Chapter XIII Data Protection and Patient Mobility in Europe*

Jean Herveg

1. Introduction

As for the Directive on the application of patients' rights in cross-border healthcare,[1] patient mobility means the possibility for a person to benefit from healthcare in a Member State other than the Member State of affiliation. In this context, the Directive insists, rightly, on the necessity to protect patient's personal data.[2] Protecting patient's personal data implies that any patient who benefits from cross-border healthcare is entitled to expect that one's personal data will not be processed by anyone in any way e.g. when using electronic medical records or transferring data for reimbursement purposes or for scientific research. In addition, it means that the patient is entitled to see his or her rights recognized on his or her personal data. The patient is also entitled to expect that specific mechanisms and bodies will contribute to ensuring the effectiveness of data protection. In other words, a patient receiving healthcare in a Member State other than the Member State of affiliation is entitled to expect to enjoy the same level of data protection as in his Country of affiliation, all other things being equal. That being said, we still have to agree on the significance and properties of this right to data protection to which the patient could claim in cross-border healthcare, both in its affirmation and in its implementation through the new European General Data protection Regulation.

2. Recognition of a right to data protection in European Law

At the level of the Council of Europe, the issue of data protection has been formally raised at the end of the 1960s. It was within the framework of reflections on the subject of human rights and modern scientific and technological achievements that the Council of Europe supported work more specifically focused on data protection. The results of this work were presented at a Conference in Salzburg on 9-12 September 1968. Based upon these results, the Committee of Ministers subsequently adopted the first two recommendations on automatic processing of personal data which shaped the first outline of the legal framework for ensuring data protection in Europe. The first of these recommendations concerned

* This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreement no. 730953 (Inspex) and in part by the Swiss Secretariat for Education, Research and Innovation (SERI) under Grant no. 16.0136 730953. This paper only reflects the author's view and does not engage the Commission.

[1] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (see the consolidated text).

[2] Cf. Recital no. 25, Article 2 (c), Article 4.2 (e) and (f), and Article 14 of Directive 2011/24/EU.

databases in the private sector[3] and the second, databases in the public sector.[4] The continuation and development of the Council of Europe's activities in data protection resulted in the adoption of the 28 January 1981 Convention for the protection of individuals with regard to automatic processing of personal data (Treaty no. 108)[5] as well as numerous sectoral or thematic recommendations.[6]

Relatively early in time several cases related to data protection were brought before the European Court of Human Rights. When assessing the necessity of an interference in a democratic society in the famous *Z v Finland* judgment of 25 February 1997, the Court explicitly stressed the importance and need to protect personal data for the exercise of the right to respect for private and family life.[7] Since then, the Court has repeatedly and consistently proclaimed that:

- The protection of personal data (and health information are not the least) plays a fundamental role in the exercise of the right to respect for private and family life.
- Respecting the confidentiality of health information is an essential principle of the legal system of all Contracting Parties to the Convention; it is essential not only to protect patients' privacy but also to preserve their confidence in the medical profession and health services in general. Without such protection, persons requiring medical care could be discouraged from providing the personal and intimate information necessary to get the appropriate treatment and even to consult a doctor. That could end up jeopardizing their health or, in case of communicable diseases, that of the community.
- Domestic legislation should therefore provide appropriate safeguards to prevent the use of personal data and in particular any communication or disclosure of personal data relating to health, which does not comply with the guarantees provided by Article 8 of the Convention.

In addition to this assertion of the importance and need to protect personal data for the exercise of the right to respect for private and family life,[8] the European Court of Human Rights has developed a substantial case-law in many areas interesting data protection:[9]

---

[3] Council of Europe, Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

[4] Council of Europe, Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector, adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

[5] This Convention is under revision.

[6] Recommendation 97 (5) on the protection of medical data is also under revision.

[7] *Z v Finland* (ECtHR, 25 February 1997), appl. no 22009/93, para 95.

[8] On the basis of which it could already be argued that each State has a positive obligation to protect personal data.

[9] Without prejudice to the question of the relationship between personal data and the sphere of private life (do all personal data fall within the private sphere?) and the question between interference and data processing (does any processing of data amount to an interference with the exercise of the right to respect for private life?). These are difficult and unresolved questions to date in the case-law of the European Court of Human Rights. Regarding the case-law of the Court to date (until 31 December 2016), it does not seem possible to say that all personal data fall within the private sphere within the meaning of Article 8.1 or that any processing of data constituted an interference with the exercise of the right to privacy within the meaning of Article 8.2. On the other hand, there are sufficient indications in the Court's decisions and judgments, as well

- surveillance of individuals and protection of their communications;

- personal identity and filiation;

- protection of reputation;

- systematic collection of public data;

- collection, conservation and use of data;

- protection against disclosure of data;

- protection of medical data;

- medical records;

- medical records security;

- access right (including the right to get a copy);

- data security;

- the right to one's image;

- genetic testing;

- collection and retention of data by the police;

- taking and preservation of fingerprints, human cellular substantive, and realization and conservation of DNA profiles;

- criminal records and files of sexual offenders;

- search and seizure of computer data;

- national security;

- protection against hidden cameras;

- motor vehicle registrations;

- records of bankrupts;

- protection of bank data.

