Beyond One Million Genomes

D2.3

Report on legal set-up including DPIA

Project Title (grant agreement No)	Beyond One Million Genomes (B1MG) Grant Agreement 951724		
Project Acronym	B1MG		
WP No & Title	WP2 - ELSI		
WP Leaders	Regina Becker (UNILU), Jasper Bovenberg (Legal Pathways)		
Deliverable Lead Beneficiary	14 - Legal Pathways		
Deliverable	D2.3 - Report on legal set-up including DPIA		
Contractual delivery date	31/05/2023	**Actual delivery date**	05/10/2023
Delayed	Yes		
Authors	Part 1: Jasper Bovenberg Part 2: Dr. Olga Tzortzatou, Marina Makri, Alexandra Ziaka Part 3: Jasper Bovenberg		
Contributors	Part 1: Alison Hall, Ragnhild Agnell Holst, Manolis Nymark, Susanne Rebers, Olda Bakken. Part 2: Part 2: Prof. Mette Hartlev, Dr. Tom Southerington, Christine Dalebø Gjerdevik, Prof. Jane Reichel, Dr. Olga Tzortzatou, Prof. Marialuisa Lavitrano, Dr. Matteo Macilotti, Dr. Ruth Vella Falzon, Prof. Carla Barbosa, Prof. Aliuska Duardo, Dr. Susanne Rebers, Teodora Lalova, Gauthier Chassang, Dr. Fruzsina Molnár-Gábor, Dorota Krekora-Zajac, Radek Halouzka, Jan Kuráň, Santa Slokenberga, Signe Mežinska, Silja Elunurm, Regina Becker Part 3: Alison Hall, Ragnhild Agnell Holst, Manolis Nymark, Susanne Rebers, Olda Bakken.		
Acknowledgements (not grant participants)	Part 1 and Part 3 : Szymon Bielecki (Secretariat of the 1+Million Genomes Initiative, DG CONNECT), Owe Langfeldt (DG Santé).		

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Deliverable type	Report
Dissemination level	Public

Document History

Date	Mvm	Who	Description
17/03/2022	Ov1	Dr. Olga Tzortzatou, Marina Makri, Alexandra Ziaka.	Initial draft sent to WP leader- Regina Becker.
31/03/2022	Ov2	Dr. Olga Tzortzatou, Marina Makri, Alexandra Ziaka.	Draft circulated to national experts for feedback.
04/05/2022	Ov3	Dr. Olga Tzortzatou, Marina Makri, Alexandra Ziaka.	National experts' comments addressed. Draft circulated to WP participants for feedback.
25/11/2022	0v1	Dr. Jasper Bovenberg	Initial draft sent to WP Leader - Regina Becker Draft to be circulated to national experts and WP participants for feedback.
09/02/2023	0v2	Dr. Jasper Bovenberg	Second draft sent to WP Leader – Regina Becker Draft to be circulated to national experts and WP participants for feedback.
09/06/2023	0v3	Dr. Jasper Bovenberg	Third draft circulated among WP 2 participants for comments.
14/07/2023	0v4	Dr. Jasper Bovenberg	Fourth draft incorporating all comments circulated among WP 2 participants. All questions asked by commentators answered..
21/07/2023	0v4	Nikki Coutts (ELIXIR Hub)	Version circulated to B1MG-OG, B1MG-GB and Stakeholders for feedback
31/07/2023	0v5	Dr. Jasper Bovenberg	No comments to be addressed.
15/09/2023	0v6	Dr. Jasper Bovenberg	Amalgamation of all work into one deliverable
28/09/2023	0v6	Nikki Coutts (ELIXIR Hub)	Version circulated to B1MG-OG, B1MG-GB and Stakeholders for feedback
05/10/2023	1v0	Nikki Coutts (ELIXIR Hub)	Version uploaded to the EC Portal

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Table of Contents

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

1. Executive Summary

- *Introduction*. This report presents (i) an analysis of the legal data protection (GDPR) framework governing the creation of a federated cohort of human genomic data across multiple Member States of the European Union ("EU"), followed by (ii) an analysis of the delineation of the pertinent national and EU competences, for a number of selected Member States, establishing the existence, scope and impact of GDPR exemptions at the level of the Member States, which analyses collectively feed into (iii) a workable mechanism to bridge the legal national divergences found, in the form of a Transnational Code of Conduct respecting national minimum standards with respect to privacy, medical secrecy (aka patient confidentiality) and protection of personal data.

- While there seems to be a tendency to view privacy and data protection rights as "barriers", or "roadblocks", impeding the pursuit of data driven medical research, this report is based on and stresses the fact that the protection of natural persons in relation to processing of their personal data is a fundamental right. Article 8 (1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

- Based on the fundamental right to data protection enshrined in the Charter and the Treaty, the EU General Data Protection Regulation (GDPR) provides every identified or identifiable person ("a data subject", under the GDPR) with a set of rights ("data subject rights") which, alone and in combination, protect his or her personal data. These rights are set forth in Chapter III of the GDPR and form the core element of the GDPR. Also, when any definition or provision of the GDPR is subject to interpretation, the test applied by the Court of Justice for the European Union ("CJEU") for the proper interpretation is that the interpretation must ensure the effective and comprehensive protection of the persons concerned.

- *Part I of the Report: data subject rights and cross-border access issues under GDPR*. Part I of this report analyses the scope of and exemptions to data subject rights under the GDPR when it comes to processing genetic data for biomedical research, as well as the obligations of controllers of personal data to facilitate the exercise of these rights, referencing the most recent Guidance of the European Data Protection Board and recent case law of the Court of Justice of the European Union.

