The EU General Data Protection Regulation

Answers to Frequently Asked Questions

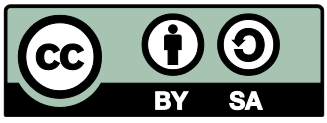
Updated Version 2.0

Prepared by the BBMRI-ERIC Common Service ELSI

March 1, 2017

CONTENTS

We encourage translations of this document. In case of questions, please get in touch with us through the BBMRI-ERIC ELSI Helpdesk: elsi@helpdesk.bbmri-eric.eu.



INTRODUCTION

On May 24, 2016, the Regulation of the European Parliament and of the Council 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 (the General Data Protection Regulation, also referred to as the "GDPR" or as the "Regulation") entered into force. The Regulation shall be binding in its entirety and directly applicable in all Member States from May 25, 2018.

The following is an update of answers to Frequently Asked Questions (FAQs) about how the EU General Data Protection Regulation is expected to apply to biobanks, collections of human samples and associated health data, in the EU. The FAQs do not constitute legal advice and may be subject to change, as a result of further analysis or when provisions of the GDPR are being implemented. In applying the GDPR, overlapping obligations contained in other national and European legislation such as EU Clinical Trial Regulation 536/2014 should also be taken into account.

This FAQ expands on the version that was published by the BBMRI-ERIC Common Service ELSI Task Force on the EU General Data Protection Regulation in 2016. The following Task Force members contributed to the FAQ: Jasper Bovenberg, Martin Boeckhout, Gauthier Chassang, Victoria Chico, Michaela Th. Mayrhofer, Irene Schlünder, and Olga Tzortzatou.

WHAT IS THE GENERAL DATA PROTECTION REGULATION (GDPR)?

The EU General Data Protection Regulation is the novel, EU-wide legal framework for the protection of personal data. The objectives of the Regulation are to protect individuals' rights and freedoms in relation to the processing of their personal data, while also facilitating the free flow of such data within the Union. It provides that the free movement of personal data within the European Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. The Regulation (the Position of the Council at first reading) can be downloaded in different languages. The official text of the Regulation was published in the Official Journal of the European Union in all official languages on May 4, 2016 and can be downloaded here.

HOW AND WHEN DOES THE REGULATION APPLY?

The Regulation, which was adopted in April 2016, will be binding in its entirety and directly applicable in all Member States as from May 25, 2018. It will repeal the Data Protection Directive (95/46/EC) and will override national data protection legislation based on that Directive. However, the Regulation also provides space for national and EU-level derogations and specifications in some areas, including the use of personal data in scientific research.

DOES THE GDPR AFFECT BIOBANKING?

Yes, because biobanks collect, store and/or process human biological material, in combination with other forms of personal data, including sensitive data, such as genetic and health data.

DOES THE GDPR AFFECT THE TRANSFER OF DATA BETWEEN BIOBANKS WITHIN THE EU?

The GDPR provides that the free movement of personal data within the European Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. The GDPR allows Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

WHAT IS NEW IN THE GDPR?

Key changes to the existing EU Data Protection Directive include:

- Transparency and accountability are now main principles of data protection
- Special provisions for scientific research
- Enhanced rights for data subjects, such as the right to be forgotten and the right to data portability
- Mandatory procedures for managing data breaches
- Special provisions for protecting data of minors
- Mandatory Data Protection Impact Assessments
- Mandatory appointment of a Data Protection Officer (subject to exceptions)
- Pan-European validation of European Codes of Conduct for non-profit organisations
- Certification mechanisms specifically for data protection
- Remedies, sanctions and fines.

WHAT ARE THE MAIN ELEMENTS OF THE GDPR?

The GDPR contains a number of principles relating to the processing of personal data, the rights of data subjects, and the obligations of data controllers and processors.

The main principle is that personal data need to be processed 'lawfully, fairly and in a transparent manner in relation to the data subject'. For scientific research and biobanking, this will principally require informed consent from individuals whose data are processed, unless the law provides an alternative legal basis for the processing of personal data (i.e. specific permission provided by law). In addition, principles of data minimisation and storage limitation are particularly important to biobanking research.

Data subjects (i.e. patients and participants contributing their data or samples for research) have a number of rights as against the controller(s) and processor(s) of their data. They include the right to consent, to information, to access, to rectification, to erasure (aka 'the right to be forgotten'), to restrict processing, to data portability and to object. A number of these rights may be subject to limitations in the context of scientific research in certain cases.