At the level of the European Community (now the European Union), the issue of data protection was formally embraced by the European Parliament on 8 April 1976. At that date, it instructed its Legal Committee to report on the Community actions to be taken or pursued with a view to ensuring the protection of human rights in relation to the development of technical progress in the field of informatics.[10] This Legal Committee then set up a subcommittee on "Informatics and Human Rights". The latter organized a public debate on

as in some dissenting opinions, to support the opposite view. In any event, the principle adopted in the context of the assessment of the necessity of the interference in a democratic society makes it possible not to have to decide.

[10] Resolution adopted on 8 April 1976 OJ C 100, 3 May 1976 p. 27.

informatics and human rights in early 1978. This work resulted in the adoption on 5 June 1979 of a Resolution on the protection of human rights in the face of the development of technical progress in the field of informatics.[11] Then, after the adoption of the OECD Guidelines for the Protection of Privacy and Transborder Data Flows on 23 September 1980, the European Community adopted on 24 October 1995 the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[12] Its objective was to harmonize data protection legislations across the European Community and to state the principle of the free movement of personal data within the common market.[13] As from 25 May 2018, data protection will be ensured in Europe by the General Data Protection Regulation.[14]

But fundamentally, beyond the recognition of the importance and need to protect data for the exercise of the right to respect for private and family life, beyond the Member States' positive obligation to ensure data protection, beyond the development of the European Court of Human Rights case-law on data protection, and beyond the establishment of a specific legal framework to ensure data protection (at the level of the Council of Europe or the European Union), it was not until the adoption of the Charter of Fundamental Rights of the European Union on 7 December 2000 that the existence of a right to data protection was explicitly and formally recognized as a fundamental right at the European level. Since then, Article 8 of this Charter provides that:[15]

---

[11] OJ 5 June 1979 no. C 140/34.

[12] OJ L 281 23 November 1995 p. 31 (take into account the consolidated text).

[13] This legal framework has been supplemented by Regulation (EC) no 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Directive 2002/5EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Commission Regulation (EU) no 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (the latter has been declared invalid by the Court of Justice of the European Union in a judgement of 8 April 2017 in joined cases C-293/12 and C-594/12).

[14] Regulation (EU) 2016/679 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), OJ L 119 4 May 2016 p. 1. This Regulation was adopted at the same time (and as a prerequisite), on the one hand, that Directive (EU) 2016/680 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 and, on the other hand, that Directive (EU) 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The General Data Protection Regulation is applicable in 28 countries and concerns directly more than five hundred million people (without taking into account its indirect effects notably in the matter of transfers of personal data to third countries or international organizations). On the Regulation, see: S Gutwirth, R Leenes and P De Hert (eds.), *Reforming European Data Protection Law*, Law, Governance and Technology Series, Issues in Privacy and Data Protection, volume 20, Springer, 2015.

[15] Charter of fundamental rights of the European Union, 2016/C 202/02. See Working Party on the Protection of Individuals with Regard to the Processing of Personal Data *Recommendation 4/99 on the inclusion of the*

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 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.
> 3. Compliance with these rules shall be subject to control by an independent authority.

If the Charter had no legal value at the time of its adoption, it is now legally binding on the same basis as all the Union Treaties[16] since the entry into force of the Treaty of Lisbon in December 2009. The provisions of the Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law (which includes national authorities as well as regional or local authorities or public bodies).[17] They all have to respect the rights, observe the principles and promote their application in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.

On the other hand, the *Treaty on the Functioning of the European Union* also recognizes, under its provisions of general application, the right to data protection:[18]

> 1. Everyone has the right to the protection of personal data concerning them.
> 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

It is to this extent that any patient who comes under the jurisdiction of a Member State[19] has the right to claim the protection of his or her personal data in cross-border healthcare[20]

---

fundamental right to data protection in the European catalogue of fundamental rights WP 26 7 September 1999.

[16] This is confirmed by Article 6 of Treaty on the European Union.

[17] On this, see the Explanatory Report on Article 51 of the Charter. It follows that the Charter of Fundamental Rights of the European Union does not apply in a general and undifferentiated or unconditional way.

[18] See Article 16.

[19] In the meaning of the first Article of the European Convention on Human Rights to which Article 52 of the Charter of Fundamental Rights of the European Union refers.

