Privacy and data protection in Europe

de Terwangne, Cécile

Published in:
Research Handbook on Privacy and Data Protection Law

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

1. Privacy and data protection in Europe: Council of Europe's Convention 108+ and the European Union's GDPR

Cécile de Terwangne

I. INTRODUCTION

Two main texts deserve particular attention in Europe: Council of Europe's Convention 108, and the European Union (EU) General Data Protection Regulation (GDPR). The presentation and analysis of these texts is of great interest since EU Member States are bound by both. Furthermore, Convention 108, ratified by States both within and outside the Council of Europe, is in the process of becoming the main international legally binding instrument in the field of data protection. Its influence reaches far beyond European boundaries, making it worth discovering its provisions. A modernized version of Convention 108, known as Convention 108+, is currently available for signature and ratification. The EU GDPR also has a far-reaching geographical scope, and many actors will have to comply with it in different parts of the world. Both texts present in consequence a great interest for lawyers in Europe and abroad.

The following pages discuss them jointly. A joint presentation of Convention 108+ and GDPR has been considered preferable in order to avoid excessive repetitions, since their content is similar on many points. Divergences or specificities are of course clearly indicated. This chapter will first present a general overview of the European legal landscape (section II) before highlighting the fundamental rights dimension attributed in Europe to the issue of the protection of personal data (section III). Section III is dedicated to clarifying the main notions and the material and geographical scope of the European texts. Section IV presents the basic general principles of the data protection, whereas section V is devoted to the specific regime offering a higher protection to sensitive data. The remarkable list of data subjects' rights is presented in section VI, and the duties and obligations imposed to data controllers and processors are detailed in section VII. The rules to respect in case of transborder data flows outside European borders are examined in section VIII. A last section presents the specialized supervisory authorities put in place to monitor the respect of the whole protection regime, and to provide advice on these matters.

II. GENERAL SETTING

In Europe, two regional organizations have taken action in the field of data protection: the Council of Europe and the EU.

The **Council of Europe** adopted one of the first international texts on the subject on 28 January 1981: Convention 108 for the Protection of Individuals as Regards the Automatic

Processing of Personal Data. This Convention is the only legally binding text in the field with an international scope. All 47 member States of the Council of Europe have ratified it. This text has moreover the particularity of being open to signature for non-European States. At this stage,[1] it has been ratified by Argentina, Cabo Verde, Uruguay, Mauritius, Mexico, Morocco, Senegal and Tunisia, and Burkina Faso has also been invited to accede, which is the first stage before becoming party to the Convention.

As any international convention, the text contains high-level principles. It was further supplemented in 2001 by an Additional Protocol Regarding Supervisory Authorities and Transborder Data Flows (ETS No. 181).

A Convention committee (named T-PD) gives orientations to face the challenge of applying Convention 108 in an ever-moving reality. This committee has published recommendations about the application of the Convention in particular contexts such as the police sector,[2] insurance,[3] social security,[4] but also about the processing of medical data,[5] or statistics.[6]

In 2016, a modernizing process launched six years earlier to take account of the new technological and societal landscape lead to a substantive rewriting of the text.[7] The modernization notably melted the content of the original Convention and that of its mentioned Additional Protocol. Overall, it has brought the changes needed in our connected world to better balance the data subjects' rights and interests and those of the person or entity processing personal data about them. The Modernised Convention[8] was finally adopted by the Committee of Ministers of the Council of Europe on 18 May 2018, and opened for signature on 10 October 2018.[9] It has already been ratified by fifteen States Parties to Convention 108, including two non-European States (Mauritius and Uruguay) and signed by twenty-eight others.

The EU had found it necessary to adopt a set of more precise rules as regards data protection than those included in Convention 108. The latter left a margin of manoeuvre to the Parties that had brought divergences between national legislations, and such divergences inhibited the free flow of personal data through the EU.

A first attempt to harmonize European national legislations took place in 1995 with Directive 95/46/EC of 24 October 1995.[10] The adaptation of this text, 15 years later, to the

---

1 November 2020.

2 Recommendation No. R(87) 15, regulating the use of personal data in the police sector, 17 September 1987.

3 Recommendation No. CM/Rec(2016)8 on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, 26 October 2016.

4 Recommendation No. R(86) 1, on the protection of personal data for social security purposes, 23 January 1986.

5 Recommendation CM/Rec(2019)2 on the protection of health-related data, 27 March 2019.

6 Recommendation No. R(97) 18, on the protection of personal data collected and processed for statistical purposes, 30 September 1997.

7 See the consolidated text of the modernisation proposals of Convention 108 for the Protection of Individuals with Regard to the Processing of Personal Data finalised by the CAHDATA, meeting of 15–16 June 2016.

8 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+).

9 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series (CETS) No. 223, 10 October 2018.

10 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

new connected reality that has brought 'a profound change of scale in terms of the role of personal data in our economies, societies and daily lives'[11] proved to be necessary and led to the adoption on 27 April 2016 of the GDPR.[12] The change from a directive to a regulation aimed at achieving a greater uniformization of the European legal landscape in the field of data protection. However, certain possibilities of disparities remained: for example, for data processing in the public sector[13] or to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.[14] [15] Besides this specific instrument, Article 8(1) of the Charter of Fundamental Rights of the EU provides that everyone has the right to the protection of personal data concerning him or her.[16] This Charter, legally binding since 2009, was the first regional catalogue of human rights that proclaimed the right to data protection. The two European data protection regimes are convergent. The Council of Europe's Convention contains high-level principles, while the EU GDPR is a set of detailed rules, but both texts have been elaborated having in mind a total compatibility to avoid that Parties having to comply with both texts would be submitted to conflicting requirements. Before presenting the main elements of this double European data protection regime, it is necessary to highlight what characterizes the European approach of this topic: its fundamental rights dimension.

III. THE PROTECTION OF PERSONAL DATA IN EUROPE: A FUNDAMENTAL RIGHTS APPROACH

In Europe, the right to data protection has been considered a fundamental right, primarily derived from the right to privacy and later recognized as an autonomous right in the EU Charter of Fundamental Rights. This approach differs from the one that considers data protec-

---

[11] The OECD Privacy Framework, 2013, Foreword.

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1. Another text was adopted simultaneously, regarding data processing in the field of police and justice: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89. This text is not analysed in the present contribution.

[13] Art. 6(2) GDPR.

[14] Art. 85 GDPR.

[15] Cécile de Terwangne, Karen Rosier and Bénédicte Losdyck, 'Le règlement européen relatif à la protection des données à caractère personnel: quelles nouveautés ?', *Journal de droit européen*, 2017/8, 302.

[16] Art. 8 of EU Charter of Fundamental Rights states:
Protection of personal data: Art. 8(1) Everyone has the right to the protection of personal data concerning him or her. Art. 8(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Art. 8(3) Compliance with these rules shall be subject to control by an independent authority.

tion concerns a matter of consumer protection. Autonomy, in the sense here of informational self-determination, and dignity are the main values underlying the legal protection of individuals as regards the processing of their personal data. They should help to re-balance the relationship between humans, on the one hand, and machines or algorithms, on the other. The intention is obviously not to stop progress, but to accompany it and surround it.

III.1 Data Protection as a Right to Informational Self-determination

At the level of the Council of Europe, it has been stated that a major objective of Convention 108 is 'to put individuals in a position to know about, to understand and to control the processing of their personal data by others. Accordingly, the Preamble expressly refers to the right to personal autonomy and the right to control one's personal data, which stems in particular from the right to privacy'.[17] The revised version of the Preamble of Convention 108 affirms that:

> it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalization of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data.[18]

Convention 108 is about data protection notably as a right of control guaranteed to the individuals based on his or her personal autonomy or personal self-determination.[19] Data protection is indeed here an offshoot of the right to privacy taken in this dimension of personal autonomy rather than in the sense of a confidentiality requirement traditionally attached to the notion of privacy. The right to data protection is linked to a right to 'informational self-determination' that has been recognized as part of the right to privacy.[20]

At EU level, while Directive 95/46/EC stated that '[i]n accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in

---

[17] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 10 (hereafter Explanatory Report).