Obligations of data controllers and processors include the obligation to establish clear and transparent procedures for data protection, security and confidentiality, as well as accountability and demonstration of compliance. Scientific research may enjoy exceptions to some obligations.

DOES THE GDPR CONTAIN EXCEPTIONS FOR BIOBANKS?

Biobanks could be exempted from a number of the GDPR's general principles, obligations and data subject rights, as, if and when processing personal data for the purpose of scientific research purposes. For example, the data storage limitation principle can be modified and personal data can be stored for longer periods provided that they will be processed solely for scientific research purposes in accordance with the provisions of article 89(1) of the GDPR and subject to implementation of technical and organisational measures required by the GDPR. Also, the GDPR retains the presumption of compatibility of use for research purposes, thereby enabling further data processing for scientific research purposes of personal data initially processed for a different purpose, provided that there is a valid legal ground for the initial processing in EU or Member States law exists.

The GDPR also allows for exemptions to various data subjects' rights in so far as the exercise of these rights is likely to render impossible or seriously impair the achievement of the research and such derogations are necessary to the fulfilment of these purposes. A number of these exemptions may directly apply on a case-by-case basis, while others will have to be provided by Union or Member States law. All exemptions are subject to the existence of appropriate technical and organisational measures ensuring in particular the respect of data minimisation principle (including for example pseudonymisation or anonymisation techniques), as mentioned in article 89. For more examples, see the answers relating to the various principles, obligations and rights under the Regulation.

WHAT IS THE RELATIONSHIP BETWEEN DATA PROTECTION AND PRIVACY?

Data protection is the legal terminology central to the Regulation. Privacy encompasses personal data protection but also comprises individuals' rights to private and family life and respect for the confidentiality of their correspondence and communications.

WHAT IS THE RELATIONSHIP BETWEEN DATA PROTECTION AND DATA SECURITY?

Data security is an element in safeguarding the rights and fulfilling the obligations set out in data protection law. More roughly put: data security is a necessary (though not in and of itself sufficient) means to achieve the ends of data protection. Security measures may serve other purposes unrelated to personal data protection as well, such as protecting commercial interests.

WHAT IS ANONYMISED/ANONYMOUS DATA?

The GDPR only applies to personal data, not to anonymised/anonymous (i.e. non-personal) data. The Regulation does not distinguish between anonymous and anonymised data.

Anonymised/anonymous data is defined in opposition to personal data as '*information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.*

Anonymity is not a static term, but dependent on context knowledge and 'all the means reasonably likely to be used' to re-identify the individual behind a data record. Whether data qualifies as anonymous has to be established on a case-by-case basis, requiring risk assessment. 'Objective factors' (such as the costs and the amount of time required for identification, the available technology at the time of processing and technological developments) need to be considered when deciding whether this standard is met in practice.

HOW IS ANONYMISATION ACHIEVED?

There are multiple methods, techniques and strategies to anonymise personal data. The GDPR does not favour a certain method.

In substance, the Regulation did not change the definition of personal and anonymous data. Therefore, methods meeting the standards of the 1995 Data Protection Directive should still hold in the legal sense, although these should always be assessed against the background of constant technical developments. There are many technical methods that can be used, such as deletion, redaction or generalisation, perturbation or dissociation of identifying information. Notably, the Opinion of the Article 29 Working Party on Anonymisation remains relevant under the GDPR.

IS ANONYMISATION REQUIRED IN SCIENTIFIC RESEARCH?

The principle of data minimisation is a requirement under the GDPR. This means that data have to be de-identified to the extent that research objectives can be achieved. However, anonymisation will not always be required. Other means such as pseudonymisation should also be considered. Future research purposes as well as the rights of individuals participating in research should be taken into account as well. Anonymisation makes it impossible to further communicate with the individual behind a data record, for example in order to feedback research results or to ask for follow-up information. In addition, it deprives him or her of the right to withdraw consent.

WHAT IS PSEUDONYMISATION OF DATA?

The GDPR defines pseudonymisation as '*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*.'

WHAT'S THE DIFFERENCE BETWEEN PSEUDONYMISATION AND ANONYMISATION?

With pseudonymisation, attributing data to individuals remains possible using 'additional information' (e.g. a key or encryption code). For anonymised data, such information is not or no longer available. Pseudonymised data is still considered personal data in principle, whereas anonymised/anonymous data is not.

DOES THE REGULATION REQUIRE PSEUDONYMISATION IN SCIENTIFIC RESEARCH?