[20] That is confirmed by Recital no 25 of Directive 2011/24: "The right to the protection of personal data is a fundamental right recognized by Article 8 of the Charter of Fundamental Rights of the European Union. Ensuring continuity of cross-border healthcare depends on transfer of personal data concerning patients' health. These personal data should be able to flow from one Member State to another, but at the same time the fundamental rights of the individuals should be safeguarded." 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 establishes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any

due to the fact that, on the one hand, the European Union have a competence in cross-border healthcare and, on the other hand, the patient's right to data protection concerns, at least, the implementation of European law in the matter of cross-border healthcare.

All this means that data protection must be ensured in the context of cross-border healthcare provided to a patient by a health professional in a Member State other than the Member State of affiliation. This also means that the patient has the right to claim the benefit of this protection in the context of cross-border healthcare. It is therefore not only an obligation on the part of the health professional or the Member State but also, and above all, a right which the patient can claim against them.[21]

It remains to agree on the content of this protection as it is implemented in the new European General Data Protection Regulation,[22] either in terms of substantive and territorial scope, applicable substantive rules governing data processing, data subject's rights, obligations of data controller and processor, and data protection specific authorities and mechanisms ensuring data protection effectiveness.

3. Scope of the General Data Protection Regulation

In order to claim the benefit of the General Data Protection Regulation, the patient's personal data must be automatically processed, in whole or in part, or at least be included in a file, and the situation has to fall within the territorial scope of the General Data Protection Regulation.

3.1 Material scope of the General Data Protection Regulation

As it was already the case with Directive 95/46/EC, the General Data Protection Regulation applies[23] to the processing[24] of personal data wholly or partly by automated means and to

treatment or interventions provided. Those provisions should also apply in the context of cross-border healthcare covered by this Directive.

[21] On the right to data protection, see: G Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law, Governance and Technology Series, Issues in Privacy and Data Protection, volume 16, Springer, 2014; B van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right ?', in R Leenes, R van Brakel, S Gitwirth and P De Hert (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures*, Law, Governance and Technology Series, Issues in Privacy and Data Protection, volume 36, Springer, 2017, p. 3.

[22] The provisions of which apply from 25 May 2018.

[23] See Article 2 for the material scope of the Regulation. See the exclusion for activities falling outside the scope of Union law and purely personal or household activities (Recital no. 18: "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 and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities)".

[24] 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or

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.[25]

The definition of *personal data* remains substantially unchanged except for the description of the elements likely to help to identify the data subject.[26] It should be recalled that, in accordance with Directive 95/46/EC, the General Data Protection Regulation and the case-law of the Court of Justice of the European Union, the concept of *personal data* must be interpreted as widely as possible. However it has been suggested, but to no avail so far, to set contextual limits on the possibility of identifying the data subject, in order to respond to the criticism, partially justified, that by giving an excessive and somehow unlimited scope to the legislation,[27] it ends up covering almost any kind of situations even when there is no informational content or when no one involved in the data processing is able to reasonably identify the data subject. It is possible to wonder whether this does not proceed from an operational difficulty in distinguishing the data or the processing which really matters.

However, whatever the controversies surrounding the notion of personal data,[28] it is likely that in almost all situations the patient's data in cross-border healthcare will be subjected to an automated processing, in whole or in part, or will be included in a file, as it should be in a modern and state-of-the-art practice of healthcare.

3.2 Territorial scope of the General Data Protection Regulation

The General Data Protection Regulation applies first of all to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.[29] It is thus beyond doubt that the processing of patient's data carried out by a healthcare professional providing cross-border healthcare to a patient falls under the scope of the Regulation.[30]

---

otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4.2 of the Regulation).

[25] The filing system means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis (Article 4.6 of the Regulation).

[26] Personal data means 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. The data subject does not have to be identified. It only has to be possible to identify the data subject. (Article 4.1 of the Regulation).

[27] Like data which does not yet qualify as personal data but which could become so in the light of technological developments.

[28] And they will be solved gradually as the Regulation is implemented and enforced.

[29] Article 3.1 of the Regulation.

[30] If the data controller or processor is not established in the Union, the Regulation applies to the processing of personal data of data subjects who are in the Union where the processing activities are related to 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 the monitoring of their behavior as far as their behavior takes place within the Union (Article 3.2). But the Regulation does not specify what is meant by a person who is on the territory of the European Union. This concept may cover accidental or tourist presence, transit, mere residence, domicile or principal or

4. Main actors in Data Protection

Like the Convention of 28 January 1981 or Directive 95/46/EC, the General Data Protection Regulation does not explicitly determine its personal scope. However, the Regulation identifies the main actors in data protection. As in Directive 95/46/EC, the [data] controller is the person who, alone or jointly with others, determines the purposes and means of the data processing[31] and the processor is the one who processes personal data on behalf of the [data] controller.[32] The Regulation also identifies the recipient,[33] the third party,[34] the representative,[35] the enterprise[36] and the group of undertakings.[37]

However, as with Directive 95/46/EC, the General Data Protection Regulation still does not provide a formal definition of the data subject even though the latter is supposed to be at the heart of the regulatory system. Whatever, the Regulation insists on the point that the protection applies irrespective of the nationality or residence of the data subject.[38]

---

secondary establishment in the territory of the European Union [within the territory of a Member State of the European Union]. Moreover, these notions do not have necessarily the same meaning in all the Member States. Finally the Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

[31] The [data] controller means 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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (Article 4.7 of the Regulation). See Article 29 Data Protection Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"* WP 169 16 February 2010.

