BRILL
NIJHOFF

EUROPEAN JOURNAL OF HEALTH LAW 25 (2018) 479-500

European Journal of Health Law

brill.com/ejhl

Data Protection and Biobanks in 2018

Jean Herveg
CRIDS, University of Namur, Belgium
jean.herveg@unamur.be

Abstract

Data protection rules applies to biobanks' activities to the extent that they fall under the scope of the General Data Protection Regulation, which is already susceptible to raising some difficult issues to solve. If subjected to it, biobanks' activities will have to comply with the applicable substantive rules governing data processing, data subject's rights, obligations of data controller and processor, without omitting the specific authorities and mechanisms ensuring data protection effectiveness.

Keywords

privacy – data protection – patient's rights – biobanks

1 Introduction: Some Preliminary Reminders on the Evolution and Meaning of Data Protection in European Law

Data protection is a legal discipline that studies the legal mechanisms that should be adopted and implemented with the view to protect individuals' rights and liberties, and more specifically their right to private life, in front of technologies that allows for the exploitation of data related to them.

At the level of the Council of Europe, the issue of data protection has been formally raised as soon as 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

 | DOI:10.1163/15718093-12255410

the legal framework for ensuring data protection in Europe. The first of these recommendations concerned databases in the private sector[1] and the second, databases in the public sector.[2] 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 n° 108)[3] as well as numerous sectoral or thematic recommendations.[4]

On the other hand, 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.

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,[5] the European Court of Human Rights has developed a substantial case-law in many areas interesting data protection.[6]

---

1 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.

2 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.

3 This Convention has been revised and the Convention 108+ has been adopted by the Committee of Ministers on 18 May 2018 at its 128th meeting.

4 Recommendation 97(5) on the protection of medical data is also under revision (see doc. T-PD(2018)06).

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

6 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 formally 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 2017), 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 as in some dissenting opinions, to support the opposite view and claim that any processing of personal data concerns the right to private life understood as protecting a right to informational self-determination. In any event, the principle adopted in the context of the assessment of the necessity of the interference in a democratic society made it possible not to have to decide.

At the level of the European Community (now the European Union), the issue of data protection was formally raised by the European Parliament on 8 April 1976. On 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.[7] This Legal Committee then set up a subcommittee on "Informatics and Human Rights". The latter organised a public debate on 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.[8] Then, after the adoption of the O.E.C.D Guidelines for the Protection of Privacy and Transborder Data Flows on 23 September 1980, on 24 October 1995 the European Community adopted 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.[9] Its objective was to harmonise data protection legislations across the European Community and to state the principle of the free movement of personal data within the common market. From 25 May 2018, the General Data Protection Regulation (GDPR) ensures data protection in Europe.[10]

All this has led to the explicit and formal recognition of data protection as a citizen's fundamental right in the Charter of Fundamental Rights of the European Union in 7 December 2000.[11] 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 [12] since the entry into force of the Treaty of Lisbon in December 2009.[13]

---

7 Resolution adopted on 8 April 1976 OJ n° C 100 3 May 1976, p. 27.

8 OJ 5 June 1979 n° C 140/34.

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

10 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.

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 (Heidelberg: Springer, 2015).

11 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 Fundamental Right to Data Protection in the European Catalogue of Fundamental Rights WP 26, 7 September 1999.

12 This is confirmed by Article 6 of Treaty on the European Union.

13 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) (on this, see the Explanatory

The Treaty on the Functioning of the European Union also recognises a right to data protection under its provisions of general application.[14] It is to this extent that any person who comes under the jurisdiction of a Member State[15] has the right to claim the protection of his or her personal data.[16]

More recently, in the case of *Satakunnan Markkinapörssi Oy et Satamedia Oy* c. *Finlande,* the European Court of Human Rights has, for the first time in its history, explicitly and formally stated that Article 8 of the European Convention on Human Rights protected a form of informational self-determination, which is remarkable.[17]

In other words, it is now widely accepted in Europe that everyone is entitled to master and control to a certain degree what could be done for what purpose by who and under which circumstances and conditions about personal data related to them. It is usually understood that this right is protected by the right to private life. In other words, the right to private life includes a right to master and control personal data.

