Safeguards and Derogations Relating to Processing for Scientific Purposes: Article 89 Analysis for Biobank Research

Anne-Marie Duguet and Jean Herveg

Abstract When complying with appropriate safeguards, the processing of personal data for scientific research under the GDPR benefits from a special regime which is of interest for biobank research. On the one hand, under this condition, the further processing of personal data will not be incompatible with the initial purposes for which the data were originally collected and processed and it allows for retaining data for longer periods of time for scientific research. Complying with this condition is a condition to lift the prohibition to process special categories of personal data in the context of scientific research. On the other hand, complying with this condition makes it possible to derogate to some extent to several data subjects' rights such as the right of access, the right to rectification, the right to the restriction of processing and the right to object to the processing.

Possible safeguards range from specific procedures to support the exercise of data subjects' rights to the use of anonymous data or (where necessary) of pseudonymised data, the appointment of a data protection officer, enforcing a procedure to ensure a feedback to data subjects on the results of the research, requiring specific professional accreditations, creating a specific supervisory body for the biobank research, or the creation of a specific Code of conduct for biobank research activities.

This double regime under the GDPR is finally compared with the 2009 OECD Guidelines in biobanks and genetic research databases.

1 Introduction

The GDPR regulates the processing of personal data and recognizes subjective rights to data subjects. In particular, it provides special rules for processing personal data for scientific research. Thereby, as a rule, the processing of personal data for scientific research must be subject to appropriate safeguards for the rights and

A.-M. Duguet (✉)
UMR/INSERM 1027 Université Paul Sabatier, Toulouse, France

J. Herveg
Centre de recherches information, droit et société, University of Namur, Namur, Belgium
e-mail: jean.herveg@unamur.be; http://www.crids.eu

S. Slokenberga et al. (eds.), *GDPR and Biobanking*, Law, Governance and Technology Series 43, https://doi.org/10.1007/978-3-030-49388-2_7

freedoms of the data subject, in accordance with Article 89.1,[1] without prejudice to respecting the other rules imposed by the GDPR.[2]

The obligation to comply with appropriate safeguards applies to all data processing for scientific research, whether it is a primary or secondary data processing or an initial or further data processing.

Complying with these appropriate safeguards opens the door to a specific regime for processing personal data for scientific research: relaxing of some rules applicable to all data processing and possibility for Member States to provide for derogations to data subject's rights.

This chapter aims at grasping the specificities of this regime in the matter of data processing for scientific research and studying the ways to conceive these appropriate safeguards, in the field of biobanks.

2 The Special Regime for Processing of Personal Data for Scientific Research Applied to Biobanks

Biobanks for research consist of a collection of biological materials and associated medical data. The biological material collected is variable: blood, urine, tissue samples, surgical pieces, organ fragments, tumors, etc. Data of different nature are associated with the samples: data relating to the subject's identity (first name, name, age, date of birth, etc.), data relating to the pathology and the state of health (diagnosis, results of biological tests, treatments, risk factors, etc.), data relating to the results of the research which has been carried out (identification of biological markers, responses to certain treatments, genetic analysis, etc.). Sometimes, the data subject is not even aware about the mere existence of these data. Studies carried out in the domain of Public Health are epidemiological (and/or statistical) studies and population studies, in which cohorts of subjects are monitored over the long term and information about each individual should be nominative or coded to avoid duplication.

In principle, it is prohibited to process special categories of personal data such as those revealing racial or ethnic origin, political opinions, religious or philosophical

[1] Compare with Articles 4.1.b & 15.1 of Council of Europe Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data (Adopted by the Committee of Ministers on 27 March 2019 at the 1342nd meeting of the Ministers' Deputies).