[32] The processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4.8 of the Regulation).

[33] The recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing (Article 4.9 of the Regulation).

[34] The third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data (article 4.8 of the Regulation).

[35] The representative means a natural or legal person established in the Union who, designated by the controller or processor, represents the controller or processor with regard to their respective obligations (Article 4.8 of the Regulation).

[36] The enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity (Article 4.8 of the Regulation).

[37] The group of undertakings means a controlling undertaking and its controlled undertakings (Article 4.8 of the Regulation).

[38] See recital 14. The protection extends to persons who are not nationals of any Member State and who do not reside in the territory of any Member State but whose data are processed by a data controller subject to the Regulation. In any case, this protection is expressly excluded for legal persons (see recital 14). The Regulation is, however, once again ambiguous. Indeed, it states that "This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person". This last sentence seems to imply a form of derogation, which would mean that there would be some form of

In any case, all these actors must be properly identified when a health professional provides healthcare to a patient from a Member State other than the Member State of affiliation. This can lead to some problems in particular in the context of Internet platforms for patient's data communication, cloud computing services[39] or mobile applications (mHealth).[40]

5. Substantive rules applicable to the processing of patient's personal data

The processing of patient's personal data may be subject to two types of substantive rules: on the one hand, the common uniform substantive rules laid down by the General Data Protection Regulation and, on the other hand, additional national substantive rules laid down by Member States.

5.1 Common uniform substantive rules applicable to the processing of personal data

The Regulation enumerates and details the principles applicable to all data processing. The principles are not that substantially different from the rules previously laid down in Directive 95/46/EC.

Principles relating to the processing of personal data

There are seven principles relating to the processing of personal data:

i) Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (principles of *lawfulness, fairness and transparency*);

ii) Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is *incompatible* with those purposes (principle of *purpose limitation*).[41] Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should not be considered as incompatible with the initial purposes provided that it is subject to appropriate safeguards for the rights and freedoms of the data subject. These guarantees must ensure that technical and organizational measures are set in place to ensure compliance with the data minimization principle.[42] Whenever

protection for other data related to enterprises. In theory, this would be inaccurate, but this recital brings unnecessary doubt.

[39] See Article 29 Data Protection Working Party *Opinion 05/2012 on Cloud Computing* WP 196 1st July 2012.

[40] See Article 29 Data Protection Working Party *Opinion 02/2013 on apps on smart devices* WP 202 27 February 2013.

[41] See Article 29 Data Protection Working Party *Opinion 03/2013 on purpose limitation* WP 203 2 April 2013.

[42] These measures may include pseudonymization, to the extent that these purposes can be achieved in this way. Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure

possible, further processing should not or no more allow for the identification of the data subject.

iii) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of *data minimization*).

iv) Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (principle of *accuracy*).

v) Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (principle of *storage limitation*). Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes provided that it is subject to appropriate safeguards for the rights and freedoms of the data subject. These guarantees must ensure that technical and organizational measures are set in place to ensure compliance with the data minimization principle.[43] Whenever possible, further processing should not or no more allow for the identification of the data subject.

vi) Personal data must be processed in a manner that ensures an appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (principle of *integrity and confidentiality*).

vii) The controller is responsible for the compliance with the principles applicable to the processing of personal data. The controller must also, and that is formally new, be able to demonstrate that the data processing is compliant with these principles (principle of *accountability*).[44]

Data processing lawfulness

The General Data Protection Regulation lists the categories of situations in which it is a priori, lawful, that is to say, as permitted by law, to process personal data.[45] It is assumed, for each of these situations, that it is legitimate in general to process personal data. To put it another way, each of these categories is supposed to represent a situation in which the interests involved are in an acceptable balance. The interests to be taken into consideration are those of the data controller, the data subject and the community. In line with the legitimation mechanisms set up in Directive 95/46/EC, it is of course necessary to verify in each individual case for each data processing taken and considered separately and

---

that the personal data are not attributed to an identified or identifiable natural person (Article 4.5 of the Regulation).

[43] ibid.

[44] See Article 29 Data Protection Working Party *Opinion 3/2010 on the principle of accountability* WP 173 13 July 2010.

