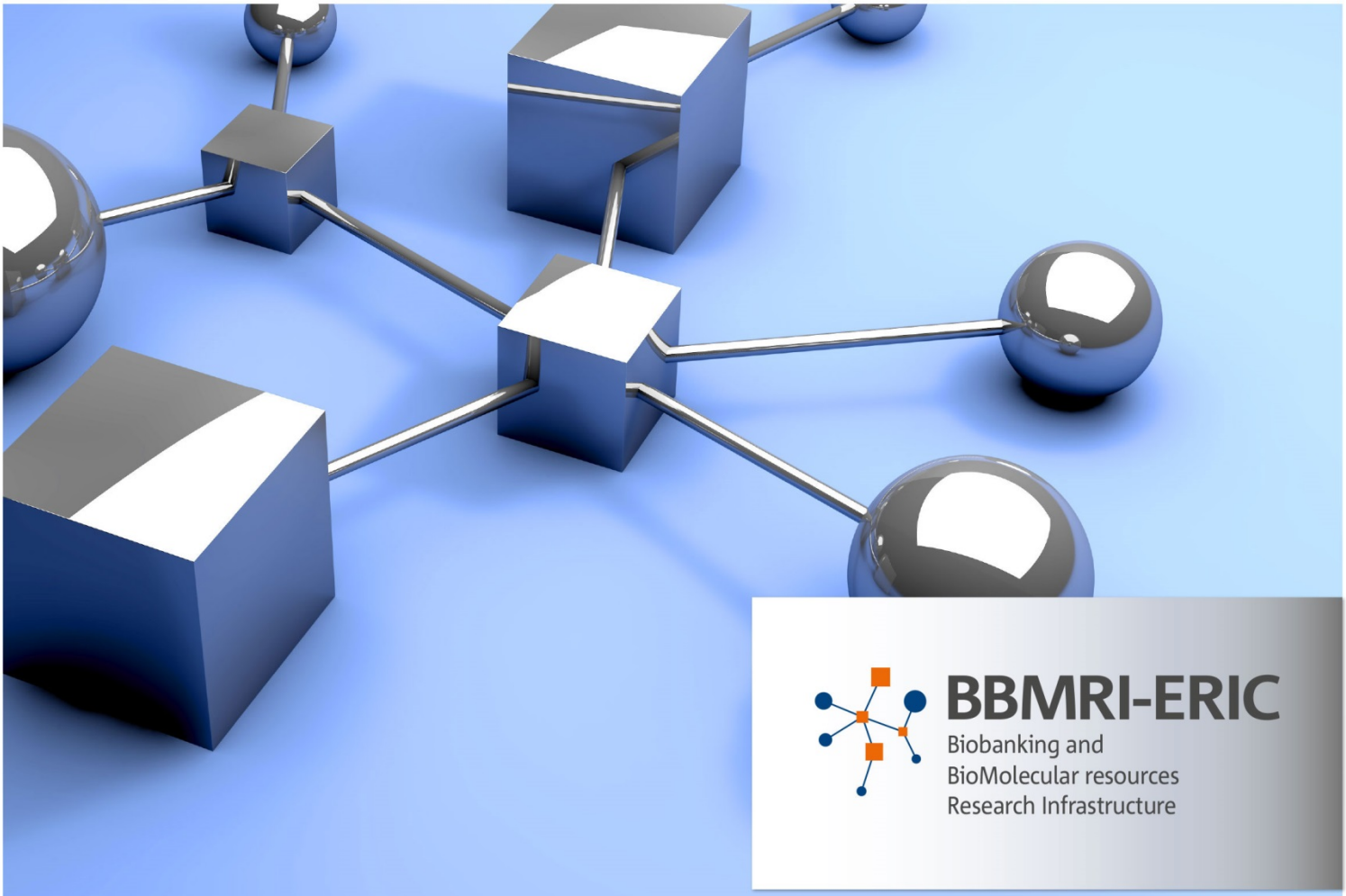

BBMRI-ERIC
Biobanking and
BioMolecular resources
Research Infrastructure

The EU General Data Protection Regulation

Answers to Frequently Asked Questions 1.0

Prepared by the BBMRI Common Service ELSI

May 1, 2016

CONTENTS

Introduction 3
What is the General Data Protection Regulation (GDPR)? 3
How and when does the Regulation apply? 3
Does the GDPR affect biobanking? 3
Does the GDPR affect the transfer of data between biobanks within the EU? 4
What is new in the GDPR? 4
What are the main elements of the GDPR? 4
Does the GDPR contain exceptions for biobanks? 5
What is anonymised/anonymous data? 5
How is anonymisation achieved? 5
Is anonymisation required in scientific research? 6
What is pseudonymisation of data? 6
What's the difference between pseudonymisation and anonymisation? 6
Does the Regulation require pseudonymisation in scientific research? 6
What are the requirements for consent? 6
Can biobanks use 'broad consent' under the Regulation? 7
Do biobanks need consent to process sensitive data? 7
What are the specific povisions for consent in the case of children? 7
Will consent obtained under the current Directive remain valid under the new Regulation? 7
Are there any new rights for data subjects? 7
Will data subject rights apply to biobanks? 8
Will the new 'Right To Be Forgotten' apply to Biobanks? 8
What about the new 'Right to Data Portability? 8
Must Biobanks appoint a Data Protection Officer? 8
What does the Regulation say about data breaches? 9
Must Biobanks do a Data Protection Impact Assessment? 9
How can personal data be transferred outside the EU? 9
Can Biobanks continue to transfer personal data to the United States? 10
How will the Regulation be enforced? 10

INTRODUCTION

On April 14, 2016, the European Parliament adopted 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").

Following is a first set 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. This set of FAQs has been prepared by the BBMRI ERIC Common Services ELSI Task Force on the EU General Data Protection Regulation, in Graz, April 2015 and was finalized on May 1, 2016. The current members of the Task Force are Jasper Bovenberg, Martin Boeckhout, Gauthier Chassang, Irene Schlünder, Olga Tzortzatou and Ruth Vella Falzon.

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 here. The official text was published in the Official Journal of the European Union in all official languages on May 4, 2016.

HOW AND WHEN DOES THE REGULATION APPLY?

The Regulation will be directly applicable in the entire European Union and will override national data protection legislation. However, the Regulation also provides space for national and EU-level specification in some areas, including scientific research. The Regulation, which was adopted in April 2016, replaces the Data Protection Directive (95/46/EC). The GDRP will become applicable as from May 25, 2018.

DOES THE GDPR AFFECT BIOBANKING?