[18] Modernised Convention 108, Preamble.

[19] For the explicit recognition of a *right* to self-determination or to personal autonomy contained in the right to respect for private life under Art. 8, see: *Evans v. UK* App no 6339/05 (ECHR, 10 April 2007); *Tysiac v. Poland* App no 5410/03 (ECHR, 20 March 2007); *Daroczy v. Hungary* App no 44378/05 (ECHR, 1 July 2008); *Satakunnan Markkinapörssi oy and Satamedia oy v. Finland* App no 931/13 (ECHR, 27 June 2017).

[20] *Satakunnan Markkinapörssi oy and Satamedia oy*, para. 137:

> [...] Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged.

It is worth highlighting here that lessons deriving from the European Court of Human Rights case-law present a great interest also to enlighten the understanding of Arts 7 and 8 of the European Union Charter of Fundamental rights (providing the right to privacy and the right to data protection). Art 52.3 of this Charter states:

> In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.

particular their right to privacy with respect to the processing of personal data',[21] the GDPR no longer mentions the right to privacy, but refers to the right to data protection.[22] Following its first recital: 'The protection of natural persons in relation to the processing of personal data is a fundamental right'.

III.2 Data Protection and Human Dignity

Convention 108 – in its original version of 1981 – does not mention the protection of human dignity. The evocation of human dignity in the new Preamble has been introduced as a reminder of the fact that human beings are subjects, and should not be reduced to mere objects of surveillance and control.[23] It follows from the idea that human beings should not be subjected to a machine, but that, instead, machines should be at their service and shall not undermine individuals' core values. This proclamation of the fundamental value of dignity as underlying data protection is without doubt necessary in view of certain uses of technology. Information systems are increasingly carrying out comprehensive monitoring of individuals and whole populations, creating systems based on people's transparent behaviour, which may be contrary to human dignity. Similarly, when profiling leads to deriving information without the knowledge of data subjects in order to take all sorts of decisions concerning them, it can seriously impair the dignity of the profiled persons. The GDPR does not expressly mention human dignity, but in the very first recitals of the text the EU legislator included a statement indirectly evocating this value and the idea that data processing should be at the service of human beings: 'The processing of personal data should be designed to serve mankind'.[24]

IV. DEFINITIONS AND SCOPE OF EUROPEAN DATA PROTECTION LEGISLATIONS: KEY ELEMENTS

IV.1 Definition of Personal Data

'Personal data' means 'any information relating to an identified or identifiable individual ("data subject")'.[25] Article 4(1) of the GDPR specifies that:

> 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.[26]

---

[21] Art. 1(1) of Directive 95/46/EC.

[22] Art. 1(2) GDPR: 'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'.

[23] Explanatory Report, para. 10.

[24] Recital 4 GDPR.

[25] Art. 2(a) Convention 108; Art. 4(1) GDPR (which mentions 'natural person' instead of 'individual').

[26] On the notion of personal data within the EU, see also: Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007; Case C-434/16 *Peter Nowak v. Data protection Commissioner* [2017]; Case C-582/14 *Breyer v. Germany* [2016].

The Explanatory Report of Convention 108+ provides that an individual shall not be regarded as 'identifiable' if his or her identification requires unreasonable time, effort or means.[27] Recital 26 of GDPR goes in the same direction. Both texts specify that to determine whether somebody is identifiable account should be taken of the available technology at the time of the processing and technological developments,[28] since technological and other developments may change what qualifies as 'unreasonable' time, effort or means.[29] In addition – and this new element is particularly important in the current context – 'identifiable' does not only refer to the individual's civil identity, but also to whatever may allow singling out somebody,[30] or distinguish one person amongst others, such as an identification number, geolocation data, an IP address,[31] etc. This singling out may occur by referring to a person, but also to an access point (computer, mobile phone, connected objects, etc): individualization is possible both in relation to a person and to equipment.[32]

IV.2 Definition of Data Processing

Convention 108 originally relied on the concept of 'automated data file', which had a dated technological connotation. The term was eventually abandoned and replaced in the modernised Convention by terminology used by Directive 95/46/EC. The concept of 'data processing' appears thus in Convention 108+. Under its Article 2(c), data processing means:

> any operation or set of operations which is performed upon personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data; where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria.

This definition presents a noticeable difference with the prior text: it includes data processing not involving any automated means, the so-called 'manual processing'. Indeed, it seems appropriate to include such processing under the scope of protection, especially if the Convention is to be adopted by countries where manual processing operations are still numerous.

The revised Convention is in line with the definition of the GDPR, which states that processing means:

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[33]

---

27 Explanatory Report, para. 17.

28 Recital 26 GDPR.

29 Explanatory Report of Convention 108, para. 17. See also: Article 29 Working Party, *Opinion 05/2014 on anonymisation techniques*, WP 216, 10 April 2014.

30 Recital 26 GDPR; Explanatory Report of Convention 108, para 18: 'The notion of 'identifiable' does not only refer to the individual's civil or legal identity as such, but also to what may allow to "individualise" or single out (and thus allow to treat differently) one person from others'.

31 Frederik J Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition', *EDPL*, 2017/1.

32 Explanatory Report of Convention 108, para. 18; Recital 26 GDPR.

33 Art. 4(2) GDPR.

As mentioned earlier, it was considered highly desirable that both texts be coherent, not to have EU Member States subject to contradictory rules or heterogenous notions.

IV.3 Definition of the Main Actors: Controller and Processor

The main actors are named controller and processor in Convention 108+ and the GDPR. The definitions of these actors are quite similar in both texts.

Regarding the controller, Convention 108+ refers to the person or body having decision-making power over the processing of personal data,[34] whether this power derives from a legal designation or from factual circumstances.[35] According to Article 4(7) of the GDPR, the:

> 'controller' is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

As to the notion of 'processor', it receives a quasi-identical definition in both texts and means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[36]

IV.4 Scope of the Instruments

The two analysed texts apply to the processing of personal data wholly or partly by automated means. If no automated means are used, they still apply where the data are part of a structured set or are to become part of such a structured set.[37]

In its 1981 version, Convention 108 states that its purpose is to offer protection to personal data 'in the territory of each Party for every individual, whatever his nationality or residence' (Art. 1). The 2018 version opted for a criterion different than territory. The protection will apply on the basis of the 'jurisdiction' of the Parties. The revised Article 3 provides that 'Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's' right to protection of his or her personal data'. Convention 108+ applies thus when data processing is carried out within the jurisdiction of a Party, be it in the public or private sector. All data processing in the public sector falls directly within the jurisdiction of the Party, including data processing carried out for national security purposes. This all-encompassing scope of Convention 108+ is wider than that of GDPR.[38] Data processing carried out in the private sector falls within the jurisdiction

---

[34] Art. 2(d) of the revised Convention: '"Controller" means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing'.

[35] Explanatory Report, para. 22.

[36] Art. 2(f) of the revised Convention 108; Art. 4(8) GDPR.

[37] Article 2(1) GDPR; Art. 3(1) of the revised Convention 108.

[38] See the restriction of GDPR scope in its Art. 2(2)(a), (b) and (d): the GDPR applies neither to the processing of personal data in the course of activities which fall outside the scope of Union law, nor to processing linked to the EU common foreign and security policy, nor to processing by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

of a Party when there is a sufficient connection with the territory of that Party. It is left to the Party to determine the criteria of this connection. For instance, there could be a sufficient link if the controller is established within the territory of that Party.