[45] See Article 6 of the Regulation and the possibility of special arrangements for processing imposed by law or carried out in the public interest or in the exercise of official authority by the controller and the flexibility of the criterion for the compatibility of further data processing.

individually whether there is a fair balance between these three kind of interests *in concreto* and not only *a priori* and *in abstracto*. In this respect, changing the balance of interests over time will have the effect of removing the legitimacy of the data processing for the future. The data processing will have to be stopped except for a solution to satisfactorily rebalance the interests involved. It must be reiterated that the assessment of the legitimacy of data processing is sensitive to other aspects of the implementation of data protection, such as the level of confidentiality and security of the data processing, the level of control exercised by the national supervisory authority, the degree of necessity of the purpose pursued, and so on.

The rule regarding the processing of sensitive data is well known and has not changed: the processing of 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[46] or data concerning a natural person's sex life or sexual orientation are prohibited.[47] This prohibition does not apply in the situations detailed in the Regulation,[48] without prejudice to the need to verify *in concreto* the existence of a fair balance between the interests involved in each processing.

If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller is no more be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the General Data Protection Regulation.[49] In addition, the Regulation provides that, if possible, the controller will inform the data subject when it is able to demonstrate that it is not in a position to identify the data subject (sic). In such cases, the data subject must provide additional information to enable the data controller to control his or her identity identify for the purpose of exercising his or her right of access, to rectify, to cancel, to limitation of treatment, to notification of rectification or deletion of data or limitation of processing, or to data portability.[50]

[46] Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status (Article 4.15 of the Regulation). Recital 35 of the Regulation provides that "Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test".

[47] Article 9.1 of the Regulation.

[48] Article 9.2 of the Regulation.

[49] Article 11.1 of the Regulation.

[50] See Article 11.2 of the Regulation.

None of this prevents the data controller from being, for the rest, subject to all the other obligations arising from the General Data Protection Regulation.

5.2 Additional national substantive rules applicable to the processing of personal data related to health

Surprisingly, while one of the objectives of the reform of the legal framework for data protection was to eliminate inconsistencies between Member States regarding the processing of personal data relating to health, the General Data Protection Regulation provides that, in respect of the subsidiarity principle, Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.[51] It follows that the differences between Member States, which have been strongly condemned, are likely to increase in the matter of personal data related to health.

It remains, of course, that, in any case, Member States are bound by the common legal framework that emerges from the case-law of the European Court of Human Rights in the field of data protection and by the rights therefore granted to individuals in terms of data control (situations in which the Court considers that the person is entitled to expect that data will not be disclosed without his or her consent), data access (including access to medical records) or medical records security, for example.

It should be noted that the General Data Protection Regulation does not lay down criteria for delimiting the territorial scope of the national provisions that Member States might adopt regarding the processing of genetic data, biometric data or health.[52]

6. Patient's rights on the processing of personal data

Where Directive 95/46/EC formally recognized three rights (right of access, right to object to data processing and right not to be subject to individual automated decisions), the General Data Protection Regulation grants data subject with eight rights (right to information, right of access, right to rectification, right to erase, right to limit treatment, right to data portability, right to object to data processing and right not to be subject to automated individual decisions).[53]

[51] Article 9.4 of the Regulation.

[52] Article 9.4 *in fine* of the Regulation.

[53] See the limits which may be imposed on these rights by Union law or by the law of the Member State to which the controller or processor is subject, by means of legislative measures, in accordance with Article 23 of the Regulation. These limits are permissible only if they respect the essence of fundamental rights and freedoms and are necessary and proportionate measures in a democratic society to guarantee one of the objectives listed in this provision.

In particular, the right to data portability[54] means that, where the data are processed on the basis of the data subject's consent or a contract and by automated means, the data subject has the right to request and receive in a structured, commonly used and machine-readable format, the data he or she has provided to the data controller. The data subject is then entitled to forward these data to another data controller. The data subject may also ask the first controller to send them directly to another data controller if technically feasible.[55] This right inevitably brings to mind the situation in which the patient's medical record is communicated between healthcare professionals in order to ensure the continuity of care. The implementation of this newly formalized right may therefore not be a problem in the health sector as long as it is extended to data not provided by the patient.[56]

That being said, the real challenge is to know how these rights will really and effectively prosper in the light of the debates around cloud computing services, big data and mobile applications,[57] and whether this formal increase in the number of rights will improve data protection and the benefit to the patient from the information society participation. Doubt is permitted.

7. Additional obligations of the data controller and processor

Beyond the uniform substantive rules laid down by the General Data Protection Regulation and the substantive rules that national law of each Member State could add, the data controller (and the processor)[58] is subject to another series of general obligations which represent as many new uniform substantive rules to comply with.

Implementation of technical and organizational measures

The data controller (and processor) must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the data processing is performed in accordance with the General Data Protection Regulation. In doing so, the data controller has to take 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. Those measures must be reviewed and updated where necessary. Where

[54] Article 29 Data Protection Working Party *Guidelines on the right to data portability* WP 242 13 December 2016.