Yes, to the extent 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 sets forth 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 grants another legal basis (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 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, as a modification of the data storage limitation principle, 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 a valid legal ground for such initial processing in EU or Member States law exists.

The GDPR furthermore 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 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 as opposed 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 data has to be established on a case-by-case basis, requiring a risk assessment. 'Objective factors' (such as the costs of and the amount of time required for identification, the available technology at the time of the 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 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, but should always be assessed against the background of constant technical developments. There are many technical methods, that can be used, such as deletion or generalization, perturbation or disassociation of identifying information. Notably, the Opinion of the Article 29 Working Party on Anonynimisation 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.

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 ARE THE REQUIREMENTS FOR CONSENT?

Consent for research in the sphere of biobanking for health research should be freely given in a clear, affirmative act, informed, unambiguous, explicitly cover the processing of health data for purposes of research, and be provided for 'one or more specified purposes'.

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 recognised ethical standards for scientific research'.

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. This prohibition, however, shall not apply, inter alia, in the event the data subject has given explicit consent or 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 POVISIONS 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. 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.

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.

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 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 DATA SUBJECT 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 introcudes 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, This right applies where either the processing is based on consent or on a contract. 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).

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 REGULATION SAY ABOUT DATA BREACHES?

According 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?

Yes. A single assessment may address a set of similar processing operations that present similar high risks.

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. Such a transfer shall not require any specific authorization (referred to as an 'adequacy decision').

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?

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.

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 a.o. 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.