The GDPR kept, for the determination of its territorial scope, a criterion from Directive 95/46/EC that referred to processing in the context of the activities of the establishment of the controller, but extending this criterion to cover also the establishment of the processor. The GDPR thus applies to the processing of personal data in the context of the activities of an establishment in the EU of a controller or a processor, regardless of whether the processing itself takes place in the EU or not.[39] What is important to trigger the GDPR applicability is that data are processed in the framework of the activities of an establishment which is in the territory of the EU. The location of processing activities or the place of storage of the data do not matter.

The GDPR also applies in certain cases where personal data are processed by a controller or a processor not established in the EU, thus extending the territorial scope of the GDPR potentially far beyond European borders.

First,[40] the EU instrument applies when the processing activities relate to the offering of goods or services – for free or against payment – to data subjects in the EU. To determine whether a controller or processor is offering goods or services to data subjects who are in the EU, the mere accessibility of their website in the Union is not sufficient; however, 'factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, […] may make it apparent that the controller envisages offering goods or services to data subjects in the Union'.[41]

Secondly, the GDPR also applies when the processing of data relates to the monitoring of the data subjects' behaviour (e.g., the tracking of their activities on the Internet) in so far as their behaviour takes place within the EU.[42]

IV.4.1 Limitation of the scope: Activities exclusively for personal purposes

In its 1981 version, Convention 108 had left it open to States Parties to exclude certain data processing operations from its scope. This was changed in the modernized version of the Convention, which excludes from its scope of application any 'data processing carried out by an individual in the course of purely personal or household activities'.[43] The GDPR provides a scope limitation in almost the same terms.[44] The justification of this exclusion lies in that it aims 'at avoiding the imposition of unreasonable obligations on data processing carried out by individuals in their private sphere for activities relating to the exercise of their private life',[45] as well as on the supposed low level of risk that such processing activities represent.

---

execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In this latter case, Directive (EU) 2016/680 (cited in note 12 *supra*) applies instead of GDPR.

39 Art. 3(1) GDPR.

40 Art. 3(2)(a) GDPR. See also Recital 23.

41 Recital 23 GDPR.

42 Art. 3(2)(b) GDPR. See also Recital 24.

43 Art. 3(2) of the revised Convention.

44 Art. 2(2)(c) GDPR: 'This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.'

45 Explanatory Report, para. 27.

The scope of this limitation, however, must take into account the major changes in the delimitation of public and private spheres on the Internet. As pointed out by Douwe Korff, reflecting on whether a middle way should be found:

> [t]he overall problem is that the granting of a full exemption from data protection requirements to anyone who uploads materials to the Internet as a private individual would lead to easy circumvention of the rules and, in an age of user-generated content, would fundamentally undermine data protection (and privacy) itself; yet the full imposition of the law to all such individuals would seem excessive and, because of the sheer numbers, would be largely unenforceable.[46]

The personal sphere can be defined according to various criteria. It is the nature of the circle of recipients of the data that matters: '[T]he private sphere encompasses notably the family, a restricted circle of friends or a circle which is limited in its size and based on a personal relationship or a particular relation of trust.'[47]

Recital 18 of the GDPR notes that a purely personal activity has no connection with a professional or commercial activity.[48] As examples of personal activities, it mentions correspondence and the holding of addresses, or social networking and other online activities undertaken within that context.

The Court of Justice of the EU (CJEU) has stated that the personal or household limitation should not apply when data are made available to an undetermined number of people, as it is the case for publication on the Internet.[49] It has interpreted strictly this limitation of the scope of application: if the personal or household activity extends – even only partially – to the public space (like a private camera in a house filming part of the street), the limitation will not apply.[50]

IV.4.2 Other limitations of the scope

The GDPR foresees certain additional limitations of its scope.[51] It does not apply to the processing of personal data related to activities falling outside the scope of EU law, such as activities concerning national security. Nor does it apply to the processing of personal data by the Member States when carrying out activities in relation to the EU's Common Foreign and Security Policy (CFSP). It does not apply either to processing activities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties by 'competent authorities'.[52]

---

[46] Douwe Korff, *New challenges to data protection study - Working Paper No. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, European Commission Directorate-General Justice, Freedom and Security Report (2010).

[47] Explanatory Report, para. 27 *in fine*.

[48] Recital 18 GDPR.

[49] Case C-101-01 *Lindqvist* [2003], paras 46–47; Case C-73/07 *Satamedia* [2008].

[50] Case C-212/13 *František Ryneš* [2014].

[51] Art 2(2)(a), b) and d) GDPR; Recital 16 GDPR.

[52] The latter processing activities fall under the scope of directive (UE) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

V. BASIC PRINCIPLES

The fundamental principles of data protection have not changed for several decades. The principles laid down in the 1981 version of Convention 108 and in Directive 95/46/EC have demonstrated their capacity to stand the test of time. They have proved to be generally appropriate and efficient also in evolving technological and societal contexts. Thus, they were maintained both in Convention 108+ and in the GDPR, which only brought adjustments and complements where necessary.

V.1 Principle of Proportionality

One noticeable 'new principle' was added in Convention 108+: the principle of proportionality. According to this principle, data processing should not constitute a disproportionate interference with the data subject's or society's interests in light of the controller's interest in processing the data.

The case-law of the European Court of Human Rights (ECtHR) requires that a fair balance between public and private interests at stake be taken into account in the implementation of data processing. In the case *S. and Marper*,[53] for instance, the Court emphasized that data processing must be proportionate, that is to say, appropriate in relation to the legitimate aims pursued and necessary in the sense that there are no other appropriate and less intrusive measures with regard to the interests, rights and freedoms of data subjects or society. Moreover, it should not lead to a disproportionate interference with these individual or collective interests in relation to the benefits expected from the controller.

The EU Court of Justice has also ruled[54] that to be admissible a legal obligation to process personal data (*in casu*, to publish personal data on the beneficiaries of EU agricultural funds) must respect the principle of proportionality (which lies in the requirement for a legitimate purpose, see hereunder). The Court has checked the respect of this principle of proportionality in several cases,[55] one of the most famous being the *Digital Rights Ireland* case,[56] where the Court also found that the principle had not been respected.

In the original version of Convention 108, only the proportionality of the data collected and processed was evoked, but not that of the processing itself. It thus appeared imperative to the modernisers of the Convention to incorporate an explicit requirement of proportionality of data processing at all stages. This can serve as a bulwark against risks associated to technical developments (including unexpected processing abounding on the Internet) and to the generalized reliance on data subjects' consent to process their data. The balancing of interests and verification of the achieved balance provides a welcome backup when one considers the defects often attached to inappropriate reliance on consent (insufficient information given to the data subject, consent inferred from the non-change of the default settings, etc.).

As a result, Article 5(1) of Convention 108+ states: 'Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair

---

[53] *S and Marper v. UK*, App no 30562/04, 30566/04 (ECHR, 4 December 2008).

[54] Joined cases C-92/09 and 93/09 *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [2010], paras 86 and 89.

[55] All those cases were based on Directive 95/46/EC mentioned *supra*.

[56] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014].

balance between all interests concerned, whether public or private, and the rights and freedoms at stake.'

V.2 Lawfulness, Fairness and Transparency Principle

Personal data is to be processed lawfully, fairly and in a transparent manner.[57]

Data processing must be lawful to the effect that it respects all applicable legal requirements (even outside the scope of data protection regulation, such as, e.g., the obligation of professional secrecy, if applicable).