Pseudonymisation is promoted in the Regulation as one of the main methods to reduce the risks associated with processing personal data to 'help controllers and processors to meet their data-protection obligations'. However, other safeguards (such as encryption) will need to be considered and implemented as well (recital 28). At the same time, pseudonymisation is not required if it prevents pursuing particular scientific research purposes (according to article 89.1).

WHAT IS CONSENT?

The GDPR defines 'consent' of the data subject as meaning 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent is one way to meet the GDPR requirement that processing of personal data must be lawful.

The GDPR specifies the conditions under which data subjects can validly consent to the processing of their personal data.

HOW SHOULD CONSENT BE OBTAINED FROM DATA SUBJECTS?

Where processing is based on consent:

- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters.
- Consent must be requested in an intelligible and easily accessible form, using clear and plain language.
- Consent must be freely given.
- Consent must be informed, as specified in the GDPR (see FAQs on rights to information).
- Consent must be provided by a clear and affirmative action (silence, pre-ticked boxes or inactivity are not considered valid forms of consent under the GDPR).
- Consent can be provided in writing, by electronic means, as well as orally.

- Consent must represent the specific, informed and unambiguous indication of the data subject's agreement to data processing.
- The controller must be able to demonstrate that consent was lawfully provided, also if consent was provided orally.
- National laws can maintain or introduce further conditions regarding data subjects' consent in specific contexts, for instance with regard to the processing of genetic data.

CAN BIOBANKS USE 'BROAD CONSENT' UNDER THE REGULATION?

The Regulation acknowledges that the purposes of scientific research cannot always be specified at the time of the initial data collection. It therefore allows biobanks to ask individuals for 'consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research'. However, the Regulation also states that '[d]ata subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose' (recital 33).

DO BIOBANKS NEED CONSENT TO PROCESS SENSITIVE DATA?

The GDPR provides that processing of sensitive personal data (such as genetic data or health data) shall be prohibited. However, the Regulation provides for a number of exceptions to this prohibition. One such exception is this prohibition if the data subject has given explicit consent. Consent is not the only exception, however. The prohibition does not apply either when the processing is necessary for scientific research purposes in accordance with Article 89(1) based on Union or Member State law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

WHAT ARE THE SPECIFIC PROVISIONS FOR CONSENT IN THE CASE OF CHILDREN?

Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. In relation to the offer of information society services directly to a child, Unless Member State Law specifies a lower age, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

ARE THERE SPECIFIC PROVISIONS REGARDING THE PROCESSING OF DATA OF DECEASED PERSONS?

The Regulation does not apply to the personal data of deceased persons. However, this may be regulated in national law, for instance in law relating to professional secrecy. Moreover, one should keep in mind that constitutional and human rights considerations may be relevant in this regard.

DOES THE GDPR ALSO RULE ON PROFESSIONAL SECRECY?

Professional secrecy law (for health professionals such as doctors, nurses, etc.) may provide additional provisions to be respected next to data protection law (e.g. article 9.2i). The Regulation does not affect obligations of professional secrecy. Wherever applicable, both professional secrecy as well as data protection law need to be respected.

WILL CONSENT OBTAINED UNDER THE CURRENT DIRECTIVE REMAIN VALID UNDER THE NEW REGULATION?

Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation before this Regulation applies, that is, by mid 2018. It is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation.

WHAT ARE THE OBLIGATIONS TO PROVIDE INFORMATION TO DATA SUBJECTS?

Different obligations are involved depending on the situation: whether data is collected from the data subject (article 13); whether data is collected from third parties (article 14); as well as whether data subjects invoke their right to access (article 15).

Under the Regulation, biobanks collecting personal data about their participants must provide their participants with extensive information about how and what data is processed. Obligations to provide data subjects with information about data processing already existed under previous data protection legislation. The GDPR expands on such obligations.

The obligation to provide information may not apply in certain cases:

- when the participant already has the information;
- where the recording or disclosure of the personal data is expressly laid down by law;
- If the personal data have been obtained from a third party: where the provision of information to the data subject proves to be impossible or would involve disproportionate effort. In that regard any appropriate safeguards adopted should be taken into consideration.

WHAT INFORMATION SHOULD BE PROVIDED TO DATA SUBJECTS IF DATA ARE COLLECTED FROM THE DATA SUBJECT?

