether a combination with other data takes place.[701] This applies especially if there is a risk of discrimination or damage to the reputation of the data subject.[702]

- *The existence of appropriate safeguards, Art. 6 para. 4 lit. e:*
  Such as in a proportionality test, appropriate safeguards need to be implemented in order to ensure both (1) that the freedoms' limitation will not be higher than the one that has been assessed (through ensuring that the context, conditions and content of the intended processing will not be modified - including protection mechanisms already implemented),

696 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., Annex 4, p. 56 et seq., 68.
697 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 25, fn. 68.
698 *Ibid.*
699 Recital 50 p. 8.
700 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 25.
701 *Ibid.*,
702 Recital 75.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

and (2) that weaknesses identified during first steps of the compatibility test and compensated. These safeguards may consist in the first place in technical and/or organisational safeguards ensuring *inter alia* anonymisation each time this is possible[703] or "functional separation", which includes the consideration of, encryption and pseudonymisation[704] techniques and of aggregation techniques[705], in other words the consideration of measures ensuring that the "*data cannot be used to take decisions or other actions with respect to individuals*"[706]). These safeguards may also consist in ensuring transparency (including purpose re-specification) and data subjects' control (collection of users' new consent, opt-out possibilities, data subjects' rights…)[707].

2.4.3 Compatible use in case of privileged purposes

According to Art. 5 para. 1 lit. b archiving purposes, scientific or historical research purposes or statistical purposes are considered as privileged purposes, which means that there is a presumption of conformity for such a purpose. However, the lawfulness of the further processing for these purposes presupposes that it complies with the conditions laid down in Article 89 para. 1. The latter provides for appropriate guarantees for this process which may be supplemented and specified in the form of Member State legislation.[708] Amongst those guarantees, lies the requirement to perform a compatibility test in order to identify all safeguards that are appropriate to the specific context[709]. Besides, any such processing must of course also comply with all the fundamental principles of Art.

[703] See for example Recital 39 of the GDPR; Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 27
[704] See the Definition in Art. 4 No. 5.
[705] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 27.
[706] *Ibid.*
[707] *Ibid.*
[708] Art. 89 para. 2 and 3.
[709] This requirement has been highlighted by the Article 29 Data Protection Working Party (Opinion 03/2013 on purpose limitation, *op. cit.* III.2.3, p.28) in relation to Article 5 of Directive 95/46/EC. However, it is also applicable in the context of the GDPR since its Article 5 refers to Article 89, which requires the implementation of "safeguards (that must be) "*appropriate (...), in accordance with this Regulation*" (while the Directive required the provision of appropriate safeguards). Safeguards proposed in Article 89 of the GDPR are only elements of a proposed list that must be complemented by all the safeguards that are appropriate in the specific context.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

5[710] and more generally with all the other requirements of the GDPR, including the requirement to be based on one of the grounds listed in Article 6 para 1 of the GDPR[711] and the requirement to inform the data subject of the processing' purposes and of his or her rights.[712]

3 Principle of data minimisation

Art. 5 para. 1 lit. c states that the processed data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". According to this principle, personal data may only be processed if the purpose of the processing cannot be reasonably achieved by other means.[713] This includes the implementation of anonymisation techniques if possible, which would cease the personal reference and thus the data would be no longer subject to data protection law.[714] Obviously, there is a close relation to the principle of time limitation for data storage.

A specification of this principle takes place, inter alia, in the concepts of privacy by design and by default in Art. 25.

[710] Recital 50 p. 8.
[711] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, *op. cit.*, III.2.3, p.28. This opinion has been delivered in relation to Article 6b of Directive 95/46/EC. However, the formulation of Article 5 of the GDPR being almost the same, this decision appears to be applicable in this context too.
[712] Recital 50 p. 8.
[713] Recital 39 p. 9.
[714] See *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 58; See for the procedure of anonymization: Art. 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, op. cit., 2.2.1, p. 7 et seq.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4 Principle of accuracy

According to Art. 5 para. 1 lit. d personal data must be "*accurate and, where necessary, kept up to date*". To ensure the data quality, the data controller must actively take every "*reasonable step*" to rectify or delete inaccurate data without delay.[715] Since the usage of personal data might produce legal consequences for the data subject, the data shall reflect reality at any given time.[716]

To enforce this principle, the data subject has the right to rectification (Art. 16) and the right to erasure (Art. 17).

It is important to notice that this obligation must be complied especially with respect to the purposes and the specific circumstances of processing.[717] For instance, if the processing purpose is preservation of evidence it can be necessary to process outdated data.[718]

[715] Art. 5 para. 1 lit. d; Recital 39 p. 11.
[716] See *Voigt/von dem Bussche*, in: Voigt/von dem Bussche, The EU General Data Protection Regulation (GDPR) – A Practical Guide, *Springer*, Cham (Switzerland) 2017, 4.1.4, p. 91; *Frenzel*, in: Paal/Pauly, op. cit., Art. 5 para. 39.
[717] Art. 5 para. 1 lit. d.
[718] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 24; *Frenzel*, in: Paal/Pauly, op. cit. Art. 5 para. 40 et seq.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

5 Principle of storage time limitation

Art. 5 para. 1 lit. e determines that the storage period of personal data should be kept to a 'strict minimum'.[719] Decisive for the permissible duration of storage is the purpose of the processing. Thus, the principle of storage time limitation is an application of the principle of proportionality defined in terms of time. In order to preserve this principle, it is sufficient to remove the personal reference of the data (identifiability) according to the wording in Art. 5 para. 1 lit. e.[720]

To ensure the concept of limitation the data controller should establish time limits for erasure and for a periodic review.[721] Pursuant to Art. 13 para. 2 lit. a, Art. 14 para. 2 lit. a and Art. 15 para. 1 lit. d the data controller must inform the data subject of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

To enforce this principle, the data controller is obliged to erase personal data under the provision of Art. 17.