[2] See e.g. Article 5 (b) for the purpose limitation principle, Article 9 (i) & (j) for the regime applicable to personal data concerning health and without prejudice to the power of Member State to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. On the GDPR, please consult: de Terwangne et al. (2018); Herveg (2018b), pp. 333–392; Herveg and Van Gyseghem (2018), pp. 703–762. On the specific topic of biobank, please refer to : Herveg J (2018a).

beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[3]

However, the GDPR provides derogations to the prohibition to process special categories of personal data such as e.g. having the explicit consent of the data subject or pursuing a substantial public interest or for reasons of public interest in the area of public health or for scientific research.[4] Directive 95/46/EC already provided exemptions to this prohibition which were useful for biobank activities such as e.g. the explicit consent of the data subject or appropriate national provisions applicable to biobank activities.

In comparison with the Data Protection Directive, the GDPR may be seen as having extended the notion of personal data concerning health. Indeed, it is defined as '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). Recital 35 precises 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 (1) 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.

Moreover, the strict application of data protection rules (such as the purpose limitation, the data minimization or the storage limitation principles) may be seen as being in conflict with certain research activities, particularly in the secondary use of data which requires extending the shelf life. By instance, it is not always possible to determine, at the time of data collection, the exact purposes for which data are going to be processed for scientific research purposes.

However, recital 33 recognizes that data subjects should be allowed to consent to the processing of data relating to them, in accordance with recognized ethical standards and recital 157 confirms that the prohibition to process personal data should be lifted in order to facilitate scientific research, subject to appropriate conditions and safeguards provided for in Union law or the law of Member States.

> By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on

[3] Article 9(1), GDPR.

[4] Article 9.2 (a), (g), (i) & (j), GDPR.

> a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

Thus, as long as it complies with the requirement of appropriate safeguards imposed by Article 89(1) of the GDPR, the further processing of personal data for scientific research purposes will not be incompatible with the original purposes for which the data were collected and processed.[5] The further processing then constitutes a compatible and therefore lawful processing operation.[6] This means, a contrario, that the further processing of personal data for scientific research, which does not offer adequate guarantees and therefore does not comply with the requirement laid down in Article 89(1) of the GDPR, is incompatible with the original purposes for which the data were collected and processed. Being incompatible, the processing is prohibited [unlawful] and the person who nevertheless ventures in this direction would be exposed to the risk of being prosecuted, if necessary, taking into account all the circumstances and regarding the penalties provided for by the applicable national legislation.

Similarly, compliance with Article 89(1) of the GDPR allows data to be retained for longer periods of time for scientific research purposes. More precisely, the data controller may retain the data for a longer period than is necessary for the purposes for which the data were initially processed, but only insofar as, on the one hand, the data are processed exclusively for the purposes of scientific research in accordance with Article 89(1) and, on the other hand, provided that the appropriate technical and organizational measures required by the GDPR are implemented in order to guarantee the rights and freedoms of the data subject.[7]

As seen before, compliance with Article 89(1) of the GDPR also makes it possible to lift the prohibition on processing special categories of data insofar as their processing is necessary for scientific research purposes. However, the processing must, in addition, be authorized either under Union law or under the law of a Member State, and this legal basis must (1) be proportionate to the objective pursued, (2) respect the essence of the right to data protection and (3) provide for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.[8] In any event, it should be recalled that Member States may maintain or introduce additional conditions, including limitations, for the processing of genetic, biometric or health-related data.[9] It means that there is no need to collect data subjects' consent in this case.

---

[5] Article 5(1)(b), GDPR.

[6] Recital 50, GDPR.

[7] Article 5(1)(e), GDPR.

[8] Article 9(2)(j) and recitals 52 and 53, GDPR.

[9] Article 9(4), GDPR.

It remains to find an agreement on the notion of 'scientific research', the latter being open to debate. In any case, the GDPR defines research as studies or evaluations in the health field. Recital 159 states in this respect that:

> (…) For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures. (…)

3 Derogations to Data Subjects' Rights When Processing Personal Data for Scientific Research in the Context of Biobanks

3.1 On Derogations

Compliance with the requirement of appropriate safeguards imposed by Article 89(1) of the GDPR also makes it possible to derogate from certain rights of the data subject insofar as (1) their exercise would risk making impossible or seriously impair the achievement of a specific scientific research purpose and (2) the derogation from these rights is necessary to achieve that purpose (Article 89(2) of the GDPR).