As specified in article 13, biobanks must provide their participants the following information at the time data is obtained *and* when information is updated (subject to general principles of fair and transparent processing):

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the recipients or categories of recipients of the personal data, if any;
- 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, as the case may be, reference to the appropriate or suitable safeguards and the means by which their participants can obtain to obtain a copy of these safeguards or where these safeguards have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where biobanks process personal information on the basis of, inter alia, consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right of participants to lodge a complaint with a supervisory authority;
- information on any processing of the personal data for a purpose other than that for which the personal data were collected and any relevant further information as referred to above.

WHAT INFORMATION SHOULD BE PROVIDED TO DATA SUBJECTS IF DATA ARE NOT COLLECTED FROM THE DATA SUBJECT?

As specified in article 14, biobanks must provide their participants with the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

- the recipients or categories of recipients of the personal data, if any;
- 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, as the case may be, reference to the appropriate or suitable safeguards and the means by which their participants can obtain to obtain a copy of these safeguards or where these safeguards have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where biobanks process personal information on the basis of, inter alia, consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right of participants to lodge a complaint with a supervisory authority;
- where the processing is based on legitimate interests instead of on consent (for instance in some cases of residual or secondary use of data), the legitimate interests pursued by the controller or by a third party;
- if data were collected through third parties: from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

WHAT INFORMATION SHOULD BE PROVIDED TO DATA SUBJECTS IF DATA SUBJECTS INVOKE THEIR RIGHT TO ACCESS?

As specified in article 15, when data subjects invoke their right to access their data, biobanks must provide participants confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;

- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
- The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. This right to obtain a copy shall not adversely affect the rights and freedoms of others.

Note that Member States can provide derogations to this right in national law.

HOW SHOULD INFORMATION BE PROVIDED TO DATA SUBJECTS?

Pursuant to Article 12 and according the principle of transparency, any information addressed to the data subject or to the public, must be provided 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and additionally, where appropriate, visualization must be used. In particular for any information addressed to a child any information and communication should be in such a clear and plain language that the child can easily understand. Every single data subject should be provided the information. Information must be provided in writing and/or by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The information may be provided in combination with standardized icons in order to give an easily visible and meaningful overview of the intended processing.

WHEN SHOULD INFORMATION BE PROVIDED TO DATA SUBJECTS?

When data are collected from the data subject, the information must be given at the time when the personal data is obtained, as well as when information is updated, subject to general principles of fair and transparent processing. When data are collected through third parties and/or used for secondary purposes, information must be provided (article 14.3):

- 'within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed';
- 'if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject';
- 'if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.'

WHAT EXEMPTIONS TO RIGHTS TO INFORMATION MAY APPLY?

Generally, the obligation to provide information does not apply where and insofar as the data subject already has information about processing. In the event the personal data have not been obtained from the data subject (but from a third party source), the obligations to provide individuals with information can be exempted if:

- if the provision of such information proves impossible,
- if the provision of such information would involve a disproportionate effort, and/or
- if the obligation is likely to render impossible or seriously impair achieving the (research) objectives of the processing of personal data.

If a biobank wants to invoke either of these exceptions, it will have to establish that these requirements are met. Moreover, invoking these exceptions is subject to appropriate conditions and safeguards under article 89, such as technical and organisational measures, including pseudonymisation, as well as measures to protect data subjects' rights and freedoms and legitimate interests. At the very least, these measures include making the information publicly available – for instance, through the biobank's website.

These exceptions may usually not be successfully invoked by biobanks which regularly communicate with their participants. For other forms of research, such as residual use tissue banks and patient registries, these clauses may provide some leeway towards operating on the basis of an opt-out system. However, whether this is so will strongly depend on both the specifics of the infrastructure, the research involved, as well as national legislation.

Finally, the obligation to provide information may not apply, where personal data obtained from a third party source is also subject to an obligation of professional secrecy, such as doctors.

ARE THERE ANY NEW RIGHTS FOR DATA SUBJECTS?

Yes. New rights include the right to be forgotten, which amends the existing right to erasure, and the right to data portability'. In addition, a number of existing rights have been specified. These include the right to information, the right to rectification, the right to restriction of processing, the right to object to processing of personal data, and the right not to be subject to legal measures based solely on automated profiling. The GDPR also recognises the need for children as data subjects to be specifically protected regarding the processing of their personal data and provides for an enhanced specification of consent, in particular regarding consent to the processing of sensitive personal data (such as health, genetic, or biometric data). More transparent information and communication about the purposes and forms of data processing, must also be provided when data are processed by third parties.