Therefore, the first goal of data protection law is to regulate the processing of personal data in order to limit the interference with the data subjects' rights (to master and control the personal data related to them) to the extent of what is strictly necessary to achieve the legitimate goal pursued by the data processing. The second objective of data protection law is to guarantee the data subjects' rights regarding the personal data related to them (right of access, etc.).

This article aims at feeding the discussion about the impact of data protection on biobanks' activities and more especially on the extent to which they fall under the scope of the GDPR, on the duties of the data controller and

---

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).

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.

14 See Article 16.

15 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.

16 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, (Heidelberg: Springer, 2014); B van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?', in: R. Leenes, R. van Brakel, S. Gutwirth 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 (Heidelberg: Springer, 2017), p. 3.

17 *Satakunnan Markkinapörssi Oy et Satamedia Oy* c. *Finlande* App n° 931/13 (ECtHR, 27 June 2017) § 137.

processor, on the data subject's rights, and on data protection specific authorities and mechanisms ensuring data protection effectiveness.

2 The Extent to which Biobanks' Activities May Fall under the Scope of the General Data Protection Regulation

Biobanks' activities fall under the scope of the General Data Protection Regulation only to the extent that they concern the automated processing of personal data, in whole or in part, or at least that personal data are to be included in a file [*material scope*], and that the situation falls within the *territorial scope* of the General Data Protection Regulation.

2.1 *Biobanks and the Material Scope of the General Data Protection Regulation*

As was already the case with Directive 95/46/EC, the General Data Protection Regulation applies[18] to the processing[19] of personal data wholly or partly by automated means and to the processing other than by automated means of personal data that form part of a filing system or are intended to form part of a filing system.[20]

The definition of personal data remains substantially unchanged except for the description of the elements likely to help to identify the data subject.[21] 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

18 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 (cf. Recital n° 18).

19 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 (Article 4.2 of the Regulation).

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

21 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).

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 ([22]), 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 that really matters.

Regarding biobanks' activities, we should distinguish between the sources of personal data [*human corporal materials*] and the personal data processed from these sources [mainly the information produced by the analysis of these materials], even if security and organizational measures should be implemented in order to prevent any unauthorized and unlawful processing of personal data from human corporal materials.

2.2 *Biobanks and the 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.[23] Regarding biobanks' activities, it is worth knowing that when resorting to the services of a processor[24] established in the European Union, the entity established outside the European jurisdiction will nevertheless fall under the scope of the General Data Protection Regulation. This means that the data subjects located outside the European jurisdiction and

22 Like data that does not yet qualify as personal data but that could become so in the light of technological developments.

23 Article 3.1 of the Regulation. 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). 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.

24 On the notion of processor, see: J. Herveg and J.-M. Van Gyseghem, 'Un nouveau métier de la santé: la sous-traitance des données du patient', in C. de Terwangne, E. Degrave, S. Dusollier and R. Queck (eds.) *Law, Norms and Freedoms in Cyberspace. Droit, normes et libertés dans le cybermonde. Liber Amicorum Yves Poullet* (Brussels: Ed. Larcier, Collection du CRIDS, 2018), p. 747.

concerned by the data processing will be awarded the same protection and the same rights as if they were under the European jurisdiction. This might, of course, lead to real problems in the country of origin.

3 The Main Actors of Data Protection and Biobanks

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[25] and the processor is the one who processes personal data on behalf of the [data] controller.[26] The Regulation also identifies the recipient,[27] the third party,[28] the representative,[29] the enterprise[30] and the group of undertakings.[31]

25 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.

26 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).

27 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).

28 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 authorised to process personal data (Article 4.8 of the Regulation).

29 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).

30 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).

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

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. This raises an important issue in several fields and especially for biobanks notably when you need to identify the persons who have to consent to the processing of personal processing or who must receive the mandatory information about the data processing.

Whatever, the Regulation insists on the point that the protection applies irrespective of the nationality or residence of the data subject.[32]

4 Biobanks and the Substantive Rules Applicable to the Processing of Personal Data

The processing of personal data occurring in biobanks' activities 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.

4.1 *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.

4.1.1 Principles Relating to the Processing of Personal Data

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

1. Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (principles of *lawfulness*, *fairness* and *transparency*).
2. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is *incompatible*

32 See Recital n° 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 n° 14).

with those purposes (principle of *purpose limitation*) ([33]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 organisational measures are set in place to ensure compliance with the data minimisation principle.[34] Whenever possible, further processing should not or no more allow for the identification of the data subject.