- The GDPR data subject rights apply to the processing of data concerning genetic data *per se*, as well as to the processing of data, including genetic data, for the purpose of scientific research. The provision of access to genomic data of a data subject by a data controller in one Member State to a data user(s) from another Member State(s) ("Cross Border Access") is likely to involve the processing of (directly or indirectly) identifying data (personal data) and hence subject to the GDPR. As the provision of Cross Border Access involves the processing, on a large-scale, of special categories of data (i.e. genetic data), it is deemed by GDPR to be likely to result in a high risk to the rights and freedoms of the data subjects concerned.

- This high risk is likely to increase due to the proposed repeated use of the genomic data through the continued Cross Border Access to be provided to multiple data users, from a variety of jurisdictions, each with their own rules and regulations. Moreover, the high risk could increase still further due to the resultant accumulation of meaning to be ascribed to and

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

derived from genomic data, and its potential of being abused, for public, political, commercial or private purposes, whether or not by linking with other personal data, resulting in economic or social disadvantage, including discrimination and limitation or denial of access to private and public services, loss of autonomy, automated decision-making and coercive medicine, for the data subject, her family or the ethnic minority to which she belongs.

- To address these risks, processing these data within a Member State of the European Union (EU) is subject to the national legislation of that Member State, which includes but is not limited to the GDPR, as implemented in the Member State concerned. However, the processing of these personal genetic data *across the borders* of the Member States raises, inter alia, the following issues under the GDPR.

    - *Processing of special categories of personal data.* First, under the GDPR the processing of genetic data and data concerning health is prohibited[1]. This prohibition can only be lifted if one of the exceptions[2] listed in the GDPR applies and provided that the processing complies with all other requirements of the GDPR, including a legal basis for lawful processing[3].

    - *Member State conditions.* Second, the GDPR provides that Union law or Member State law may provide that the prohibition of processing genetic data under the GDPR may not be lifted by the data subject[4]. Also, Member States may maintain or introduce their own, national, conditions, including limitations, with regard to the processing of genetic data[5].

    - *Processing for purposes of scientific research requires appropriate safeguards.* Third, the GDPR provides that, regardless of the type of data, processing personal data for scientific research purposes must be subject to appropriate safeguards, in accordance with the GDPR, for the rights and freedoms of the data subject[6].

    - *Member State derogations to data subject rights.* Fourth, when personal data are being processed for scientific purposes, the GDPR allows the Member States, under certain conditions, to enact their own, national, derogations from certain data subject rights under the GDPR[7]. In brief, processing of personal genetic data for purposes of scientific research has not been harmonised under the GDPR.

    - *Accountability for compliance with GDPR - assignment of GDPR roles.* Fifth, the disclosure of genetic data by the primary collector (controller and custodian) of these data to one or more researchers established in one or more other Member State(s) raises questions about GDPR roles and responsibilities, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of the GDPR.

[1] Article 9 § 1 of the EU General Data Protection Regulation (GDPR).
[2] Article 9 § 2 of the GDPR.
[3] Article 6 of the GDPR.
[4] Article 9 § 2 GDPR.
[5] Article 9 § 4 of the GDPR ('Lawfulness of processing').
[6] Article 89 § 1 of the GDPR.
[7] Where personal data are processed for scientific or historical research purposes, Union or Member State law may provide for derogations from the right of access by the data subject (Article 15 of the GDPR), the right to rectification (Article 16 of the GDPR) the right to restriction of processing (Article 18 of the GDPR) and the right to object (Article 21 of the GDPR), subject to the conditions and safeguards referred to in Article 89 § 1 of the GDPR and in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purpose of the scientific research and such derogations are necessary for the fulfilment of this purpose (Article 89 § 2 of the GDPR).

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

- *Which national law applies?* Sixth, the transfer and subsequent processing of personal genetic data across the borders of the Member States raises the issue which Member State's national data protection law applies? The territorial scope of the GDPR is directly based on the GDPR[8]. However, this territorial effect does not apply to the territorial scope of the Member State law which is based on the GDPR. The territorial effect of such national laws depends on the national law of the Member State concerned.

- *Processing genetic data may be subject to additional national specific sector laws.* Seventh, processing genetic data within a given Member State is not only subject to the GDPR but also to specific (health) sector national laws and human rights, such as patient confidentiality laws, criminal laws and associated national and institutional regulations. In addition, use of the data is in principle subject to informed consent and any limitations therein and subject to prior approval by an ethics committee and any conditions of such an approval. Compliance with these additional laws and conditions is typically the responsibility of the initial collector and controller of these data, in his or her role as custodian of these data. A siloed regulatory approach, focusing exclusively on the GDPR, would compromise compliance by this controller who is also the custodian of these data pursuant to related laws, regulations, conditions, codes and associated guidance, and case law.

- *Part II of the Report: delineation of national and EU competences and the existence, scope and impact of national GDPR exemptions*. Part II of the Report aims to establish an acceptable ELSI framework that can strengthen the secure sharing of genomics data across Europe and determine and analyse the pan-European legal framework governing the data life cycle envisaged by the European 1+MG initiative. It aims to delineate the national and EU competences for a number of selected Member States and establish the existence, scope and impact of national GDPR exemptions, as well as flag potential challenges that can arise from cross-border processing and from bringing genomic research data to clinic. This part aims to works towards common minimum standards and identify applicable GDPR requirements as well as a relevant legal framework applicable for cross-border data sharing.

- This part navigated the national heterogeneous ethico-legal landscapes and identified existing solutions and relevant stakeholders for input and feedback. The work is based on a series of expert workshops, organised in 2021 and the first months of 2022, with the participation of representatives of different countries across the EU from Nordic, South, Central and Eastern European regions. The results of these workshops focused on adapting and further developing existing ethical standards, analysing the national legal landscape that affects a cross-border genome initiative and creating a pool of tools to centrally govern such infrastructure. Through these workshops, this study mapped the EU legal framework governing the data life cycle of a pan-European genome initiative with a specific focus on the challenges of making genomic data available across European Economic Area (EEA) countries. Specifically, we assessed how the GDPR has been implemented at national level regarding the processing of health and genetic data and thus focused on applicable GDPR requirements for cross-border sharing, in order to assess the national derogations and divergence.