It means that Member States may elaborate specific options in their national law in order to offer derogations to data subjects' rights vis-à-vis data controllers in the field of scientific research. This concerns the following rights: right of access (Article 15), right to rectification (Article 16), right to restriction of processing (Article 18) and right to object (Article 21). The same applies to studies for statistical purposes.

3.2 Derogation to the Information Requirements

Articles 13& 14 of the GDPR impose to data controllers to provide information to data subjects whether the data are obtained from the data subject or not.

When data are collected from data subjects, data controllers must provide them with the following minimal information (Article 13(1) of the GDPR):

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49.1, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Article 13.2 imposes to the data controller to provide additional information when necessary to ensure fair and transparent processing. Data controllers must also provide information to data subjects when they plan to further process the personal data for a purpose other than that for which the personal data were collected.[10] Of course, providing information is not required when data subjects already have the information.[11]

But researchers may collect personal data from a third party. Indeed, as seen previously, as long as it complies with the requirement of appropriate safeguards imposed by Article 89(1) of the GDPR, the further processing of personal data for scientific research purposes will not be incompatible with the original purposes for which the data were collected and processed.[12] The further processing then constitutes a compatible and therefore lawful processing operation.[13] In this situation, data controllers are exempted from informing data subjects if the processing is subject to appropriate safeguards imposed pursuant to Article 89(1) of the GDPR and that, in two cases:[14]

(1) the provision of such information would prove impossible or would involve a disproportionate effort, in particular for processing for scientific research purposes;
(2) the obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing.

In such cases, data controllers will take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

This means that in the event of data recovery from third parties to conduct a research, it is possible not to inform individuals, if this act of information proves impossible to perform or would require disproportionate effort.

In practice, the question is to ascertain when it really is not possible to inform the data subject. GDPR recitals indicate that account must be taken of the number of

[10] Article 13.3, GDPR.
[11] Article 13.4, GDPR.
[12] Article 5.1(b), GDPR.
[13] Recital 50, GDPR.
[14] Article 14.5 (b), GDPR.

persons concerned, the age of the data and the appropriate safeguards that would be implemented.[15] For example, one can imagine that this will be the case if too many people were to be contacted without having the necessary information to do so. However, while it is conceivable that individual information may give rise to operational or financial problems, collective information, for example through the press, is easily accessible, at least in local press and through public media.

It must also be borne in mind that the impossibility or disproportionate difficulty of informing cannot be the result of erroneous or avoidable choices made by the data controller. In other words, the latter cannot rely on his poor organization or errors or negligence in the organization of the data processing. The data controller cannot deliberately organize data processing in such a way as to make it impossible or too difficult to inform the data subject. Thus, if the data controller failed to collect contact details or any other information that would have made it possible to contact data subjects, he cannot use it to justify the impossibility or disproportionate difficulty of complying with the obligation to inform data subjects. The data controller must respect the spirit of data protection and must not attempt to identify situations in which he could be exempted from informing data subjects. On the contrary, he must do everything possible to ensure that data subjects are duly informed. This is also a requirement from the principles of privacy by design and by default.

In addition, situations in which the information could make impossible or seriously impair the achievement of the objectives pursued by the data processing must also be exceptional. Such justifications must be detailed and documented and their assessment must be particularly severe because they are in total contradiction with the basic principles of data protection, including transparency and fairness principles. Again, it should be stressed that the controller must do everything possible to avoid having to evade his obligation to inform data subjects. Data controllers acting in the opposite direction would seriously breach their obligations under the GDPR.

Where the data controller intends to further process personal data for a purpose other than that for which the personal data were obtained, he shall first provide the data subject with information about that other purpose and any other relevant information to ensure fair and transparent processing.[16]

3.3 Derogation to the Duration Requirements

As seen previously, compliance with Article 89(1) of the GDPR allows data to be retained for longer periods of time for scientific research purposes. More precisely, the data controller may retain the data for a longer period than is necessary for the purposes for which the data were initially processed, but only insofar as, on the one hand, the data are processed exclusively for the purposes of scientific research in

[15] Recital 62, GDPR.