WILL ALL DATA SUBJECTS' RIGHTS APPLY TO BIOBANKS?

According to article 89, Union or Member State law may provide for derogations from a number of data subject rights, including the rights to access, to rectification, to restriction of processing and to object to processing of personal data, when personal data are processed for scientific research purposes. These further derogations are subject to technical and organizational measures (e.g. pseudonymisation) which need to be in place in particular in order to ensure respect for the principle of data minimisation.

These derogations are only available in so far as the exercise of these rights is likely to render impossible or to seriously impair the achievement of the objectives of that processing. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes have to be fulfilled in that manner.

WILL THE NEW 'RIGHT TO BE FORGOTTEN' APPLY TO BIOBANKS?

The right 'to be forgotten' shall not apply to the extent that the processing of personal data is necessary for scientific research purposes or statistical purposes in accordance with Article 89(1), in so far as it is likely to render impossible or seriously impair the achievement of the objectives of that processing.

WHAT ABOUT THE NEW 'RIGHT TO DATA PORTABILITY'?

The GDPR introduces a 'right to data portability', i.e. the right for a data subject to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The data subject also has the right to have his or her personal data transmitted directly from one controller to another controller. This right applies where either the processing is based on consent or on a contract and the processing is carried out by automated means. Notably, the right to data portability is not part of the list of data subject rights which can be derogated from by the Member States under Article 89(2).

"Inferred data" and "derived data" such as data resulting from genetic sequencing of samples could be exempt from this obligation, as suggested by a (non-binding, draft) guideline drawn up by the EU Article 29 Working Party. Further specifications of the reach of the law in this regard remain to be established.

MUST BIOBANKS APPOINT A DATA PROTECTION OFFICER?

Since the core activities of Biobanks consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, a Data Protection Officer must be delegated by the Biobank controller or the processor/s in order to assist them monitor internal compliance with this Regulation. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

Organisations with less than 250 employees are exempt from this obligation under the Regulation. Note, however, that it is the number of employees of the organisation of which the biobank forms part which counts towards the total number of employees. For instance, this may be an academic hospital or university of which the biobank is a part.

WHAT DOES THE PRINCIPLE OF ACCOUNTABILITY MEAN IN THE GDPR?

The principle of accountability refers to the responsibility of the data controller to ensure that the fundamental principles relating to processing of personal data are respected, as well as the ability to demonstrate compliance.

WHAT DOES THE PRINCIPLE OF TRANSPARENCY MEAN IN THE GDPR?

Transparency is one of the core principles in the GDPR. It requires in particular that data subjects must be informed about whether, how and by whom data relating to them is processed, as well as a 'right to obtain confirmation and communication of personal data concerning them which are being processed' (recital 39), 'taking into account the specific circumstances and context in which the personal data are processed' (recital 60).

WHAT DOES THE REGULATION SAY ABOUT DATA BREACHES?

According to the GDPR, a personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

As soon as the controller becomes aware that a personal data breach has occurred, the controller must notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

The controller should also communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions.

MUST BIOBANKS DO A DATA PROTECTION IMPACT ASSESSMENT?

Most probably yes, assuming they engage in a type of processing of personal data, in particular using new technologies, which, 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, e.g. when they are processing on a large scale special categories of data, such as health data and genetic data. The supervisory authority in a Member State shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment; please refer to your supervisory authority to check whether it has so listed your type of processing. Also, the supervisory authority may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. Chances that processing by biobanks of sensitive data will be listed on this negative list, are slim but please refer to your supervisory authority. A single assessment may address a set of similar processing operations that present similar high risks.

WILL THE GDPR APPLY IN THE UNITED KINGDOM FOLLOWING BREXIT?

Generally, to provide legal certainty in the UK after exit from the EU, The United Kingdom's exit from and new partnership with the European Union White Paper states that the Government introduce the Great Repeal Bill to remove the European Communities Act 1972 from the statute book and convert the

body of existing EU law into domestic law. This means that, where practical and appropriate, the same rules and laws will apply on the day after the UK leaves the EU as they did before.

The UK will still be a member of the European Union on May 25, 2018, thus the GDPR will automatically become binding in the UK on that date. On Wednesday 1st February the EU Home Affairs Sub-Committee took evidence from Rt Hon Matt Hancock MP, Minister of State for Digital and Culture, Department for Culture, Media and Sport on the EU General Data Protection Regulation. He stated that the British government will fully implement the GDPR for two key reasons:

- "Thanks to some significant negotiating successes during its development we think that it is a good piece of legislation in and of itself,"
- "We are keen to secure the unhindered flow of data between the UK and the EU post-Brexit, and we think that signing up to the GDPR data protection rules is an important part of helping to deliver that."