The principle of lawful processing is however also understood as requiring the consent of the data subject or another legitimate ground provided in the data protection legislation. Article 6 of the GDPR, dealing with such legitimate grounds for processing, is entitled 'Lawfulness of processing', instead of 'Criteria for making data processing legitimate' as in Directive 95/46/EC. It lists all the grounds which can render processing personal data admissible as lawful. This, however, does not free processing from needing to be compliant also with the other aspects of the lawfulness requirement.[58]

The principle of fair processing[59] implies that personal data shall not be obtained nor otherwise processed through unfair means, by deception or without the data subject knowing.[60] Nor should personal data be processed in ways which would be completely unexpected or unforeseeable to the data subject.

The GDPR explicitly includes the transparency principle together with the requirement that data be processed lawfully and fairly, even though some commentators had attached till now such a transparency requirement to the notion of fairness.[61] This transparency principle is explained in a long Recital 39 which starts by clarifying that it 'should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed'. The recital specifies that natural persons should be made aware of risks and safeguards in relation to the processing of their personal data. The transparency principle is further developed in Article 8 of Convention 108+ and in Articles 12–14 of the GDPR.

V.3 Purpose Limitation Principle

Presented for 35 years as the true cornerstone of data protection and as a prerequisite for almost all other fundamental requirements, the purpose limitation principle[62] requires data to be collected for specified, explicit and legitimate purposes (the 'purpose specification' dimension),[63] and not further processed in a manner that is incompatible with those purposes

---

[57] Art. 5(3) and 5(4)(a) revised Convention 108; Art. 5(1)(a) GDPR.

[58] *Contra*, Jef Ausloos, 'Giving meaning to Lawfulness under the GDPR', Centre for IT and IP (CITIP) Blog, 2 May 2017.

[59] Art 5(4)(a) of the revised Convention 108; Art. 5(1)(a) GDPR.

[60] See for a case of unfair processing: *KH and others v. Slovakia,* App no 32881/04 (ECHR, 28 April 2009).

[61] 'Fair processing means transparency of processing, especially vis-à-vis data subjects.' (European Union Agency for Fundamental Right (FRA), European Court of human rights, Council of Europe, *Handbook on European data protection law,* 2014, https://rm.coe.int/16806b294a, p. 76).

[62] Art. 5(4)(b) of the revised Convention 108; Art. 5(1)(b) GDPR.

[63] Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP 203, 2 April 2013, 11–12.

(the 'compatible use' dimension).[64] The purposes for which the processing of personal data is to occur should be determined from the very beginning, when personal data are collected. The processing of personal data for undefined or unlimited purposes is unlawful, since it does not enable delimiting precisely the scope of the processing. The purposes of data processing must also be unambiguous, clearly expressed, and never kept hidden.[65]

Finally, the purposes must be legitimate and proportionate, which means that they shall not entail a disproportionate interference with the rights, freedoms and interests at stake in the name of the interests of the data controller.[66] The Explanatory Report of Convention 108+ notes:

> What is considered a legitimate purpose depends on the circumstances as the objective is to ensure that a balancing of all rights, freedoms and interests at stake is made in each instance; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as, for example, between the interests of the data subject and the interests of the controller or of society.[67]

In all cases, data processing serving an unlawful purpose (that is contrary to the law) cannot be considered to be based on a legitimate purpose.[68]

The second dimension of the purpose limitation principle implies that one may perform on these data all the operations that can be considered to be compatible with the initial purposes. This notion of 'compatible' processing of data has raised numerous questions in practice. The EU legislator and the modernizers of Convention 108 considered it necessary to clarify the requirement. They thus offered a series of criteria allowing to determine whether the processing for a purpose other than that for which the personal data have been collected is to be considered as compatible with this initial purpose.[69] Account should be taken of the possible link between both purposes, of the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller, of the nature of the personal data, ordinary or sensitive, of the possible consequences of the intended further processing for data subjects, and of the existence of appropriate safeguards.[70]

'Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'[71] is considered as compatible – and thus admissible – if subject to appropriate safeguards. A clarification of what is meant by scientific and historical research purposes and by statistical purposes can be found in Recitals 159, 160 and 162 of the GDPR, on the one hand, and in a Recommendation of the Council of Europe, on the other hand.[72]

---

64 *Ibid*., 12–13.

65 *Ibid*., 39.

66 Marie-Hélène Boulanger et al., 'La protection des données à caractère personnel en droit communautaire', *Journal des Tribunaux droit européen* [1997] 41.

67 Explanatory Report of Convention 108+, para. 48.

68 Article 29 Working Party, WP 203 (n 63).

69 Art. 6(4) GDPR; Explanatory Report of Convention 108+, para. 49. This list is based on the one elaborated by the Article 29 Working Party (see Opinion 3/2013 WP 203, 40).

70 See also Recital 50 GDPR.

71 Art. 5(4)(b) Convention 108; Art. 5(1)(b) GDPR.

72 Explanatory Memorandum to Recommendation No. R (97) 18 of the Committee of Ministers to Member States, 30 September 1997, concerning the protection of personal data collected and processed for statistical purposes, §§ 11 and 14 and Appendix, para. 1.

Finally, the processing of personal data for a purpose other than that for which it had been collected is allowed in certain circumstances even if the new purpose is not compatible with the first one. The GDPR allows it in two cases: if the data subject consents to the new incompatible purpose, or if the processing is based on a Union or Member State law.[73]

V.4 Minimization and Quality of Data

According to the data minimization principle, personal data undergoing processing must be adequate, relevant and not excessive (or limited to what is necessary[74]) in relation to the purposes for which they are processed.[75] The data minimization principle requires in particular that personal data should only be processed if the purposes cannot reasonably be fulfilled by other means.[76] Furthermore, the 'not excessive' or 'limited to what is necessary' criterion not only refers to the quantity, but also to the quality of personal data. It is thus clear that one may not process an excessively large number of data (e.g., asking an employee his complete medical file to assess their capacity to work). But one may not process a single data either if this would entail a disproportionate interference in the data subject's rights and interests (e.g., collecting information about private drugs consumption from a job applicant).[77]

The accuracy principle requires that data be accurate and, where necessary, kept up to date.[78] All inaccurate data should be rectified or erased. The controller must take every reasonable step to ensure respect of the accuracy principle. The GDPR clarifies that any requested rectification must be done without delay.

The storage limitation principle prohibits storing personal data in a form that permits identification of data subjects beyond the time necessary to achieve the purposes of processing.[79] Controllers are invited to establish time limits for erasure or for a periodic review.[80] This would ensure that the personal data are not kept longer than necessary. Article 25 GDPR is to be taken into account here since it mandates that controllers implement appropriate technical and organizational measures for ensuring notably that, by default, the legitimate period of storage of personal data be respected. Such measures could be expiry dates determined for each category of personal data.

Besides, the storage limitation principle admits storage of personal data for longer periods if for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and subject to implementation of appropriate technical and organizational measures in order to safeguard the rights and freedoms of the data subject.

---

73 Art. 6(4) GDPR.
74 Terms of Art. 5(1)(c) GDPR.
75 Art. 5(4)(c) Convention 108+.
76 Explanatory report, para. 52; Recital 39 GDPR.
77 In this way, see the explanation given for the notion of 'excessive' data in the Explanatory Report, para. 52.
78 Art. 5(4)(d) revised Convention 108; Art. 5(1)(d) GDPR.
79 Art. 5(4)(e) revised Convention 108; Art. 5(1)(e) GDPR.
80 Recital 39 GDPR.