[16] Article 14.2, GDPR.

accordance with Article 89(1) and, on the other hand, provided that the appropriate technical and organizational measures required by the GDPR are implemented in order to guarantee the rights and freedoms of the data subject.[17]

This implies that data may be stored beyond the time that was necessary to achieve the research (for example, beyond the duration of a specific research project) as long as they are then stored only for use for research purposes.

Compliance with the requirement of appropriate safeguards imposed by Article 89(1) of the GDPR also makes it possible to oppose the claim of a right to oblivion or erasure on the part of the data subject when the processing of data is necessary for the purposes of scientific research insofar as this right is likely to make impossible or seriously jeopardize the achievement of the objectives pursued by the processing of personal data.[18] Similarly, data controller may not seek to oppose this right; they must, as far as possible, make its exercise possible. It is only as a last resort that they may oppose it.

The right to forget or erase is a new feature of the GDPR which allows individuals to require data controllers to delete data relating to them without having to provide justification. Exceptions are provided for, one of which is applicable to scientific research:

> for (…) scientific (…) research purposes (…) purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing.[19]

Data controllers may therefore refuse to grant a request for deletion when processing personal data for scientific research, but this is not a discretionary power: they must be able to prove that such deletion prevents the planned research or seriously compromises it. It is quite unlikely that anonymizing or deleting the data of a single person on a panel would in itself compromise a research project. On the other hand, the repetition of deletion requests from different individuals may eventually weaken the relevance of a dataset. However, it is difficult to know whether researchers could refuse to grant requests for deletion based on a certain amount of data deleted on the basis of the right to delete.

It should be recalled that even where the data controller complies with Article 89(1) of the GDPR, the data subject still has the right to object, for reasons relating to his or her particular situation, to the processing of data relating to him or her for the purposes of scientific research, unless their processing is necessary for the performance of a task in the public interest.[20] There is no derogation to this right to object in the context of research activities, but the person who requests it must give reasons for it, citing reasons relating to his or her particular situation. It is then theoretically possible for researchers to refuse to grant this type of opposition request, but only if the processing they carry out is ‘necessary for the performance

[17] Article 5.1(e), GDPR.

[18] Article 17.3 and recital 65, GDPR.

[19] Article 17.3(d), GDPR.

[20] Article 21.6, GDPR.

of a mission in the public interest', which will probably be uncommon in the case of research activities.

4 Possible Appropriate Safeguards When Processing Personal Data for Scientific Research in the Field of Biobanks

The purpose limitation set forth in Article 5.1(b) of the GDPR requires that collected data should be processed for specified, explicit and legitimate purposes. Purposes for data collection in research and biobanks are predetermined, explicit and legitimate[21] and in accordance with ethical standards.

The principle of proportionality and necessity provides that only what is necessary should be collected upstream and only if it is really necessary to achieve the stated purpose.

Recital 156 explains that:

> The processing of personal data for (…) scientific (…) research purposes (…) should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for (…) scientific (…) research purposes (…) is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for (…) scientific (…) research purposes (…). Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

Insofar as the GDPR relaxes the regime applicable to the processing of personal data for scientific research purposes and also allows Member States to derogate under certain conditions to the data subjects' rights, the appropriate safeguards referred to in Article 89.1 of the GDPR should be understood as measures to compensate for reducing data subjects' protection as a result of relaxing the rules

[21] See recital 33, GDPR.

applicable to the processing of data for scientific research purposes as well as to compensate for the infringement of data subjects' rights.

It should be kept in mind that, in accordance with the principles of data protection by design and by default, the data controller should not seek to evade the general regime, but rather to comply with it as far as possible. Only when this is no longer possible should the implementation of the relaxation of rules and derogations from the rights of the data subject be understood.