- By examining and presenting, the national legal landscape rules that govern the processing of health and genetic data light of the GDPR, based on selected examples, this part highlights possible differences and identifies elements that might affect the cross-border exchange of health and genetic data in the EU from healthcare to research and vice versa in order to support health and genetic data use and re-use. The analysis of the results of the study proves

[8] Article 3 of the GDPR.

that there are differences between EU countries in the implementation of the GDPR in the field of the secondary use of health and genetic data and the development of a common ethico-legal framework is indispensable.

- *Part III of the Report: Cross Border Compliance by Transnational Code of Conduct.* The third and final part of this report builds on Reports I and II by delivering a draft Transnational Code of Conduct governing the provision of cross border access to human genomic data for purposes of scientific research within the EU.

- In terms of substance, the draft Transnational Code requires inter alia (i) positive advice on requests for cross border access from a cross border access committee (which could be part of a regular, national access committee), (ii) data protection safeguards, (iii) access by way of remote analysis (bringing foreign analysis to local data), (iv) allocation of obligations and responsibilities between the data custodian and the data user and (v) respecting home state specific sector rights, human rights and data subject rights, the latter as per the national implementation thereof.

- To comply with EDPB Guidance on Codes of Conduct and Monitoring Bodies[9], the draft Transnational Code is preceded by an Explanatory Note. Having commented on the draft Code. Upon review of the draft and incorporation of its comments, a competent Data Protection Agency has expressed its willingness to receive the draft to initiate the process for formal approval of the Code under Article 40 GDPR.

2. Contribution towards project objectives

With this deliverable, the project has reached or the deliverable has contributed to the following objectives/key results:

	Key Result No and description	Contributed
Objective 1 Engage local, regional, national and European stakeholders to define the requirements for cross-border access to genomics and personalised medicine data	**1.** B1MG assembles key local, national, European and global actors in the field of Personalised Medicine within a B1MG Stakeholder Coordination Group (WP1) by M6.	No
	2. B1MG drives broad engagement around European access to personalised medicine data via the B1MG Stakeholder Coordination Portal (WP1) following the B1MG Communication Strategy (WP6) by M12.	No
	3. B1MG establishes awareness and dialogue with a broad set of societal actors via a continuously monitored and refined communications strategy (WP1, WP6) by M12, M18, M24 & M30.	No
	4. The open B1MG Summit (M18) engages and ensures that the views of all relevant stakeholders are captured in B1MG requirements and guidelines (WP1, WP6).	No

[9] EDPB, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.

Objective 2 Translate requirements for data quality, standards, technical infrastructure, and ELSI into technical specifications and implementation guidelines that captures European best practice	**Legal & Ethical Key Results**	
	1. Establish relevant best practice in ethics of cross-border access to genome and phenotypic data (WP2) by M36	No
	2. Analysis of legal framework and development of common minimum standard (WP2) by M36.	Yes
	3. Cross-border Data Access and Use Governance Toolkit Framework (WP2) by M36.	Yes
	Technical Key Results	
	4. Quality metrics for sequencing (WP3) by M12.	No
	5. Best practices for Next Generation Sequencing (WP3) by M24.	No
	6. Phenotypic and clinical metadata framework (WP3) by M12, M24 & M36.	No
	7. Best practices in sharing and linking phenotypic and genetic data (WP3) by M12 & M24.	No
	8. Data analysis challenge (WP3) by M36.	No
	Infrastructure Key Results	
	9. Secure cross-border data access roadmap (WP4) by M12 & M36.	No
	10. Secure cross-border data access demonstrator (WP4) by M24.	No
Objective 3 Drive adoption and support long-term operation by organisations at local, regional, national and European level by providing guidance on phased development (via the B1MG maturity level model), and a methodology for economic evaluation	**1.** The B1MG maturity level model (WP5) by M24.	No
	2. Roadmap and guidance tools for countries for effective implementation of Personalised Medicine (WP5) by M36.	No
	3. Economic evaluation models for Personalised Medicine and case studies (WP5) by M30.	No
	4. Guidance principles for national mirror groups and cross-border Personalised Medicine governance (WP6) by M30.	No
	5. Long-term sustainability design and funding routes for cross-border Personalised Medicine delivery (WP6) by M34.	No

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

3. Methods

3.1 Deliverable scope

Part 1 of this Report is part of Task 2.3 of Working Package 2, to specifically, with a view to the empowerment of data subjects under the GDPR, analyse the scope and exemptions to data subject rights when it comes to processing for biomedical research and to develop the legal specifications to help build workable mechanisms to make these rights operational and form the basis for a Code of Conduct for the cross-border sharing of genetic data. Part 2 of the Report is part of Task 2.3 of Working Package 2, which focuses on the analysis of legal framework and the development of common minimum standards. In this report, the first three Tasks of the "D2.3 - Analysis of legal framework and development of common minimum standard" of WP2 will be addressed. The scope of Task 2.3.1 is to determine and analyse the pan-European legal framework governing the data life cycle envisaged by the European 1+MG initiative. Task's 2.3.2 aim is to delineate the national and EU competences for a number of selected Member States and establish the existence, scope and impact of national GDPR exemptions, as well as flag potential challenges that can arise from cross-border processing and from bringing genomic research data to clinic. The aim of Task 2.3.3 is to work towards common minimum standards and identify applicable GDPR requirements as well as a relevant legal framework applicable for cross-border data sharing. The scope of part 3 of the Report is to provide elements for a Code of Conduct to address the issues yielded by the analyses in Reports 1 and 2.