V.5 Security – Data Breaches

In the GDPR the security requirement appears in the list of the basic data protection principles under the title of 'integrity and confidentiality' principle.[81] Besides, in both the GDPR and Convention 108+, the security requirement is developed in specific provisions.[82] While the security requirement has been provided since the emergence of data protection legislation, it is especially crucial today. Cybercrime (including hacking, identity theft, computer fraud, extortion, phishing, virus, malwares, and so on) has increased to staggering levels.[83] In response to these security concerns, both European legal texts require that personal data be processed in a manner that ensures their appropriate security, 'including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.[84]

This security duty includes, and this is new compared to previous texts (Directive 95/46/EC and the initial version of Convention 108), the requirement to notify personal data breaches to the supervisory authority and in certain cases to the data subjects too. An additional paragraph has been added to Article 7 of Convention 108+ on the security of data. It concerns those security problems known as 'data breaches'. It provides that the controller must notify, without undue delay, at least the supervisory authorities of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects. Article 33.1 of the GDPR is slightly more precise, as it states that:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent […], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.[85]

Illegal access to personal data falls within the scope of this obligation, as well as situations in which personal data has been lost (e.g., on CD-ROMs, USB sticks or other portable devices), or communicated to third parties in breach of the purpose principle. A threshold is set to trigger the notification obligation, corresponding in Convention 108+ to a serious interference with the rights and freedoms of the data subject, and in the GDPR to a potential risk to the rights and freedoms of natural persons. The aim is not to overburden data controllers, nor to drown supervisory authorities with trivial messages that would blunt the alert function. If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate it to the data subject in addition to the notification to the supervisory authority.[86]

---

[81] Art. 5(1)(f) GDPR.

[82] Art. 7 revised Convention 108; A whole section (Section 2. Security of personal data) of Chapter IV dedicated to controllers and processors develops this security duty: Arts 32–34 GDPR.

[83] European Commission, *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN(2017) 450 final, 13 September 2017; McAfee & Centre for Strategic and International Studies, *Net losses: Estimating the global cost of cybercrime*, 2014; Europol, *Serious and organised crime threat assessment*, 2017.

[84] Art. 5(1)(f) GDPR.

[85] See also: Céline van Waesberge, and Stéphanie De Smedt, 'Cybersecurity and Data Breach Notification Obligations Under the Current and Future Legislative Framework', *EDPL*, 2016/3.

[86] Art. 34 GDPR. See also Explanatory report, para. 66.

V.6 Accountability Principle

The last principle of the European data protection regime is the accountability principle according to which controllers are not only responsible for ensuring compliance with all the legal requirements, but they must also be in a position to demonstrate that they have taken all appropriate measures and that the processing is compliant with the applicable legal rules.[87] Accountability has been strengthened in the GDPR and in the new version of Convention 108. Both texts, in compensation, have reduced the existing notification and approval procedures in order to remove needlessly burdensome bureaucracy on data controllers.

The obligations linked to the accountability principle are further developed below, in the section about the duties of the actors.

VI. SENSITIVE DATA

Certain categories of data are recognized as deserving greater protection since the processing of this data is linked to an increased risk of harm for individuals. It is mainly the risk of illegal or arbitrary discrimination that is at stake, or of injury to an individual's dignity or physical integrity, as well as the risk of affecting the most intimate sphere of individuals or where processing of data could affect the presumption of innocence.

The new Article 6(1) of Convention 108+ provides the following:

> The processing of:
> - genetic data;
> - personal data concerning offences, criminal convictions and related security measures;
> - biometric data uniquely identifying a person;
> - personal data for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life shall only be allowed where the applicable law provides appropriate safeguards, complementing those of the present Convention.

The major difference compared to the text of 1981 lies in the fact that without sacrificing the drawing of a predetermined list, it is proposed to take into account the context of use of data. Some data follow the pattern of 1981: they are considered sensitive in all circumstances and simply because they are subject to processing, regardless of its purpose, the more protective regime will be applicable (i.e., genetic data[88] and personal data concerning offences, criminal convictions and related security measures). However, for other categories of data the new text presents a list of data identified as sensitive but triggering the protection regime only if it is the

---

[87] Art. 10, § 1 revised Convention 108; Art. 5(2) and 24 GDPR. The accountability principle had already been mentioned in the very first international text on data protection: the OECD Guidelines of 22 September 1980, article 14. See also Article 29 Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, 13 July 2010.

[88] In the *S and Marper* case, para. 75, the ECtHR states that genetic data raise particular concern with regard to the protection of privacy. DNA profiles contain a significant amount of unique and irrefutable personal data that allow authorities to go beyond a neutral identification (to search the genetic relationships between individuals, for instance). Moreover, genetic data can reveal things the individual wishes not to know.

sensitive element of the data that is specifically sought and processed. Biometric data appears now in the list but is to be considered as sensitive only when it is processed for identifying an individual.[89]

It should be noted that the new text of Convention 108+ brings some specification about the 'appropriate safeguards' that States must take to allow sensitive data to be processed. These safeguards are already mentioned in the current Article 6 of the Convention, but nothing was added to clarify them. This time, two clarifications are made:[90] The appropriate safeguards must come in addition to the safeguards put in place by the Convention; and the appropriate safeguards are those likely to prevent the serious risk that the processing of sensitive data presents as regards the interests and rights of the data subject, notably the risk of discrimination. The Explanatory Report adds that appropriate safeguards must be adapted to the risks at stake and to the interests, rights and freedoms needing protection. Examples of appropriate safeguards are:

> alone or cumulatively, the data subject's explicit consent, a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted, a professional secrecy obligation, measures following a risk analysis, a particular and qualified organisational or technical security measure (data encryption for example).[91]

The GDPR also presents a list of categories of data to be considered as sensitive and deserving higher protection. This list is nearly identical to the one of Convention 108: sensitive data are 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.[92] The GDPR addresses separately 'personal data relating to criminal convictions and offences or related security measures'. Their higher protection is provided, in a separate provision but also linked to the higher risk such data present, notably a risk of discrimination.[93] The processing of all these categories of data is prohibited except in the circumstances listed in GDPR provisions.[94]

VII. RIGHTS OF THE DATA SUBJECT

Rights have been recognized by the Council of Europe to data subjects since 1981, such as the right of access to data, the right to rectify or erase them and the right to remedy (Art. 8, b, c, and d of the Convention 108). These rights are strengthened in the modernized text of the Convention while new ones complete the list of safeguards offered to data subjects. As for GDPR, it offers the most elaborate catalogue of rights among data protection legal instru-

---

[89] Catherine Jasserand, 'Legal nature of biometric data: From 'generic' personal data to sensitive data', *EDPL*, 2016/3; Els Kindt, *Privacy and Data Protection Issues of Biometric Applications* (Springer 2013).

[90] Art. 6(2) revised Convention 108.

[91] Explanatory Report, para. 56.

[92] Art. 9 GDPR.

[93] Art. 10 GDPR.

[94] Arts 9(2) and 10 GDPR.

ments, in line with the rights listed in the new Article 8 of the Convention, but deeply further developed.

These rights are presented in the paragraphs below, following the order of Article 8 of Convention 108+. This order aims at highlighting the values linked to these rights: at first human dignity (machines cannot dominate human beings) and then autonomy, that implies individuals must know and understand what is being done with the data about them, by whom and for which purpose, and that implies the right to object, to rectify and to erase. In case of difficulties in exercising these rights, a right to remedy is granted to data subjects. The GDPR adds a new right to this list: the right to data portability.[95]

The right to receive information from the controller about the processing of personal data will be evoked *infra* under the section devoted to the controllers' duties. These rights are not absolute. Exceptions are admitted for each of them. In both texts, a provision is specially dedicated to the exemptions that Parties have the possibility to adopt as regards the main provisions on data subject rights of the Convention[96] and of the GDPR.[97] To be admissible these exemptions must be provided for by law and must constitute a necessary measure in a democratic society for the protection of certain public or private interests.