It now remains to agree on the notion of appropriate guarantees under Article 89(1) of the GDPR. This one specifies that:

> Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

Therefore, as an example of appropriate safeguards, we can mention the implementation of specific procedures allowing data subjects to exercise their rights with regard to data relating to them which are processed within the scope of the GDPR (such as collective information campaigns instead of individual information), the adoption and implementation of technical and organisational measures to reduce data processing to a minimum (in accordance with the principles of proportionality and necessity) and compliance with the rules on clinical trials, if relevant.

However, it seems impossible to determine the kind of measures that could help securing appropriate safeguards for data subjects' rights and freedoms without first considering performing a data protection impact assessment, whether Article 35 is applicable (when the data processing is likely to result in a high risk to the rights and freedoms of data subjects) or not, knowing that, in the first case, the data controller will have to consult the data protection officer and sometimes the supervisory authority. This data protection impact assessment must provide,[22] a minima:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR rules taking into account the rights and legitimate interests of data subjects and other persons concerned.

[22] For detailed insights in data protection imact assessment see Dara Hallinan 'Biobank Oversight and Sanctions under the General Data Protection Regulation' in this book.

The results of this impact assessment must guide the determination of the measures aiming at securing the protection of data subjects' rights and freedoms, who are concerned by the data processing carried out in biobanks' activities.

A first measure to consider is the way to implement the data minimization principle.

The principle of minimization consists in processing only the data strictly necessary for the purpose. There can be no question of collecting data that would not be directly justified by the purpose of the research. This could be the case for collecting genetic data.

The GDPR acknowledges that research activities may derogate to some extent from the rights of individuals, but the text insists that even in this case, the principle of necessity and minimization must be strictly respected:

> The conditions and guarantees in question may include specific procedures allowing the data subjects to exercise these rights if appropriate having regard to the purposes of the specific processing operation concerned, as well as technical and organisational measures aimed at reducing the processing of personal data to a minimum in accordance with the principles of proportionality and necessity.

This implies that the GDPR allows for derogations from the rights of individuals for scientific research but only on the condition that researchers strictly apply the principle of minimization upstream (collect only what is necessary and only if it is really necessary).

As a rule, the data controller should favor the use of anonymous data. If it is not possible to realize the scientific research with anonymous data, the data controller must use coded or pseudonymized data. '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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Article 4.5 of the GDPR).

In a way, pseudonymised data are those that can be attributed to a natural person by using additional information (in this sense, see recital 26), such as a conversion table.

Clearly, the GDPR encourages researchers to process at least pseudonymised data (see supra Article 89.1 of the GDPR).

Pseudonymisation is favoured by the GDPR as it is likely to reduce the risks for data subjects and to help data controllers and processors to fulfil their data protection obligations. However, the use of pseudonymisation should not be understood as being exclusive of other data protection measures.[23] In other words, pseudonymization does not exempt from compliance with the other obligations imposed by the GDPR, and its implementation does not imply that no further action should be taken.

Recital 29 adds that:

[23] See recital 28, GDPR.

> In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

Pseudonymisation is a security measure promoted by the GDPR, but it should not be confused with anonymisation (the process of making it impossible to identify individuals from the data). Pseudonymized data remain subject to the application of the GDPR, unlike anonymized data, which are excluded.

Anonymization could be a good way to use data secondarily without having to collect new consent. However, in the context of scientific research, it is necessary to be able to identify the person in order to enrich the data with the results of the new research.

Pseudonymization raises several issues: when should it happen (after data collection or before the further processing), who may have access to the pseudonymization keys, what about de-pseudonymization, who should realize the pseudonymization (a trusted third party especially when they are several sources from which the data are collected?), etc.

If it is not possible to use coded or pseudonymized data, the data controller may, to some extent, use non-coded or non-pseudonymized data.

Another measure consists in considering the appointment of a data protection officer knowing that the latter is mandatory where data controller's core activities consist of processing on a large scale of special categories of personal data such as genetic data or data concerning health, by instance.