3. 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 minimisation*).
4. 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*).
5. Personal data must be kept in a form that 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 organisational measures are set in place to ensure compliance with the data minimisation principle.[35] Whenever possible, further processing should not or no more allow for the identification of the data subject.
6. Personal data must be processed in a manner that ensures an appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss,

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

34 These measures may include pseudonymisation, to the extent that these purposes can be achieved in this way (on pseudonymisation, see Article 4.5 of the Regulation).

35 *Ibid.*

destruction or damage, using appropriate technical or organisational measures (principle of *integrity and confidentiality*).

7. 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*).[36]

4.1.2 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.[37] It is assumed, for each of these situations, that it is legitimate in general to process personal data. In line with the legitimation mechanisms set up in Directive 95/46/EC, it is of course necessary to verify in each individual case, and each data processing taken and considered separately and individually whether there is a fair balance between these three kinds 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[38] or data concerning a

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

37 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.

38 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). (See also Recital n° 35.)

natural person's sex life or sexual orientation are prohibited.[39] This prohibition does not apply in the situations detailed in the Regulation,[40] 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 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.[41] 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. In such cases, the data subject must provide additional information to enable the data controller to control his or her identity 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.[42]

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.

4.2 *Additional National Substantive Rules Applicable to the Processing of Personal Data Related to Health*

Complying with 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.[43] 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.[44]

4.3 *Safeguards and Derogations for Scientific Research or Statistical Purposes*

Data processing for scientific research or statistical purposes must be subjected to appropriate safeguards that refer notably to data minimisation (e.g. through pseudonymisation). However, the use of processing that does not permit or no

39 Article 9.1 of the Regulation.
40 Article 9.2 of the Regulation.
41 Art. 11.1 of the Regulation.
42 See Article 11.2 of the Regulation.
43 Article 9.4 of the Regulation.
44 Article 9.4 *in fine* of the Regulation.

longer permits the identification of data subjects is favoured. Member States may provide for derogations to data subjects' rights.[45]

5 Data Subject's Rights on the Processing of Personal Data in Biobanks' Activities

Data subjects' rights apply also to biobanks' activities falling under the scope of the General Data Protection Regulation. But, where Directive 95/46/EC formally recognised 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,[46] right to object to data processing and right not to be subject to automated individual decisions.[47]

In the field of biobanks, the right to portability raises the question of the kind of data subjected to portability. Obviously, it covers the data effectively handed over by the data subject. However, does it cover clinical observations or results from clinical analysis? The European Data Protection Committee considers that, in general, it covers data resulting from the monitoring of data subject's activities but not the data produced by the data controller.[48] It excludes deduced or derived data, including data produced by a third-party service provider.

45 Article 89 of the Regulation.

46 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. See also Article 29 Data Protection Working Party *Guidelines on the right to data portability* WP 242 13 December 2016.

47 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.

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

6 Biobanks and the 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)[49] is subject to another series of general obligations that represent as many new uniform substantive rules to comply with. It also applies to biobanks' activities relating to the processing of personal data.

6.1 *Implementation of Technical and Organisational Measures*

The data controller (and processor) must implement appropriate technical and organisational measures to ensure and 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 consider 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 proportionate in relation to processing activities, these measures must include the implementation of appropriate data protection policies by the data controller.[50]

6.2 *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 organisational measures (such as pseudonymisation) that are designed to implement data-protection principles (such as data minimisation) 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

49 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.

50 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.

well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.[51]

6.3 *Privacy by Default*

The data controller (and processor) must implement appropriate technical and organisational measures for ensuring that, by default, only personal data that 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.[52]

6.4 *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.[53]

6.5 *Records of Processing Activities*

The General Data Protection Regulation has ended the obligation to hold a public registry. It has been replaced by the data controller obligation to maintain a record of processing activities.[54] This obligation does not apply to an enterprise or an organisation 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.[55]

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.

---

51 On this, see Article 25.1 of the Regulation. An approved certification mechanism may serve as an element to demonstrate compliance with these requirements.

52 See Article 25.2 of the Regulation. Again, an approved certification mechanism can serve as an element to demonstrate compliance with these requirements.

53 Article 29 of the Regulation.

54 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.