VII.1 Right not to be Subject to an Automated Decision

It appeared imperative to the reviewers of Convention 108 to guarantee to any person the right 'not to be subject to a decision significantly affecting him or her, based solely on an automated processing of data without having his or her views taken into consideration'[98]. Presented now as the first right of the data subject, this right ensues from the will that a human being be not entirely subject to a machine. It is not desirable that a decision imposed on a person depends on the sole findings of a machine. This right is the expression of the pre-eminence to be given to human dignity.

The right was already present in Directive 95/56/EC[99] and it appears also in Article 22 of the GDPR, which states in similar terms: 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.' Automated decisions are admitted however in a contractual process or with the data subject's consent, but in both cases the data subject must have the right to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision.[100] Individuals are not explicitly granted these rights if the automated decision is authorized by a law. However, that law must lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.[101]

---

95 Art. 20 GDPR; See Article 29 Working Party, *Guidelines on the right to data portability*, WP 242, 13 December 2016.

96 Art. 11 of the revised Convention 108.

97 Art. 23 GDPR.

98 Art. 9(a) of the revised Convention 108.

99 Art. 12(a) of Directive 95/46/EC.

100 Art. 22(2)(a) and (c) and Art. 22(3) GDPR.

101 Art. 22(2)(b) GDPR; Explanatory Report, para 73 *in fine*.

VII.2 Enriched Right of Access

Authors of the modernization of Convention 108 as well as of GDPR have expanded the right of access so as to broaden the information that should be communicated to the data subject exercising their right. Beside the communication 'in an intelligible form of the data processed'[102] or of 'a copy of the personal data undergoing processing',[103] the right of access implies also access to the purposes of the processing, to the preservation period and to the origin of data.[104] This latter information is indeed crucial because one often questions the source of the data (how did they get this information, who did provide it?). In addition, information on the origin of the data allows to verify the legality of the communication or collection of it and to possibly 'stop the bleeding' if the first holder of the data unlawfully transmits it. In case of problems with data quality and a need of correction, it becomes possible as soon as information is obtained as to the source of the data to make these corrections at the source, preventing the further spread of errors.

VII.3 Right to Know the Reasoning Underlying the Data Processing

In today's technological context, there is a right of great interest, particularly with regard to the exponential phenomenon of profiling where one relies on 'profiles' to make decisions about a person or predict their preferences, behaviour and personal attitudes. This is the right to know the reasoning underlying a data processing the results of which are applied to someone.

Faced with a refusal of credit, a failure at a multiple-choice question examination, the targeting as suspected fraudster, etc., it is clear that one may wish to understand the assessment or the decision by accessing to the reasoning underlying the data processing. We can legitimately want to know the criteria used and the weight given to each of these criteria.[105] This right is a key right largely contributing to transparency and therefore to individuals' informational self-determination, because it allows them not only to know what is happening with their data, but also to understand it.

This right, first guaranteed in Directive 95/46/EC,[106] was logically taken over in GDPR.[107] As exposed in this text, the right to receive information as well as the right of access include the right to know the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

As for the Council of Europe, the reviewers of Convention 108 have it considered mostly appropriate to enshrine this right within the Convention. They have consequently added to the list of guarantees offered to data subjects the right of every individual to 'obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her' (new Art. 8, d).

---

[102] Art. 8(b) of the revised Convention 108.
[103] Art. 15(3) GDPR.
[104] Art. 8(b) of the revised Convention 108; Art. 15(1)(a, c, d, g) GDPR.
[105] See Joshua A. Kroll et al., 'Accountable algorithms', *University of Pennsylvania Law Review* [2017] 165.
[106] Art. 12(a) of Directive 95/46/EC.
[107] Arts 13(2)(f), 14(2)(g) and 15(1)(h) GDPR.

Like with other data subject rights, this right is not absolute and may be limited by national laws in accordance with the conditions laid down in Article 9 of the Convention 108+ and in Article 23 of the GDPR.

VII.4 Right to Object

Both European texts[108] include the right to object to processing of data in order to enable individuals to exercise control over what happens to the data about them. Individuals are entitled to object at any time, on grounds relating to their situation, to the processing of personal data concerning them unless the controller demonstrates legitimate grounds for the processing which override the data subject's interests or rights and fundamental freedoms.

This right is particularly relevant where data processing is not based on the data subject's consent. It may be used in cases where the controller has weighed up the interests at stake beforehand and has concluded that the result is balanced, and that they could legitimately process the data.[109] Thanks to the right to object, the data subject has an opportunity to challenge the outcome of that weighing up, at least in their personal case. The burden of proof rests on the controller who has to demonstrate that their legitimate interests in processing the data prevail over the rights and interests of the data subject.

VII.5 Right to Correct and Erase – Right to be Forgotten

The right to obtain rectification of inaccurate data and erasure of data which have been processed contrary to data protection rules has been granted to data subjects since the adoption of the very first European text.[110] This right has not changed and is protected under the modernized Convention 108,[111] as well as in the GDPR.[112]

In the GDPR, the right to erasure is presented associated with the 'right to be forgotten'. In the Internet environment, this right has appeared as an appropriate answer to the problems raised by the eternal electronic memory (creating an 'eternity effect') combined with the retrieving and gathering power of search engines (and the de-contextualization of the data that ensues).[113] Like the other data subject rights, this right to erasure/to be forgotten is not absolute and limitations are admitted. Contrary to the other rights, some of these limitations are embedded in Article 17 GDPR itself.

Convention 108 does not provide for an explicit inclusion of a 'right to be forgotten'. It was felt by the group of modernizers of the Convention that the existing safeguards (the limited length of time of data storage, and the right of rectification or erasure of data) combined with an effective right of opposition would offer adequate protection. T-PD members intend to

---

[108] Art. 9(1)(d) of the revised Convention 108; Art. 21 GDPR.
[109] Art. 6(1)(f) GDPR.
[110] Art. 8(c) of Convention 108.
[111] Art. 9(1)(e) of the revised Convention 108.
[112] Arts 16 and 17 GDPR.
[113] See Cécile de Terwangne, 'The right to be forgotten and informational autonomy in the digital environment', in Alessia Ghezzi, Ângela Guimarães Pereira and Lucia Vesnić-Alujević (eds) *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten* (Palgrave 2014); EUCJ (G.C.), 13 May 2014, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* C-131/12.

specifically address this issue through a future recommendation on social networks because it is mainly – although not exclusively – in this context that the question of the right to be forgotten is arising today.

VII.6 Right to Data Portability

Article 20 of the GDPR creates a new right to data portability that allows for data subjects to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller, or to have it directly transferred.[114] The purpose of this new right is to empower the data subject and give them more control over the personal data concerning them.[115] By facilitating data subjects' ability to transfer personal data easily from one IT environment to another, without hindrance, data portability provides consumer empowerment and prevents 'lock-in'.[116]

VIII. DUTIES OF THE ACTORS

Besides the security obligation mentioned above (see section V.5), a range of other duties and obligations are incumbent on data controllers and processors. Some new obligations implement the 'accountability principle' in concrete measures, such as the obligation to establish internal mechanisms to demonstrate the compliance of the processing with the national law or with the GDPR,[117] to carry out a risk analysis,[118] and to design processing in such a way as to minimize risks for data subjects.[119]

As regards the obligation to conduct data protection impact assessments, this is a new tool in order to assess the risk before one starts with data processing.[120] Such assessment is required whenever data processing is likely to result in a high risk to the rights and freedoms of individuals. The GDPR mentions three specific situations where this is the case: when a company evaluates systematically and extensively personal aspects of an individual (including profiling); when it processes sensitive data on a large scale; and where it systematically monitors public areas on a large scale. National data protection authorities have to draw a list of additional cases requiring a data protection impact assessment.