[55] See Article 20 of the Regulation. This right is without prejudice to the right to erasure or to be forgotten. That right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition, it cannot adversely affect the rights and freedoms of others.

[56] In any case, Article 4.2 (f) of Directive 2011/24/EC provides that "in order to ensure continuity of care, patients who have received treatment are entitled to a written or electronic medical record of such treatment, and access to at least a copy of this record in conformity with and subject to national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC".

[57] What about algorithmic governance in healthcare?

[58] See Article 26 of the Regulation for the case of joint data controllers, Article 27 for the representative of data controllers or processors who are not established in the territory of the European Union and Article 28 for the special rules applicable to processors.

proportionate in relation to processing activities, these measures must include the implementation of appropriate data protection policies by the data controller.[59]

Privacy by design

The data controller (and processor) must implement, both at the time of the determination of the means for processing and at the time of the processing itself, appropriate technical and organizational measures (such as pseudonymization) which are designed to implement data-protection principles (such as data minimization) in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of General Data Protection Regulation and protect the rights of data subjects. In doing so, the data controller has to take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.[60]

Privacy by default

The data controller (and processor) must implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures must ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.[61]

Processing on instruction

As a rule, the processor and any person acting under the authority of the data controller or processor who has access to personal data cannot process these data unless instructed by the data controller, unless a legal duty to do so imposed by Union law or the law of a Member State.[62]

Records of processing activities

Due to a lack of understanding of its use in the daily enforcement of the data subject's rights, the General Data Protection Regulation regrettably has ended the obligation to held a public registry which was easily accessible on line by everyone. This public registry has been replaced by the data controller obligation to maintain a record of processing activities.[63] This means that a unique public registry has been replaced by a multitude of private registries which are not freely and unconditionally accessible. Moreover, this

[59] See Article 24 of the Regulation. The application of an approved code of conduct or approved certification mechanisms may serve as a means of demonstrating compliance with the obligations of the data controller.
[60] On this, see Article 25.1 of the Regulation. An approved certification mechanism may serve as an element to demonstrate compliance with these requirements.
[61] See Article 25.2 of the Regulation. Again, an approved certification mechanism can serve as an element to demonstrate compliance with these requirements.
[62] Article 29 of the Regulation.
[63] See Article 30 of the Regulation. This register may be in written or electronic form. It must be made available to the supervisory authority on request.

obligation does not apply to an enterprise or an organization employing fewer than 250 persons unless the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional or the processing includes special categories of data or personal data relating to criminal convictions and offences.[64]

Similarly, and under the same conditions as the data controller, each processor and, where appropriate, the processor's representative, must maintain a record of all categories of processing activities carried out on behalf of the data controller.

Cooperation with supervisory authorities

The data controller and the processor and, where applicable, their representatives, must cooperate, on request, with the supervisory authority in the performance of its tasks.[65]

Security of personal data

The data controller and processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. They must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. In assessing the appropriate level of security, they must take into account in particular the risks presented by the data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.[66]

In any case, the data controller and processor must take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless required to do so by Union or Member State law.

Notification of personal data breach to supervisory authorities and data subjects

In the case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (known as *personal data breach*),[67] the data controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it,[68] notify the personal data breach to the competent supervisory authority.[69] The data

[64] See Article 30.5 of the Regulation.
[65] Article 31 of the Regulation. The application of an approved Code of Conduct or an approved certification mechanism may serve as an element to demonstrate compliance with data processing security requirements.
[66] See Article 32 of the Regulation.
[67] Article 4.12 of the Regulation. See Article 29 Data Protection Working Party Working *Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* WP 184 5 April 2011 and *Opinion 03/2014 on Personal Data Breach Notification* WP 213 25 March 2014.
[68] See Article 33 of the Regulation. Where the notification to the supervisory authority is not made within 72 hours, it has to be accompanied by reasons for the delay. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
[69] The notification must, at least: i. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; ii. communicate the name and contact details of the data

controller is exempted when the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. But, in any case, the data controller must document any personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken. That documentation must enable the supervisory authority to verify the compliance with the obligations applicable to the data controller.

Similarly, the processor must notify to the data controller without undue delay after becoming aware of a personal data breach. It must be assumed that it is also required to document any data breaches even if this is not expressly foreseen in the Regulation.

Asymmetrically in relation to the obligation to notify the supervisory authority, the data controller must only communicate the personal data breach to the data subject if the breach is likely to result in a high risk to the rights and freedoms of natural persons. The communication must be done without undue delay. The communication to the data subject must describe in clear and plain language the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned. It must also contain the name and contact details of the data protection officer or any other contact point where more information can be obtained, the likely consequences of the personal data breach, the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

However, even in the event of a high risk to rights and freedoms, this communication is not always required. Furthermore, if the data controller has not already communicated the data breach to the data subject, the supervisory authority may, after examining whether this data breach is likely to result in a high risk, require the data controller to do the communication or decide that the controller is in one of the situations in which he is exempted to do so.[70]

Privacy impact assessment

Prior to the processing, the data controller must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data[71] where a type of processing, particularly when using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights

protection officer or other contact point where more information can be obtained; iii. describe the likely consequences of the personal data breach; iv. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

[70] Article 34 of the Regulation.