Similar to the constitution of privileged purposes in Art. 5 para. 1 lit. b, there are exceptions to the principle of storage time limitation as well. If the personal data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the storage for a longer period is explicitly allowed.[722] In such a case, appropriate guarantees in accordance with Art. 89 para. 1 are required.

[719] Recital 39 p. 8.
[720] See Recital 26 p. 3 and 4 for further explanations on the criterion of identifiability.
[721] Recital 39 p. 10.
[722] Art. 5 para. 1 lit. e.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

6 Principle of integrity and confidentiality

According to Art. 5 para. 1 lit. f processing must be carried out "*in a manner that ensures adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures*".[723]

In this way, the principle addresses the need for organisational safeguards for the processing operation. Specifications of the protective measures especially take place in Art. 32, Art. 28 para. 2 p. 2 lit. b and Art. 29.[724] Moreover, personal data breaches must be reported to the supervisory authority (Art. 33) and, in certain situations, to the data subject (Art. 34).

[723] See also recital 39 p. 12.
[724] For further explanations to the concrete nature and extent of adequate protective measures see the sections of the specific obligations of data controller and data processor.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

7 Accountability

The data controller is responsible for and must be able to **demonstrate compliance with the fundamental principles** relating to processing of personal data, Art. 5 para. 2.[725] The extended obligation of accountability is an expression of the enhanced self-responsibility of the data controller under the GDPR.

7.1 Liability of the data controller or data processor

Irrespective of the possibilities of the data subject for remedy against the processing activity of the data controller (Art. 77-79), any infringement of the regulation may lead to a claim for compensation of damage caused by processing, unless the controller or the processor has complied with the obligations of the regulation, Art. 82.

7.2 Accountability and data protection by design and by default[726]

A specification of the notion of self-responsibility takes place in Art. 24 which requires of the data controller to "*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with*" the regulation, "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons*". As recital 75 phrase 2 points out, this can be done by having the data controller adopt internal strategies and take measures that comply with the principles of data protection by design and by default (Art. 25 para. 1 and 2).

In any case the data controller must ensure accountability by keeping a record of processing activities (Art. 30), cooperating with supervisory authorities (Art. 31), reporting and notification of data

[725] See for the notion also Article 29 Data Protection Working Party, Opinion 03/2010 on the principle of accountability (WP 173), 13 July 2010, III.2, p. 9 et. seq., available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (last accessed on 15 December 2017).
[726] For further explanations on the concept of accountability see the sections of the specific obligations of data controller and data processor.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

breaches (Art. 33, 34), carrying out a data protection impact assessment in certain situations (Art. 35) and the corresponding prior consultation of the supervisory authority (Art. 36).

The overall responsibility and accountability of the data controller include the responsibility for the processing of the data processor (who is acting on behalf of the data controller).[727] Nevertheless, the processor is also demanded to take appropriate technical and organisational measures to take care of the risk associated with data processing.[728]

[727] Art. 28 para. 1.
[728] Art. 32 para. 1.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

8 Prohibition of automated decision-making

Not in Art. 5 but in Art. 22 of the GDPR the right of the data subject is stated, "*not to be subject to a decision solely based on automated processing, including profiling, which produces legal affects concerning him or her or similarly significantly affects him or her*". From the perspective of the data controller, this determination leads in turn to the fact that there is a prohibition on fully automated decision-making that has a legal or similarly significant effect concerning the data subject.[729] A decision is based solely on automated processing if there is no human involvement and the outcome of the processing is not reviewed by a competent and authorised person.[730] The intention is that the data subject shall have the right to a final decision by a human being if the decision implies an increased risk for his or her situation.[731]
The wording of Art. 22 para. 1 and the complementary recital 71 indicate a narrow interpretation of 'similarly significant effects', since it is in a close context to 'legal affects'. According to the Art. 29 Data Protection Working Party it depends upon the characteristics of each case, including:

- the intrusiveness of the profiling process;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- the particular vulnerabilities of the data subject targeted.[732]

As a result, certain practices of targeted online advertising may have such an effect, especially when it comes to differential pricing strategies.[733]

There are three exceptions to the prohibition listed in para. 2 of Art. 22: If the automated-decision making is necessary for the performance of a contract between data controller and data subject, if

[729] See Art. 29 Data Protection Working Party, Guidelines on automated individual decision-making and Profiling for the purposes of Regulation 679/2016 (WP 251), 3 October 2017, II., p. 9, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed 18 December 2017).
[730] *Ibid.*, II.A., p. 9 et seq.; See also *Schrey*, in: Rücker/Kugler, New European General Data Protection Regulation – A Practitioner's Guide, *Nomos, C.H. Beck, Hart*, Baden-Baden, Munich and Oxford 2017, p. 149, para. 692.
[731] See Art. 29 Data Protection Working Party, Guidelines on automated individual decision-making and Profiling for the purposes of Regulation 679/2016., op.cit., II.B., p. 10 et seq.
[732] *Ibid.*, II.B., p. 11.
[733] *Ibid.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

there is an authorisation provided by Union or Member State law or if the data subject has given his or her explicit consent. Regarding special categories of data (Art. 9 para. 1) the exceptions for automated decision-making are not applicable, unless the conditions of Art. 9 para. 2 lit. a or g are met. In all cases, it is necessary to "*implement suitable measures to safeguard data subject's rights and freedoms and legitimate interests*"[734].

[734] Art. 22 para. 2 lit. b, para. 3, para. 4.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.