3.2 Methodology

Part I of the Report comprises a legal analysis of the data subject rights under the GDPR, the exemptions thereto and the obligations of controllers to facilitate the exercise of these rights and includes reference to the most recent Guidance of the European Data Protection Board and recent case law of the Court of justice of the European Union.[10] [11] Part II of the Report uses a mixed-methods approach, consisting of workshops with national experts and literature review. More specifically, four (4) workshops including Nordic, South, Central and Eastern European countries were organised focusing on the implementation of GDPR and secondary use of health and genetic data in these different countries. The topics touched upon during the workshops included, among others, the legal basis for the secondary use of health and genetic data for scientific research purposes, the ways that each national legislation system in the examined countries has reacted to GDPR derogations with a particular focus on the derogations from the right to access, the right to restriction of processing and the right to object to processing, the specific safeguards in place, the ethico-legal framework used in the examined countries to transfer health and genetic data from healthcare to research settings and vice versa and the set of legal instruments and soft law documents, as well as the responsible committees/bodies, which are of relevance for the ethico-legal control and/or approval of the data life cycle from healthcare to research settings and vice versa. The presentations of twenty (20) experts from seventeen (17) selected Member States were used to feed into our research, which was complemented by desk-based research on relevant literature, including

[10] EDPB Guidelines 01/2022 on data subject rights - Right of access Version 2.0, Published April 17, 2023.
[11] For an analysis of any national exemptions, to the GDPR data subject rights, please refer to the BMG report by Dr. Olga Tzortzatou, Marina Makri, Alexandra Ziaka, T2.3 - Analysis of legal framework and development of common minimum standards

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

academic papers, guidelines and reports. The combination of the workshops and the literature review helped us assess the implementation of GDPR at national level and the applicable framework on the secondary use of health and genetic data in the examined countries. The results assisted our efforts in establishing the existence, scope, and impact of national GDPR exemptions and flagging potential challenges that can arise from cross-border processing and from bringing genomic research data to the clinic. By analysing the pan-European legal framework governing the data life cycle in different countries, we can designate the main points of the common ethical-legal framework that need to be determined by the B1MG project Part III of the Report comprises a draft Transnational Code of Conduct intending the proper application of the EU General Data Protection Regulation to cross border analysis of human genetic data for purposes of scientific research within the European Union. Rather than simply suggesting elements for a Code, a back to back Transnational Code was drafted, in accordance with EDPB Guidance on Codes of Conduct, as that is typically the best way to test its feasibility. In addition, this draft was discussed informally with a competent national Data Protection Agency, which, on the basis of this draft, confirmed its willingness to receive a formal submission for approval of the Transnational Code.

4. Description of work accomplished

4.1 Data subject rights, derogations and facilitation of the exercise of rights

4.1.1 Introduction

1. The protection of natural persons in relation to processing of personal data is a fundamental right. Article 8 (1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

2. The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. The EU General Data Protection Regulation (Regulation (EU) 2016/679) is intended to ensure a consistent and high level of protection of natural persons and to remove obstacles to flows of personal data within the Union.

3. Based on the fundamental right to data protection enshrined in the Charter of Fundamental Rights of the European Union (EU), the EU General Data Protection Regulation (GDPR) provides data subjects with a set of rights (data subject rights) which, alone and in combination, protect the personal data of everyone. These rights are set forth in Chapter III of the GDPR and form the core element of the GDPR[12]. Also, when any definition or provision of the GDPR is subject to interpretation, the test applied by the Court of Justice for the European Union for the proper interpretation is that the

[12] See also Recital 11 of the Regulation.

interpretation must ensure the effective and comprehensive protection of the persons concerned[13].

4. The GDPR data subject rights apply to the processing of data concerning health and genetic data per se, as well as to the processing of data, including genetic data, for the purpose of scientific medical research. The GDPR data subject rights include the right to information about the processing, access to one's personal data, to receive a copy of one's personal data, rectification and erasure, the right to restriction of processing, the right to data portability, the right to restrict processing, the right to object and the right not to be subject to fully automated decision-making and profiling.

5. Some data subject rights have been limited in the GDPR itself, other rights may be derogated from by Union or Member State law, including in the event the processing of the data is necessary for the purpose of scientific research, in so far as these rights are likely to render impossible or seriously impair the achievement of this specific purpose and such derogations are necessary for the fulfilment of those purposes. Some data subject rights are not subject to any derogations whatsoever.

6. Specifically, where personal data are processed for scientific or historical research purposes, Union or Member State law may provide for derogations from the right of access by the data subject (Article 15 of the GDPR)[14], the right to rectification (Article 16 of the GDPR)[15], the right to restriction of processing (Article 18 of the GDPR)[16] and the right to object (Article 21 of the GDPR)[17], subject to the conditions and safeguards referred to in Article 89 § 1 of the GDPR and in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purpose of the scientific research and such derogations are necessary for the fulfilment of this purpose (Article 89 § 2 of the GDPR).

7. In addition, Article 23 of the GDPR provides for Member States (or the EU) to legislate for further restrictions on the scope of the data subject rights in relation to transparency and the substantive data subject rights where such measures are necessary and proportionate to safeguard one or more of the ten objectives set out in Article 23.1(a) to (j). As research is not listed as one of the objectives, no derogations on the basis of Article 23 can be issued.

8. The GDPR provides that the controller shall facilitate the exercise of the rights of the data subject and provides for modes of provision and deadlines[18]. The controller shall take appropriate measures to provide the information required under the GDPR. In addition, the controller must take appropriate measures to provide communication in respect of the data subject rights relating to processing to the data subject, in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

[13] E.g Judgment of the Court (Second Chamber), 29 July 2019 (*)In Case C-40/17, citing judgments of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 34, and of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, paragraph 28).
[14] EU Regulation, Article 89(2) juncto Article 15.
[15] EU Regulation Article 89(2) juncto Article 16.
[16] EU Regulation Article 89(2) juncto Article 18.
[17] EU Regulation Article 89(2) juncto Article 21.
[18] Article 12 of the Regulation.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

4.1.2 Analysis of the GDPR data subject rights 'right by right'[19]

4.1.2.1 Right to Information and Access to Personal Data

9. The Rights to Information where personal data are collected from the data subject. The right to information stems from the GDPR principles of fairness and transparency and is an essential right to ensure fair and transparent processing[20]. Also, the requirements of data protection by design and by default require data controllers implementing measures consisting of transparency with regard to the functions and processing of personal data[21].