Even if the UK does fully implement the GDPR post-Brexit, it would become a so-called third country. At that point, the free flow of data between the UK and the EU would be dependent upon arrangements similar to those currently in place to enable data flows to other third countries. outside the EU. One option would be for the UK to apply for an 'adequacy decision' (see further on).

HOW CAN PERSONAL DATA BE TRANSFERRED OUTSIDE THE EU?

Personal data may be transferred to a third country where the Commission has decided that the third country, or one or more specified sectors within that third country, ensures an adequate level of protection. The effect of such an 'adequacy decision' is that personal data can flow from the EU to that third country or sector without further safeguards. Such a transfer shall not require any specific authorization.

In the absence of an adequacy decision of the Commission, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards may be provided for by standard data protection clauses adopted by the Commission. They could also be provided for by an approved code of conduct or certification mechanism, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In the absence of an adequacy decision or of appropriate safeguards, a transfer or a set of transfers of personal data to a third country may take place on the condition that the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

CAN BIOBANKS CONTINUE TO TRANSFER PERSONAL DATA TO THE UNITED STATES OF AMERICA?

Yes, subject to the general transfer provisions to transferring data outside the EU discussed in the question above. Transfers under the Safe Harbour principles are no longer valid. New specific rules (the EU-US Privacy Shield) are still under negotiation.

CAN BIOBANKS TRANSFER PERSONAL DATA TO THE UNITED STATES OF AMERICA BASED ON THE EU-US PRIVACY SHIELD?

Only if the receiving organisation is listed under the Privacy Shield Framework and the data fall within the covered data of the listing.

On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers from the EU to the USA under EU law (the Privacy Shield replacing previous EU-US Safe Harbour agreements).

Personal data are transferred under the EU-U.S Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the 'Privacy Shield List', maintained and made publicly available by the U.S. Department of Commerce. Transfer of personal data to such an organisation would then qualify as a valid transfer under the Regulation. Any U.S. organisation that is subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT) may participate in the Privacy Shield. Generally, the FTC's jurisdiction covers acts or practices in or affecting commerce. For all practical purposes, academic and not for profit research organisations are unlikely to be eligible for listing under the Privacy Shield Framework and hence biobanks cannot ground any transfer of personal data to such organisations based on the Privacy Shield. This may be different for commercial institutions, provided of course, they are listed and the data to be transferred is covered by the listing; e.g. 23andMe. The Privacy Shield list can be found here.

CAN BIOBANKS TRANSFER PERSONAL DATA TO THE UNITED STATES OF AMERICA BASED ON THE SWISS-US PRIVACY SHIELD?

Regarding Switzerland (non-EU member State), in January 2017, the Federal Council states that a new framework, Privacy Shield, has been established for the transfer of personal data from Switzerland to the USA. With the introduction of Privacy Shield, the same standards apply for Swiss exports of personal data to the USA as for data exports from the EU. The Federal Data Protection and Information Commissioner (FDPIC), as the other supervisory authorities in EU Member States will act as a point of contact for persons in Switzerland in the event of any problems in connection with the transfer of data to the USA.

Regarding the transfer of personal sensitive data (as defined in Article 9(1), including e.g. health, genetic/genomic, biometric data) for research purposes, although it is not obligatory under the GDPR, it is recommended to use additional contractual measures intended to specifically frame the activities in terms of purposes, methodologies, confidential data management and data subjects' rights protection. Such a contract can take the form of a Data Transfer Agreement or a Material Transfer Agreement.

HOW WILL THE REGULATION BE ENFORCED?

The Regulation provides for three types of mechanisms to enforce its provisions: corrective measures, fines and penalties.

Each supervisory authority shall have a set of corrective measures, which include issuing warnings or reprimands, imposing a limitation or even a ban on processing, ordering the rectification or erasure of personal data, and imposing an administrative fine to the controller or the processor.

Infringement of the basic principles for processing, including conditions for consent, but also infringements of the data subjects' rights the transfers of personal data to a recipient in a third country or an international organization, can be subject to administrative fines of up to €20.000.000.

Member States shall lay down the rules on other penalties applicable to infringements of this Regulation, in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented.

Photo: eliasfreiberger.at

BBMRI-ERIC®
gateway for health