The duty of 'privacy by design' has long existed as a concept before becoming part of a legal requirement with the GDPR. The GDPR states that the controller shall implement appropriate technical and organisational measures in order to meet its requirements and to protect the rights of data subjects.[121]

---

[114] Art. 20 GDPR; see also Article 29 Working Party, WP 242rev.01.
[115] *Ibid.*, 3–4.
[116] *Ibid.*
[117] Art. 10(1) of the revised Convention 108; Art. 24 GDPR.
[118] Art. 10(2) of the revised Convention 108; Art. 35 GDPR.
[119] Art. 10(3) of the revised Convention 108; Art. 25 GDPR. See: Lee A. Bygrave, 'Hardwiring privacy', in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of the Law and Regulation of Technology* (Oxford University Press 2017).
[120] Atanas Yordanov, 'Nature and ideal steps of the Data Protection Impact Assessment under the General Data Protection Regulation', *EDPL*, 2017/4.
[121] Art. 23 GDPR.

A transparency duty has been imposed on controllers by EU law since Directive 95/46/EC. It was taken over in GDPR (where it is connected to data subject rights)[122] and in the revised version of Convention 108.[123] It is indeed imperative, given the particularly opaque current information systems, to provide for active transparency requirements. Data subjects may not be willing to exert their rights as regards a data processing if they do not even suspect their data to be processed. It is therefore of utmost importance to require controllers to spontaneously inform data subjects about what they are doing with their data:

> Each Party shall provide that the controller informs the data subjects of: a) his or her identity and habitual residence or establishment, b) the legal basis and the purposes of the intended processing, c) the categories of personal data processed, d) the recipients or categories of recipients of the personal data, if any, and e) the means of exercising the rights set out in Article 8, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data (Art. 8 of the revised Convention).

Given that the Convention, as an international treaty, should not enter into too much detail, there is no indication as to when and how information must be provided by the controller.

The GDPR, on the contrary, foresees a detailed transparency obligation. Controllers are required to communicate a series of information pieces to the data subject, and to do it in a clear manner. In addition to the information listed in the new version of the Convention 108, they must also indicate 'the contact details of the data protection officer', 'the legitimate interests, if any, pursued by the controller or by a third party', 'where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of adequate protection for the data in that case, the period of storage of the data, the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[124] The controller must provide all this information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[125] The GDPR specifies that the information must be provided in writing, and, where appropriate, by electronic means.

When personal data are not collected from the data subjects, the controller is not required to provide the information where it is impossible or would involve disproportionate effort. The impossibility may be of a practical or legal nature (e.g., professional secrecy). The second exception is granted where the processing is expressly prescribed by law. But this is valid only if the law is sufficiently precise and provides the necessary information to ensure fair information of data subjects.[126]

Finally, a last duty consists in appointing a Data Protection Officer (DPO). While this is just a suggestion linked to the accountability requirement in the Explanatory Memorandum of the Convention 108 in order to help to reach compliance,[127] it is mandatory in the GDPR in cases

---

[122] Arts 13–14 GDPR. See: Merle Temme, 'Algorithms and transparency in view of the new General Data Protection Regulation', *EDPL*, 2017/4.

[123] Art. 8 of the revised Convention 108.

[124] Arts 13 and 14 GDPR.

[125] Art. 12(1) GDPR.

[126] Arts 14(5)(b) and (c) GDPR; Art. 8(3) of the revised Convention 108.

[127] Explanatory Report, para. 87.

where the processing is carried out by a public authority or body, and for those controllers and processors whose core activities consist of processing on a large scale sensitive data or data relating to criminal convictions and offences or consist of processing operations which require regular and systematic monitoring of data subjects on a large scale.[128] [129] The DPOs must be independent[130] and appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices.[131]

IX. TRANSBORDER DATA FLOWS

Although there is no definition of a transborder data flow or transborder transfer of personal data in the GDPR,[132] one can find one in the Explanatory Memorandum of Convention 108+. The latter states: 'A transborder data transfer occurs when personal data is disclosed or made available to a recipient subject to the jurisdiction of another State or international organisation'.[133]

The issue of transborder data transfers was key in the modernization process of Convention 108+. The new provisions revise the existing provisions on flows of personal data to other Parties (Art. 12 of the current Convention) and to non-Parties (Art. 2 of the 2001 additional Protocol[134]). Between Parties, the rule is still that of free flows unless the sending Party is 'bound by harmonised rules of protection shared by States belonging to a regional international organisation'.[135] In this case, a transfer of data may nevertheless take place if it is governed by ad hoc or standardized measures. Freedom of flows is thus not systematic among Parties to Convention 108+. This is due to the necessity to coordinate the two European legal spheres and to take into account the constraints from the European Union legal regime.

Transfers to recipients not subject to the jurisdiction of a Party to the Convention can only occur where an appropriate level of data protection based on the principles of the Convention is guaranteed.[136] This appropriate level of protection can be ensured by the law of that State or international organization, including the applicable international treaties or agreements. If no such law offers appropriate protection, protection can be guaranteed by several mechanisms: it can be ensured by 'ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer

---

[128] Art. 37(1) GDPR.

[129] Fanny Coton and Jean-François Henrotte, 'Everything you always wanted to know about DPO (but were afraid to ask)', *Cahier du juriste*, 2017/2.

[130] Art. 38(3) GDPR.

[131] Art. 37(5) GDPR.

[132] Gloria González Fuster, 'Un-mapping personal data transfers', *EDPL*, 2016/2.

[133] Explanatory Report, para. 102. See also the definition given by the European Data Protection Supervisor (EDPS) in its position paper *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, 14 July 2014, 7. See also: González Fuster (n 132).

[134] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, 8 November 2001 (ETS no. 181).

[135] Art. 14(1) revised Convention 108.

[136] Art. 14(2) revised Convention 108.

and further processing'.[137] Contractual clauses or binding corporate rules are examples of such mechanisms.

As for the GDPR, it does not change the existing regime much, but it brings interesting light and precision, and it enlarges the list of legal instruments that can be used to provide for appropriate safeguards and thus to allow transborder data transfers. Chapter V takes over the rules regulating the question. It integrates the legal tools that have appeared since 1995 to protect personal data once they cross EU borders. Transfers of data outside the EU are forbidden unless the third country or the international organization has been recognized by the European Commission as ensuring an adequate level of protection to the data, or unless the sending party offers itself an adequate protection through appropriate safeguards.

These safeguards can be provided for by binding corporate rules in accordance with the GDPR provision[138] dedicated to this instrument, or by standard contractual clauses adopted by the European Commission, or by ad hoc clauses authorized by a national supervisory authority.[139] New legal tools can be used such as administrative arrangements between public authorities or bodies, and codes of conduct or standardization mechanisms approved by a supervisory authority. In the absence of an adequacy decision or of appropriate safeguards, derogations to the forbidding of transborder transfers of personal data are foreseen, allowing them in specific situations: with the data subject's explicit consent, if necessary for a contract or for important reasons of public interest, if necessary for the defence of legal claims or to protect a vital interest, and if the transfer is made from a public register, under certain conditions.[140]

X. SUPERVISORY AUTHORITIES

Specialized supervisory authorities are an integral part of the European system of protection of personal data. All over the European territory, national supervisory authorities are responsible for monitoring compliance with all the data protection rules outlined in the previous paragraphs. Both Convention 108+ and the GDPR set up data protection authorities (DPAs)[141], see to the independence of these authorities[142] and to their dialogue, cooperation and mutual assistance[143].[144]

National DPAs are established to enforce data protection rules, and to offer guidance. They supervise, through investigative and corrective powers,[145] the application of data protection rules. They handle complaints lodged against violations of these rules.[146] Moreover, they provide expert advice on data protection issues.[147] DPAs have now significant enforcement