10. Where personal data are collected from the data subject, the controller shall inform the data subject regarding the processing of his personal data[22]. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information, including but not limited to: the identity of the controller and the contact details of the controller, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for processing and the recipients or categories of recipients of the personal data, if any, and, where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and reference to the appropriate or suitable safeguards and the means by which to obtain a copy thereof.

11. As to the information on the recipients of the data, in a recent judgement by the Court of Justice of the European Union ("CJEU") of 12 January 2023, the CJEU held that when exercising their right of access under the GDPR, data subjects must be provided with the individual data recipients of their personal data[23]. Under Article 15 GDPR, data subjects have the right to obtain confirmation from the controller as to whether or not personal data concerning him or her are being processed, and, where this is the case, "information relating to 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" (Article 15(1)(c) GDPR). According to the court, this also follows from article 19 of the GDPR which confirms that, in order to ensure the effectiveness of the data subject's rights to rectification, to erasure and to restriction of processing provided for by Articles 16, 17 and 18 of the GDPR, the data subject must in principle have the right to be informed of the identities of specific recipients, where his or her personal data have already been disclosed. Indeed, only in this way can the data subject assert his or her rights against them.

12. In the case at hand, the data subject had requested information regarding the identity of third parties to whom the controller had disclosed his personal data. In response to the request, the controller provided the data subject with the categories of recipients and

[19] For an analysis of any national exemptions, to the GDPR data subject rights, please refer to the BMG report by Dr. Olga Tzortzatou, Marina Makri, Alexandra Ziaka, D2.3 - Analysis of legal framework and development of common minimum standards

[20] Art. 13-14 Regulation; Rec. 58, 60;

[21] Article 25 of the GDPR.

[22] Art. 5(1)(a), 12-14 Regulation; Rec. 39, 58, 60.

[23] Judgement of the Court (First Chamber), 12 January 2023 (Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 15(1)(c) – Data subject's right of access to his or her data – Information about the recipients or categories of recipient to whom the personal data have been or will be disclosed – Restrictions) In Case C-154/21, request for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 18 February 2021, received at the Court on 9 March 2021, in the proceedings RW v Österreichische Post AG.

also referred to a website that set out more information and further data processing purposes. The CJEU held that the right of access under Article 15 GDPR contains an obligation on the controller to provide the data subject with the actual identity of recipients of their personal data. In particular, the CJEU held that the information provided to the data subject under Article 15(1)(c) GDPR must be as precise as possible. Whether the individual recipients are disclosed or only the categories of recipients are disclosed is, in principle, a choice of the data subject. The CJEU held that Article 15(1)(c) GDPR allows the data subject to obtain information from the controller about the specific recipients to whom the data have been or will be disclosed or, alternatively, "to elect merely to request" information concerning the categories of recipient. Article 15 GDPR "lays down a genuine right of access for the data subject, with the result that the data subject must have the option of obtaining either information about the specific recipients to whom the data have been or will be disclosed, where possible, or information about the categories of recipient."

13. In addition, the CJEU ruled that data subjects must, in particular, have the "right to be informed of the identity of the specific recipients where his or her personal data have already been disclosed." Finally, the CJEU highlighted that there are two 'exceptions' to the general rule that the data subject has a right to know the identity of the specific recipients. First, "the right of access may be restricted to information about categories of recipients if it is impossible to disclose the identity of specific recipients, in particular where they are not yet known." Notably, this exception is not laid down in the GDPR. And, second, when the controller can demonstrate that a request is manifestly unfounded or excessive, within the meaning of Article 12(5) of the GDPR.

14. In addition, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: 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 the processing is based on informed consent, the data subject must be informed of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

15. The controller must also inform the data subject about the right to lodge a complaint with a supervisory authority and whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data. The controller must further provide the existence of automated decision-making, including profiling, and at least in certain cases, meaningful information about the logic involved, as well as the significance and the envisaged consequence of such processing for the data subject.

16. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information. The Article 29WP Guidelines provide in this respect that the requirement "to inform a data subject about further processing promotes the position in the GDPR that a data subject should reasonably expect that at the time and in the context of the collection of personal data that processing for a particular purpose

may take place. In other words, a data subject should not be taken by surprise at the purpose of processing of their personal data."[24] The Article WP29 also recommends that, in order to be transparent, fair and accountable, controllers should consider making information available to data subjects in their privacy statement/ notice an explanation as to how the processing for the other purpose(s) is compatible with the original purpose. This is to allow data subjects the opportunity to consider the compatibility of the further processing and the safeguards provided and to decide whether to exercise their rights e.g. the right to restriction of processing or the right to object to processing, amongst others[25].

17. Notably, as to the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively, the Article 29 Working Party has stated that there is no difference; all of the information across these sub-articles is of equal importance and must be provided to the data subject[26].

18. In the event of joint controllers, Article 26.1 of the GDPR requires them to determine their respective responsibilities for complying with regard to the exercise by data subjects of their rights and the duties to provide the information under Articles 13 and 14. The essence of the arrangement between the data controllers must be made available to the data subject and it must be completely clear to a data subject as to which data controller he or she can approach where they intend to exercise one or more of their rights under the GDPR[27].

19. *Derogation*. The above data subject rights to information, where personal data are collected from the data subject, are not subject to any derogation, other than when and in so far as the data subject already has the information[28].