55 See Article 30.5 of the Regulation.

6.6 *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.[56]

6.7 *Security of Personal Data*

The data controller and processor must implement appropriate technical and organisational 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 consider in particular the risks presented by the data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.[57]

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.

6.8 *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, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (known as *personal data breach*,[58] the data controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it,[59] notify the personal

56 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.

57 See Article 32 of the Regulation.

58 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.

59 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.

data breach to the competent supervisory authority.[60] 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.[61]

60 The notification must, at least: 1. 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; 2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; 3. describe the likely consequences of the personal data breach; 4. 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.

61 Article 34 of the Regulation.

6.9 *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[62] 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 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.[63]

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.[64]

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 a 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.[65]

6.10 *Data Protection Officer*

The obligation to appoint a data protection officer is one of the measures that has received particular attention and is of special interest for biobanks' activities. Beyond the situation in which that this designation is required under organisational measures to ensure the security and confidentiality of data processing, the data controller and the processor are in any case obliged to designate a data protection officer in three cases:[66]

62 See: D. Wright and P. de Hert (eds.), *Privacy Impact Assessment, Law, Governance and Technology Series*, volume 6 (Heidelberg: Springer, 2012); 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.

63 See Article 35 of the Regulation.

64 See Article 36.3 of the Regulation for the information to be provided when consulting the supervisory authority.

65 See Article 58 of the Regulation.

66 See Article 37 of the Regulation and Article 29 Data Protection Working Party *Guidelines on Data Protection Officers ('DPOs')* WP 243 rev.01 5 April 2017.

1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;[67]
2. 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;
3. 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.

7 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. This also concerns biobanks' activities.

7.1 *Supervisory Authorities*

At the level of the Member States, each Member State must provide for one or more independent public authority 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 personal data within the Union.[68] Each supervisory authority must act with complete independence in performing its tasks and exercising its powers.[69] 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).[70]

67 A justification remains to be found for this discrimination, all the more astonishing at a time when justice tries to reach the 21st century.

68 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*). 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.

69 See Article 52 of the Regulation.

70 See Article 68 of the Regulation. Article 70 lists its missions. The European Data Protection Supervisor is also the supervisory authority for EUROPOL.

7.2 *Data Subject's Remedies*

7.2.1 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.[71]

7.2.2 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.[72,73]

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority that 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.[74]

7.2.3 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 in cases where

71 See Article 80 on the question of the representation of data subjects.

72 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).

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

74 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).

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.[75]

7.2.4 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.[76] Any data controller involved in processing is liable for the damage caused by processing that 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.[77]

7.2.5 Administrative Fines and Penalties

Depending on the circumstances of each individual case, each supervisory authority may impose effective, proportionate and dissuasive administrative

75 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.

76 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.

77 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.

fines[78] in addition or in place of corrective measures.[79] Member States must lay down the rules on other penalties applicable to infringements of the General Data Protection Regulation in particular for infringements that 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.[80] But public bodies and public authorities are not concerned except if provided for otherwise by national law.

8 Conclusions

At the European Union level, the General Data Protection Regulation ensures the protection of the data subject in the matter of the processing of personal data. Data subjects are entitled to this protection even in the field of biobanks' activities.

However, the scope of the General Data Protection Regulation is not clearer than before. Regarding the new uniform substantive rules applicable to the processing of personal data, differences between Member States are likely to increase in the matter of personal data related to health since Member States may maintain or introduce further conditions, including limitations, regarding the processing of specific categories of personal data like genetic data and personal data concerning health. Of course, Member States are still bound by the 28 January 1981 Convention for the protection of individuals with regard to automatic processing of personal data (now Convention 108 +) and by 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 data security, for example. In any case, we should consider imposing that personal data concerning health should 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 reconcile the general principles applicable to data processing such as transparency, fairness,

78 On all of this and in particular the factors to be taken into account in each individual case, see Article 83 of the Regulation.

79 See the list of corrective measures in Article 58.2(a)-(h) and (j) of the Regulation.

80 See Article 84 of the Regulation.

minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability, in the light and reality of biobanks activities, 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 recognises 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, recognising 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.

The problem is not the content of data protection law but its effective enforcement. We need information and sensibility campaigns about data protection. We need fairness and transparency on data processing also in the field of biobanks. 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 Member States in the matter of public health.