A third measure to consider consists of adequately fill in the record of processing activities on basis of the data protection impact assessment. By instance, the record should contain the justification to process pseudonymized data or not, the reasons to restrict data subjects' rights when they are likely to render impossible or seriously impair the achievement of the specific purposes, and the impact assessment itself. The information to be provided to data subjects should also be attached to the record.

A fourth measure that could help securing the protection of the data subjects' rights and freedoms regarding the data processing carried out in the framework of biobanks activities consists in studying the way to implement mechanisms that could offer data subjects with a general or individual feedback on the results of the scientific research (by way of information campaigns notably through the medias), taking into account all the circumstances and the result of the data protection impact assessment.

A fifth measure could consist of requiring specific professional accreditation to the persons involved in the processing of personal data for scientific research activities and to the persons in charge of supervising their activities.

A sixth measure could consist in improving procedures for answering data subjects' requests and, considering the scale of the biobank and its impact on data

subjects' rights and freedoms, creating a supervisory body in charge of deliberating on the fundamental options of the biobank functioning.

A seventh measure could consist in confirming the data subject's right to refuse to participate to the research and the right to withdraw at any time without justification.[24]

Finally, certification or even the creation of a specific Code of conduct could help biobanks in uniformizing their practices in the field of data protection, without forgetting to be prepared to be audited by the data protection supervisory authority.

5 Concluding Reflections

The GDPR defines a very broad scope for scientific research. Kart Pormeister[25] considers that the exemptions for the processing of sensitive data for research purposes allow the processing of data without sufficient guarantees since the exemptions refer to national legislation or European Union regulations. This is the case for the important public interest,[26] large population biobanks commonly fall within this framework, and scientific research.[27]

In fact, it seems that the GDPR has confirmed certain practices that previously existed in the field and removed the vagueness that could exist in the eyes of researchers who usually processed health data according to national regulations (very variable between states).

Guidelines were proposed in 2009 by the OECD[28] that set out a number of principles to guide biobanks for genetic research. They collect particularly sensitive samples and data since genetic data are subject to a special regime in some European countries, particularly in France. These recommendations are not binding but serve as a reference in OECD countries (Europe, North America and Asia), which have very different national regulations.

It is interesting to reconcile what these guidelines say about consent and purpose change with the provisions of the GDPR. In that regard, review of addressing the purpose, specification, consent, rules for the secondary use of personal data and the changing of purpose, and data protection are of importance.

First, regarding the purpose it is clear that for the OECD, the purpose of biobanks in human genetics is to stimulate research for the advancement of scientific knowledge, while respecting the fundamental rights and privacy of participants. Operators must comply with documented and transparent procedures. Collective and general

[24] See Article 15.4 of recommendation CM/Rec(2019)2 of the Committee of Ministers on protection of data related to health, adopted on 27 March 2019.

[25] Pormeister (2017), pp. 137–146.

[26] Article 9(2)(g), GDPR.

[27] Art 9(2)(j), GDPR.

[28] OECD 2009 Guidelines for Human Biobanks and Genetic Research Databases.

research results should be published. The purpose of the biobank, both now and in the foreseeable future, must be clearly formulated and communicated.

These goals do not differ from those defined for research in the GDPR.

Second, consent. Free and informed consent is provided for in paragraph 4b. However, if consent cannot be obtained, it is the authorization of the decision-maker, an appropriate substitute, or the exemption granted by an ethics committee or a competent authority in accordance with the legal framework applicable to the research that allows the bank to be implemented.

Consent does not appear to be an essential prerequisite for the establishment of biobanks for the OECD, which gives priority to facilitating research with biobanks, while the rights of the subjects involved are secondary and in accordance with national legislation.

For its part, the GDPR, while laying down the principle of consent as means to process health and genetic data, organizes limited conditions under which the subject's consent is not sought.