20. The rights to information where personal data have not been obtained from the data subject. Where the controller has obtained personal data not from the data subject, but from a third party, the controller must provide the following information to the data subject: the identity and the contact details of the controller, the contact details of the data protection officer, the purposes of the processing, for which the data are intended as well as the legal basis for the processing, the categories of personal data concerned, the recipients or categories of recipients of the personal data, if any. Where applicable the controller must inform the data subject that the controller intends to transfer personal data to a recipient in a third country or international organisation, and the existence of appropriate or suitable safeguards and the means to obtain a copy thereof.

21. In addition, the controller must provide the data subject with the following information, necessary to ensure fair and transparent processing in respect of the data subject: 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 and to object to processing as as the right to data portability.

[24] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and adopted on 11 April 2018, page 23-24.
[25] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and adopted on 11 April 2018, page 24.
[26] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and adopted on 11 April 2018, page 14.
[27] Article 26 GDPR,; see also Article 29 WP, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and adopted on 11 April 2018, page 23.
[28] Article 13 paragraph 4 of the GDPR.

Where data processing is based on informed consent (as a legal basis and/or as a way to lift the prohibition of processing 'sensitive data'), the controller must inform the data subject on the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

22. The controller must further inform the data on his or her right to lodge a complaint with a supervisory authority and from which source the personal data originate, and, if applicable, whether it came from publicly accessible sources. In addition, the controller must inform the data subject about the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. The controller shall provide the data subject with the information set forth above, 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, the controller shall provide the information at the latest at the time of the first communication to that data subject, or if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

23. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information.

24. *Derogation.* The GDPR provides for a number of derogations to this obligation of the controller to provide information where personal data have not been obtained from the data subject[29]. As a general rule of EU law, these exceptions should be interpreted and applied narrowly[30].

25. First, the obligation does not apply where and insofar the data[31] subject already has the information. Second, the obligation does not apply where the provision of the information proves impossible or would involve either (i) a disproportionate effort, in particular for processing for scientific research purposes, or (ii) in so far as the obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing.[32] In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including in making the information publicly available. This is subject to the safeguards provided for in article 89(1) of the GDPR. These 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. Where the purpose of scientific research can be achieved by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

    a. *Proves impossible.* If a data controller seeks to rely on this exemption it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period of time, the factors that caused

[29] Article 14 5 (a)-(d).
[30] See, e.g. Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and adopted on 11 April 2018, page 28.
[31] Article 14(5)(a) of the GDPR.
[32] Article 14(5)(b) of the GDPR.

the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so.

b. *Impossibility of providing the source of the data*. The requirement to provide data subjects with information on the source of their personal data can only be lifted in the event the impossibility is due to the fact that different pieces of personal data relating to the same data subject cannot be attributed to a particular source. However, the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. The EDPB Guidelines also make it clear that, given the requirements of data protection by design and by default, transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organisation can be tracked and traced back to their source at any point in the data processing life cycle[33].

c. *Disproportionate effort*. Factors to assess whether providing the information would involve a disproportionate effort, include the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration[34]. In its Guidelines, the WP29 (EDPB) stresses in this respect that the fact that where research is the pursued purpose, the conditions set out in Article 89(1) of the GDPR must still be complied with. As also pointed out by the EDPB in its guidance on this exception, "in practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects."[35]

d. *Providing information renders objective impossible*. To be able to invoke this exception, data controllers must demonstrate that the provision of the information set out in Article 14.1 alone would nullify the objectives of the processing. As observed in the WP29 Guidelines, reliance on this aspect of the exception "pre supposes that the data processing satisfies all of the principles set out in Article 5 and that most importantly, in all of the circumstances, the processing of the personal data is fair and that it has a legal basis."[36]

e. *Assessment and measures.* In the event a data controller seeks to rely on the exception that provision of the information proves impossible, would involve a disproportionate effort, or would likely render impossible or seriously impair the achievement of the objectives (in casu: research) of the processing, it must conduct an assessment to weigh the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he was not provided with the information. This assessment should be documented by the data controller in accordance with the accountability obligations. If the assessment shows that the requirements of the exception have been met, the controller must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests. One such measure that

[33] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and adopted on 11 April 2018, page 29.
[34] Recital 62 of the GDPR.
[35] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and adopted on 11 April 2018, page 29.
[36] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and adopted on 11 April 2018, page 31.

controllers must always take is to make the information publicly available. Other appropriate measures will depend on the circumstances of the processing, but will include minimising the data collected and the storage period[37].

26. Third, the obligation to provide the information to the data subject where the controller has not obtained the data from the data subject, does not apply "where the personal data must remain confidential subject to a professional obligation of secrecy regulated by Union or Member State law, including a statutory obligation of secrecy."[38] This derogation may be of specific relevance to genetic data obtained in a clinical setting. If, for example, a clinical institution seeks to rely on this exemption, "it must be able to demonstrate that it has appropriately identified such an exemption and to show how the professional secrecy obligation directly addresses the data controller such that it prohibits the data controller from providing all of the information set out in Articles 14.1, 14.2 and 14.4 to the data subject."[39] The Article 29WP Guidelines give the following example:

> A medical practitioner (data controller), who is under a professional obligation of secrecy in relation to his patients' medical information. A patient (in respect of whom the obligation of professional secrecy applies) provides the medical practitioner with information about her health relating to a genetic condition, which a number of her close relatives also have. The patient also provides the medical practitioner with certain personal data of her relatives (data subjects) who have the same condition. The medical practitioner is not required to provide those relatives with Article 14 information as the exemption in Article 14.5(d) applies. If the medical practitioner were to provide the Article 14 information to the relatives, the obligation of professional secrecy, which he owes to his patient, would be violated.

27. It is questionable however, whether this example is correct in its application of the professional secrecy law. Under such a law, exemptions exist precisely in the above case, where clinicians may have a professional duty to inform other patients (relatives) about certain conditions. As these medical laws and duties cannot be trumped by the GDPR and the GDPR explicitly defers to these laws in Article 14(5)(d) (and elsewhere), the medical practitioner in the example may be obliged, on the basis of his professional (statutory) duties, to provide the information to the relatives and may not be allowed to invoke on an exemption under the GDPR[40].