[71] See: D Wright and P De Het (eds), *Privacy Impact Assessment*, Law, Governance and Technology Series, volume 6, Springer, 2012 and 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* WP 248 4 April 2017.

and freedoms of natural persons. The controller will seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.[72]

The data controller will consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.[73]

Where the supervisory authority is of the opinion that the processing would infringe the General Data Protection Regulation, especially when the data controller has insufficiently identified or mitigated the risk, the supervisory authority must, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its investigating powers, correcting powers, advisory powers or any other power conferred by its national law.[74]

Data protection officer

The obligation to appoint a data protection officer is one of the measures that has received particular attention. Beyond the situation in which that this designation is required under organizational measures to ensure the security and confidentiality of data processing, the

[72] See Article 35 of the Regulation. A single assessment may address a set of similar processing operations that present similar high risks. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment (leaving open the question of the obligation to do so when the controller had no obligation (formally or in the framework of technical and organizational measures) to designate one but still did it).
The supervisory authority must establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. The supervisory authority must communicate those lists to the European Data Protection Board. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board. Prior to the adoption of the lists, the competent supervisory authority will apply the consistency mechanism where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behavior in several Member States, or may substantially affect the free movement of personal data within the Union.
Compliance with approved codes of conduct by the relevant controllers or processors must be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.
Where appropriate, the data controller must 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.
[73] When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with (Article 36.3 of the Regulation): i) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings; ii) the purposes and means of the intended processing; iii) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation; iv) where applicable, the contact details of the data protection officer; v) the data protection impact assessment; vi) and any other information requested by the supervisory authority.
[74] See Article 58 of the Regulation.

data controller and the processor are in any case obliged to designate a data protection officer[75] in three cases:[76]

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;[77]
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope or purposes, require regular and systematic monitoring of data subjects on a large scale;
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

8. Specific data protection bodies, mechanisms and remedies

In order to ensure data protection effectiveness, provision was made to create specific data protection authorities as well as specific mechanisms and remedies.

8.1 Supervisory authorities

At the level of the Member States, each Member State must provide for one or more independent public authorities to be responsible for monitoring the application of the General Data Protection Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of

[75] Article 37 of the Regulation: the data protection officer must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil its tasks. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. See Article 29 Data Protection Working Party *Guidelines on Data Protection Officers ('DPOs')* WP 243 rev.01 5 April 2017. The data controller or the processor must publish the contact details of the data protection officer and communicate them to the supervisory authority.

[76] See Article 37 of the Regulation. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organizational structure and size. When there is no obligation to appoint a data protection officer, the data controller or processor or associations and other bodies representing categories of data controllers or processors may or, where required by Union or Member State law must, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

[77] There remains to found a justification for this discrimination all the more astonishing at a time when justice tries to reach the 21st century.

personal data within the Union.[78] Each supervisory authority must act with complete independence in performing its tasks and exercising its powers.[79]

At the level of the European Union, the European data protection Board replaces the Working Party on the protection of individuals with regard to the processing of personal data (the Working Party).[80] The Board is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives. The Board must act independently when performing its tasks or exercising its powers. In the performance of its tasks or the exercise of its powers, the Board will neither seek nor take instructions from anybody. The Board will draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organizations. The European data protection supervisor will provide the secretariat of the Board.[81]

8.2 Data subject's remedies

Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, every data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the General Data Protection Regulation.[82]

Right to an effective judicial remedy against a supervisory authority

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.[83, 84]

---

[78] See Article 51 of the Regulation on the principle of independence and Article 55 on the issue of the competence of the supervisory authority (cf. Article 4.22 of the Regulation for the definition of the *supervisory authority concerned*). It is expressly provided that the supervisory authorities are not competent to review the processing operations carried out by the courts in the exercise of their judicial function (Article 55.3 of the Regulation). The duties and powers of the supervisory authorities are detailed in Articles 57 and 58 of the Regulation. See Article 29 Data Protection Working Party *Guidelines for identifying a controller or processor's lead supervisory authority* WP 244 13 December 2016.

[79] See Article 52 of the Regulation.

[80] See Article 68 of the Regulation. Article 70 lists its missions.

[81] The European Data Protection Supervisor is also the supervisory authority for EUROPOL.

[82] It is not easy to argue that this right exists in the case of a breach of a rule which would be imposed by a Member State within the scope of the discretion which would be accorded to the State for the implementation of a particular provision of the Regulation. See Article 80 on the question of the representation of data subjects.