Thirdly, the secondary use of personal data and the changing of purpose. Some collections and associated data can be used for large-scale epidemiological or genetic studies of samples and data from different collection modes and locations are consolidated in a new database. Article 3.1 sets out procedures for monitoring the terms of consent. If broad general consent has been given at the time of initial collection, appropriate information mechanisms are proposed. But if the research topics were impossible to predict, the purpose is not specified at the time of collection, and in this case Article 4.6 requires additional safeguards to ensure the protection of participants.

When additional data are associated from personal medical records, Article 5.1 defines access procedures and use. In principle, specific consent is obtained to access the medical file compiled outside the collection, unless an exemption is given by an ethics committee or a competent authority.

It is clear that the OECD greatly facilitates secondary use and exchanges through its guidelines, just as the GDPR goes very far in recognizing secondary use, in all circumstances, as a compatible lawful processing.

Finally, data protection. Article 6.1 designates a data protection and privacy officer. Specific provisions are provided for the possibility of withholding certain data that would make secondary identification possible (Article 6.3) or the separation of data allowing direct identification of a subject from other data, in particular genotypic data.

Appropriate measures for the protection of privacy and confidentiality are proposed in Article 6.5: secure storage, data encryption or encryption, sample and data access logs, infrastructure to prevent unauthorized access.

Access to the bank must be in accordance with the consent given, requests must be accompanied by a scientifically and ethically appropriate research plan (Article 7B) Third party access for purposes other than research is prohibited (Article 7F). An agreement organizes access, users sign confidentiality (Article 7.5) or transfer (Article 7.6) agreements.

Article 14 of the GDPR provides for the information to be given where the data have not been obtained from the data subject: it concerns the possibility of secondary use and the possible transfer of data. This information is likely to enable the person, at the time of obtaining initial consent, to object to subsequent use or transfer. Clear and fair advance information should be provided.

The transfer of data is authorised by Article 46 of the GDPR with appropriate safeguards, including binding corporate rules,[29] an approved code of conduct[30] or a certification mechanism.[31]

References

2009 Guidelines for Human Biobanks and Genetic Research Databases
Article 29 Data Protection Working Party. Guidelines on consent under Regulation 2016/679. WP 259 rev.01
Article 29 Data Protection Working Party. Guidelines on Data Protection Officers ('DPOs'). WP 243 rev.01
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 rev.01
Article 29 Data Protection Working Party. Guidelines on the right to data portability. 13 December 2016 & revised on 5 April 2017. WP 242 rev.01
Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679. 29 November 2017 & revised on 11 April 2018. WP 260 rev.01
Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. WP 203
Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. WP 216
Article 29 Data Protection Working Party. Opinion 10/2004 on More Harmonised Information Provisions. WP 100
Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent. WP 187
Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. WP 136
Council of Europe Recommendation CM/Rec (2019) 2 of the Committee of Ministers on protection of data related to health, adopted on 27 March 2019
de Terwangne C, Degrave E, Dusollier S, Queck R (dir.) (2018) Law, norms and freedoms in cyberspace. Droit, normes et libertés dans le cybermonde. Liber Amicorum Yves Poullet. Larcier, Bruxelles. Collection du CRIDS
Herveg J (2018a) Data protection and Biobanks in 2018. Eur J Health Law:515–536
Herveg J (2018b) Réflexions autour de la protection des données et des vulnérabilités. In: Jacquemin H, Nihoul M (coord.) Vulnérabilités et droits dans l'environnement numérique. Larcier, Buxelles. Collection de la Faculté de droit de l'UNamur, pp 333–392
Herveg J, Van Gyseghem JM (2018) L'impact du Règlement général sur la protection des données dans le secteur de la santé. In: Rosier K, de Terwangne C (coord.) Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie. Larcier, Bruxelles. Collection du CRIDS, pp 703–762
Modernised Convention for the protection of individuals with regard to automatic processing of personal data (Treaty n° 108+)
Pormeister K (2017) Genetic data and the research exemption: is the GDPR going too far? Int Data Priv Law 7(2):pp. 137–146

[29] Article 47, GDPR.

[30] Article 40, GDPR.

[31] Article 42, GDPR.