---

[137] Art. 14(3) revised Convention 108.
[138] Art. 47 GDPR.
[139] Art. 46(2)(c) and (d) and Art. 46(3)(a) GDPR.
[140] Art. 49(1) GDPR.
[141] Art. 15 revised Convention 108; Art. 51(1) GDPR.
[142] Art. 15(5) revised Convention 108; Art. 52 GDPR.
[143] Art. 17 revised Convention 108; Arts 60–61 GDPR.
[144] Andra Giurgiu and Tine A Larsen, 'Roles and powers of national data protection authorities', *EDPL*, 2016/2.
[145] Art. 57(1)(h) GDPR.
[146] Art. 57(1)(f) GDPR.
[147] Art. 57(1)(c) GDPR.

powers, including the ability to impose substantial fines on controllers and processors in view of a better implementation of the rules. Those fines can go up to EUR 20 million or, in the case of a company, 4 per cent of the worldwide annual turnover.[148]

Each DPA can only exercise its powers on the territory of its own State, but this may affect processing that occurs in other States. In the EU, a 'one-stop-shop' mechanism has been put in place to prevent organizations with several establishments in the EU that might be confronted with inconsistent decisions by various local supervisory authorities. The one-stop-shop mechanism means that, as a main rule, organizations carrying out cross-border processing activities[149] will only have to deal with one supervisory authority, acting as the 'lead supervisory authority'.[150] This 'lead supervisory authority' has the primary responsibility for dealing with cross-border data processing activities and for coordinating any investigation for which it might have to involve other 'supervisory authorities concerned'.[151]

The GDPR establishes the European Data Protection Board (EDPB),[152] that comprises representatives of each of the national data protection authorities in the EU,[153] and whose functions include to advise EU institutions and to issue guidelines, recommendations and best practices – including binding decisions – in order to ensure consistent application of the GDPR.[154] The EDPB will replace the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (referred as 'Article 29 Working Party') that was established under the Data Protection Directive.

XI. CONCLUSION

Europe's advanced data protection architecture may serve as a model and have an outreach beyond European boundaries. Convention 108 is the only legally binding instrument presenting a unique potential of becoming a universal standard as concerns the protection of personal data. The revision of this text occurred at a time where sharing common core principles around the world to protect individuals as regards the processing of their personal data had become an absolute necessity. The process of revision of the Convention introduced key elements reinforcing the protection of individuals. The first of such key elements is the explicit formulation of the principle of proportionality to be respected at any stage of data processing and for all the operations done with the data.

Other major improvements correspond to elements of the protection that are also present in the GDPR. They concern the rights granted to data subjects, notably the right not to be submitted to an exclusively automated decision (human beings should never be submitted to a machine), the right to object to the processing and the right to know the reasoning underlying

---

148 Art. 83 GDPR.

149 See the explanations on 'cross-border processing of personal data' in Article 29 Working Party, *Guidelines for identifying a controller or processor's lead supervisory authority*, WP 244rev01, 5 April 2017, 3–4.

150 Art. 56 GDPR; see: Article 29 Working Party, *Guidelines for identifying a controller or processor's lead supervisory authority*, WP 244rev01, 5 April 2017, 4–10.

151 Art. 60 GDPR. For a definition of 'supervisory authorities concerned' see Art. 4(22) GDPR.

152 Art. 68(1) GDPR.

153 Art. 68(3) GDPR.

154 Art. 70(1) GDPR.

a processing. Informational self-determination means not only the right to know but also the right to understand what is done with one's data. Already existing rights have been enriched such as the right to access and, especially in the GDPR, the right to erasure linked to the right to be forgotten. GDPR has also introduced the new right to data portability. New duties have appeared in both European texts, such as the important duty of active transparency (presented as a right to receive information in the GDPR), that of implementing privacy by design and taking measures linked to the accountability principle, and that of notifying data breaches. Certain of these new obligations are incumbent upon controllers as well as processors.

The picture resulting from the revision work in Strasbourg and from the adoption of the GDPR by the EU legislator is certainly an enhanced one as regards the protection of individuals in Europe. The general nature of the text of the Convention does not allow to offer a view as precise as that resulting from the EU texts. But contrary to the EU GDPR, Convention 108+ covers all the activities of the private as well as of the public sector. This is an essential asset of this legal instrument.

REFERENCES

Article 29 Working Party *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007
Article 29 Working Party *Opinion 3/2010 on the principle of accountability*, WP 173, 13 July 2010
Article 29 Working Party *Opinion 03/2013 on purpose limitation*, WP 203, 2 April 2013
Article 29 Working Party *Opinion 05/2014 on anonymisation techniques*, WP 216, 10 April 2014
Article 29 Working Party *Guidelines on the right to data portability under Regulation 2016/679*, WP 242rev.01, 27 October 2017
Article 29 Working Party *Guidelines for identifying a controller or processor's lead supervisory authority*, WP 244rev.01, 5 April 2017
Ausloos J, 'Giving meaning to Lawfulness under the GDPR', Centre for IT and IP (CITIP) Blog, 2 May 2017
Boulanger M H et al., 'La protection des données à caractère personnel en droit communautaire', *Journal des Tribunaux droit européen* (1997) 41
Bygrave L A, 'Hardwiring Privacy', in R Brownsword, E Scotford and K Yeung (eds), *The Oxford Handbook of the Law and Regulation of Technology* (Oxford University Press 2017)
Coton F and J F Henrotte, 'Everything you always wanted to know about DPO (but were afraid to ask)' (2017) 2 *Cahier du juriste*
De Terwangne C, 'The right to be forgotten and informational autonomy in the digital environment', in A Ghezzi, Â Guimarães Pereira and L Vesnić-Alujević (eds) *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten* (Palgrave 2014)
De Terwangne C, K Rosier and B Losdyck, 'Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ?' (2017) 8 *Journal de droit européen*
European Commission, *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN(2017) 450 final, 13 September 2017
European Data Protection Supervisor (EDPS), *Position paper: The transfer of personal data to third countries and international organisations by EU institutions and bodies*, 14 July 2014
Giurgiu A and TA Larsen, 'Roles and powers of national data protection authorities', *EDPL*, 2016/2
González Fuster G, 'Un-mapping personal data transfers' (2016) 2 *EDPL*
Jasserand C, 'Legal nature of biometric data: From 'generic' personal data to sensitive data' (2016) 3 *EDPL*
Kindt E, *Privacy and Data Protection Issues of Biometric Applications* (Springer 2013)
Korff D, *New challenges to data protection study - Working Paper No. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, European Commission Directorate-General Justice, Freedom and Security Report (2010)

Kroll J A et al., 'Accountable algorithms' (2017) *University of Pennsylvania Law Review* 165
Kuner Ch., Bygrave L. ,Docksey Ch. (ed.), and Drechsier L. (ass. ed.), *The EU General Data Protection Regulation (GDPR) – A Commentary* (Oxford University Press, Oxford, 2020).
McAfee & Centre for Strategic and International Studies, *Net losses: Estimating the global cost of cybercrime*, 2014
Temme M, 'Algorithms and transparency in view of the new General Data Protection Regulation' (2017) 4 *EDPL*
Van Waesberge C and S De Smedt, 'Cybersecurity and data breach notification obligations under the current and future legislative framework' (2016) 3 *EDPL*
Yordanov A, 'Nature and ideal steps of the Data Protection Impact Assessment under the General Data Protection Regulation' (2017) 4 *EDPL*
Zuiderveen Borgesius FJ, 'The Breyer Case of the Court of Justice of the European Union: IP addresses and the personal data definition' (2017) 1 *EDPL*