4.1.2.2 Right of confirmation, access and a copy

28. Pursuant to Article 15 of the GDPR, the data subject has the right of access. As observed by the EDPB, "[I]n accordance with CJEU decisions[41], the right of access serves the purpose of guaranteeing the protection of the data subjects' right to privacy and data protection with regard to the processing of data relating to them[42] and may facilitate the exercise of their rights flowing from, for example, Art. 16 to 19, 21 to 22 and 82 GDPR. However, the exercise of the right of access is an individual's right and not conditional

[37] Article 14(5)(b) of the GDPR.
[38] Article 14.5(d) of the GDPR.
[39] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and adopted on 11 April 2018, page 33.
[40] A fourth exception, set forth in Article 14(5)(c)of the GDPR is prima facie not applicable and will not be discussed in detail.
[41] Court of Justice of the European Union (CJEU), C-434/16, Nowak and joined cases C-141/12 and C-372/12, YS and others
[42] CJEU, C-434/16, Nowak, para. 56.

upon the exercise of those other rights and the exercise of the other rights does not depend on the exercise of the right of access."[43]

29. *Right to Confirmation and Information.* The data subject rights in Article 15 GDPR include the following. First, the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning the data subject are being processed by the controller. Where that is the case, the data subject has the right to access the personal data and the right to the following information:
    - the purposes of the processing, the categories of personal data concerned;
    - the recipients of categories of recipients 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 automated decision-making, including profiling, 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(s).

30. In addition, where personal data are transferred to a third country or to an international organisation, the data subject must be informed of the appropriate safeguards required under Article 46 of the GDPR.

31. *Right to Access.* Article 15 of the Regulation provides that the data subject shall have the right to obtain from the controller access to the personal data being processed. The scope of the right of access is determined by the scope of the concept of personal data as defined in Art. 4(1) GDPR. Notably, as observed by the EDPB, "like most data subject rights, the right of access includes both inferred and derived data, including personal data created by a service provider, whereas the right to data portability only includes data provided by the data subject[44]. Therefore, in case of an access request and unlike a data portability request, the data subject should be provided not only with personal data provided to the controller in order to make a subsequent analysis or assessment about these data but also with the result of any such subsequent analysis or assessment."[45]

32. *The right to a copy.* Article 15 further provides that the controller shall provide the data subject, upon his or her request, a copy of the personal data undergoing processing[46]. This copy must be provided at no cost. 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 his request for a copy by electronic means, and unless otherwise requested by the data subject, the controller shall provide the information in a commonly used electronic form.

33. The scope of the right of access and a copy has recently been considered by Court of Justice of the European Union (CJEU) in the case *Österreichische Datenschutzbehörde and CRIF*. The CJEU ruled that the right to obtain a "copy" of personal data means that the data subject must be given a "faithful and intelligible" reproduction of all those data. This means that copies of extracts from documents, entire documents or extracts from

[43] EDPB Guidelines 01/2022 on data subject rights - Right of access Version 2.0, Published April 17, 2023.
[44] As previously stated in WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 10 and reiterated in WP29 Guidelines on Automated individual decision-making and profiling - endorsed by the EDPB, p. 17.
[45] EDPB Guidelines 01/2022 on data subject rights - Right of access Version 2.0, Published April 17, 2023, para 99.
[46] See also Recital 69 of the Regulation.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

databases which contain those data should be provided, if necessary to enable the data subject to exercise effectively the rights under the GDPR. The CJEU also interpreted the concept of "information" in Article 15(3) narrowly, concluding that it refers exclusively to the "copy of personal data undergoing processing".[47]

34. Where possible, the controller(s) should provide remote access to a secure system which would provide the data subject with direct access to his or her data. In addition, pursuant to Article 12 of the GDPR, the controllers concerned must provide this information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child[48].

35. *Limits and derogation.* The right to receive a copy of the data may not adversely affect the right and freedoms of others, according to paragraph 4 of Article 15 of the GDPR. Rights or freedoms of others include trade secrets or intellectual property and in particular the copyright protecting the software[49]. As per the EDPB Guidelines, "the general concern that rights and freedoms of others might be affected by complying with the request for access, is not enough to rely on Art. 15 (4) GDPR. The controller must be able to demonstrate that in the concrete situation, rights or freedoms of others would, in fact, be impacted."[50]

36. In addition, the GDPR provides that it is possible to provide under Union or Member State law for derogations from the rights referred to in Article 15[51]. Any derogations must be subject to the safeguards provided for in article 89(1) of the GDPR. These 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. Where the purpose of scientific research can be achieved by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

4.1.2.3 Right to rectification and supplementation

37. *Right to Rectification and a supplementary statement.* Pursuant to Article 16 of the GDPR, data subjects have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. The data subject has the right to have incomplete personal data completed, including by means of a supplementary statement. Controllers must ensure that inaccurate or incomplete data are erased or rectified[52].

38. *Derogation.* Article 89(1) of the GDPR provides that it is possible to provide under Union or Member State law for derogations from the right to rectification. Any derogations must be subject to the safeguards provided for in article 89(1) of the GDPR. These safeguards

[47] Judgement of the Court (First Chamber), 4 May 2023 (Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Data subject's right of access to his or her data undergoing processing – Article 15(3) – Provision of a copy of the data – Concept of 'copy' – Concept of 'information') In Case C-487/21, request for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Federal Administrative Court, Austria), made by decision of 9 August 2021, received at the Court on 9 August 2021, in the proceeding F.F. Österreichische Datenschutzbehörde,intervening party: CRIF GmbH. ECLI:EU:C:2023:369.
[48] Rec. 39, 59, 65, 73; Art. 5(1)(d), 16 Regulation.
[49] Recital 63 of the Regulation.
[50] EDPB Guidelines 01/2022 on data subject rights - Right of access Version 2.0, Published April 17, 2023, para 172.
[51] EU Regulation, Article 89(2) juncto Article 15.
[52] Rec. 39, 59, 65, 73; Art. 5(1)(d), 16 Regulation.