[83] Directive 95/46/EC already provided that *Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts* (Article 28.3, *in fine*).

[84] See Article 78.1 of the Regulation. Proceedings against a supervisory authority must be brought before the courts of the Member State where the supervisory authority is established. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint.[85]

Right to an effective judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the General Data Protection Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with the General Data Protection Regulation.[86]

Right to compensation and liability

Any person who has suffered material or non-material damage as a result of an infringement of the General Data Protection Regulation has the right to receive compensation from the controller or processor for the damage suffered.[87] Any data controller involved in processing is liable for the damage caused by processing which infringes the General Data Protection Regulation. A processor is liable for the damage caused by processing only where it has not complied with obligations of the General Data Protection Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions from the data controller. A data controller or processor is exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage. Where more than one data controller or processor, or both a data controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each data controller or processor is liable for the entire damage in order to ensure effective compensation of the data subject.[88]

---

the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court (Article 78.4 of the Regulation).

[85] See Article 78.2 of the Regulation. Proceedings against a supervisory authority must be brought before the courts of the Member State where the supervisory authority is established. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court (Article 78.4 of the Regulation).

[86] See Article 79.1 of the Regulation. Proceedings against a controller or a processor must be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

[87] Court proceedings for exercising the right to receive compensation must be brought before the courts competent under the law of the Member State where the data controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

[88] See Article 82 of the Regulation. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage.

Administrative fines and penalties

Depending on the circumstances of each individual case, each supervisory authority may impose effective, proportionate and dissuasive administrative fines[89] in addition or in place of corrective measures.[90]

Member States must lay down the rules on other penalties applicable to infringements of the General Data Protection Regulation in particular for infringements which are not subject to administrative fines. They must take all measures necessary to ensure that these penalties are implemented [and enforced]. Such penalties must be effective, proportionate and dissuasive.[91]

9. Conclusions

Data protection must be guaranteed in the context of cross-border healthcare provided to a patient by a health professional in a Member State other than the Member State of affiliation. That means that the patient has the right to claim the benefit of this protection in the context of cross-border healthcare. It is therefore not only an obligation on the part of the health professional or the Member State but also, and above all, a right that the patient can claim against them.

The European Union and Member States have maintain the decision to implement a common legal framework for data protection at the European level when adopting the General Data Protection Regulation. However, in the same time, Member States may add national rules for the processing of personal data concerning health. Regarding the specificities and powers of each Member State in the matter of public health, we could wonder whether this decision should not been reversed and whether we should not have instead distinct national legal frameworks with common restrictive rules applicable to the transfer of personal data related to health between Member States. That being said, the right to data protection had to be recognized at the European level especially when considering that some Member States still do not recognize data protection as a fundamental right.

The scope of the General Data Protection Regulation is not clearer than before and regarding the new uniform substantive rules applicable to the processing of personal data, differences between Member States (which have been strongly condemned) are likely to increase in the matter of personal data related to health since Member States may maintain or introduce further conditions, including limitations, with regard to the processing of data concerning health. Of course, Member States are still bound by the common legal framework that emerges from the case-law of the European Court of Human Rights in the field of data protection and by the rights therefore granted to individuals in terms of data

[89] On all of this and in particular the factors to be taken into account in each individual case, see Article 83 of the Regulation.
[90] See the list of corrective measures in Article 58.2, a) to h), and j) of the Regulation.
[91] See Article 84 of the Regulation.

control (situations in which the Court considers that the person is entitled to expect that data will not be disclosed without his or her consent), data access (including access to medical records) or medical records security, for example. In any case, we should consider imposing that personal data concerning health are not be subtracted from the effective physical and jurisdictional powers of the data subject excluding therefore the possibility to store and process them in another country without very strict and serious justifications and constraints.

On the other hand, one cannot but, wonder how to reconciliate the general principles applicable to data processing such as transparency, fairness, minimization, accuracy, storage limitation, integrity and confidentiality, and accountability, in the light and reality of cloud computing services, big data and mobile applications that are heavily promoted in the same time by the European Union.

Some may acclaim the fact that the General Data Protection Regulation recognizes more rights to the data subject. But maybe it should have been better to find new ways to enforce already existing data subject rights before adding some new ones. In other words, recognizing new rights will not help enforcing previous rights largely and voluntarily ignored such as the basic but fundamental right of access including the right to get all the needed information about the data processing.

Because the real problem does not lie in the legal framework but well in the effective enforcement of data protection rules. We need information and sensibilization campaigns about data protection. We need fairness and transparency on data processing especially in the matter of eHealth and mHealth. We have to oppose so-called health applications promising anything and everything only to get access to personal data concerning health for commercial purposes. However, in the same time, we have to strongly promote the development of all information and communication technologies that could improve healthcare and patient's rights while respecting the distribution of powers between the European Union and the Member States in the matter of public health.