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. Where the purpose of scientific research can be achieved by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

4.1.2.4 Right to Erasure

39. *Right to Erasure ('Right to be Forgotten').* Pursuant to Article 17 of the GDPR, data subjects have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase personal data without undue delay in the following events:[53]

    a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

    b. the data subject withdraws consent on which the processing is based and there is no other legal ground for processing;

    c. the data subject objects to the processing pursuant to Article 21 of the Regulation discussed below, and there are no overriding legitimate grounds for processing;

    d. the personal data have been unlawfully processed;

    e. the personal data have to be erased for compliance with legal obligation in Union or Member State law to which the controller is subject;

    f. the personal data have been collected in relation to the offer of information society services.

40. *Derogation.* The right to erasure shall not apply to the extent that processing is necessary for scientific research purposes or statistical purposes, subject to appropriate safeguards, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing[54]. The safeguards required 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. Where the purpose of scientific research can be achieved by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

4.1.2.5 Right to Restrict Processing

41. *The Right to Restrict Processing of Personal Data.* Pursuant to Article 18 of the GDPR, data subjects have the right to obtain from the controller restriction of processing of personal data, where one of the following applies:[55] the accuracy of the personal data is contested

[53] Rec. 65-66, 68; Art. 17 (1) of the GDPR.
[54] Article 17 (3)(d) Regulation.
[55] Rec. 67; Art. 18 Regulation.

by the data subject, for a period enabling the controller to verify the accuracy of the personal data; the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; the data subject has objected to processing pending the verification whether legitimate grounds of the controller override those of the data subject.

42. Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. A data subject who has obtained restriction of processing shall be informed by the controller before the restriction is lifted.

43. *Derogation.* Article 89(1) of the GDPR provides that it is possible to provide under Union or Member State law for derogations from the right to restrict processing. Any derogations must be subject to the safeguards provided for in article 89(1) of the GDPR. These 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. Where the purpose of scientific research can be achieved by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

4.1.2.6 Right to Portability

44. *Right to Portability of Personal Data.* Pursuant to Article 20 of the GDPR, a data subject has the right to data portability. The right to data portability is comprised of two sub rights. It gives the data subject the right to (i) 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 (ii) the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The right applies, where (a) the processing is based on consent or on a contract and (b) the processing is carried out by automated means. When exercising this right, the data subject has the right to have the personal data, where this is technically feasible, transmitted directly from controller to controller[56]. The right shall not adversely affect the rights and freedoms of others.

45. The purpose of the right to data portability is to empower the data subject and give her more control over the personal data concerning her[57]. This right, which applies subject to certain conditions, supports user choice, user control and consumer empowerment. It is expressly limited to the personal data concerning the data subject, 'which he or she has provided to a controller.'

46. According to Guidelines of the Article 29 Working Party, the following categories can be qualified as "provided by the data subject":

[56] Rec. 68, 73; Art.20 of the GDPR.
[57] Article 29 Working Party, draft Guidelines on the right to data portability, adopted on 13 December 2016, 16/EN WP 242.

- data actively and knowingly provided by the data subject are included in the scope of the right to data portability (for example, mailing address, user name, age, etc.)
- observed data are "provided" by the data subject by virtue of the use of the service or the device. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by fitness or health trackers[58].

47. In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". These personal data do not fall within the scope of the right to data portability. However, whether or not a data subject has the right to data portability, she has the right to access her personal data and the right to receive a copy thereof under Article 15 of the Regulation.

48. *Derogation.* The GDPR does not provide for a derogation to the right to data portability.

4.1.2.7 Right to object

49. *Right to Object.* Article 21 of the GDPR gives the data subject the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, which is based on the necessity for the performance of a task carried out in the public interest or on the necessity for the purposes of the legitimate interests pursued by the controller or by a third party, including profiling. The controller(s) shall no longer process the personal data, unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

50. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which include profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

51. Where personal data are processed for scientific research purposes, the data subject shall have the right to object to processing personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest[59].

52. The right to object shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information, at the latest at the time of the first communication with the data subject. In the context of the use of information society services, the data subject may exercise his or her right to object by automated means using technical specifications.

53. *Derogation.* The GDPR provides that it is possible to provide under Union or Member State law for derogations from the right to object. Any derogations must be subject to the safeguards provided for in article 89(1) of the GDPR. These safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure

[58] Article 29 Working Party, draft Guidelines on the right to data portability, adopted on 13 December 2016, 16/EN WP 242.
[59] Regulation, Article 21 (6).

respect for the principle of data minimisation. Those measures may include pseudonymisation. Where the purpose of scientific research can be achieved by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner[60].

4.1.2.8 Prohibition of Automated Decision-Making

54. *Prohibition of automated decision-making.* Article 22 of the GDPR prohibits the controller to subject a data subject to a decision based solely on automated processing, including profiling, which produces legal effect concerning him or her or similarly significantly affects him or her. This prohibition does not apply if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or when the decision is based on the data subject's explicit consent.

55. In case the decision is necessary for the entering into or the performance of a contract between the data subject and a controller or in case the decision is based on the data subject's explicit consent, the controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express her point of view and to contest the decision.

56. Article 21 further prohibits that automated decisions be based on special categories of personal data (which includes genetic data), unless the processing is based on explicit consent or necessary for reasons of a substantial public interest on the basis of Union or Member State law, and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

57. *Derogation.* The GDPR does not provide for derogations to the right not to be subject to automated individual decision-making.

4.1.3 Facilitating the exercise of data subject rights

58. The GDPR provides that the controller shall facilitate the exercise of the rights of the data subject and provides for modes of provision and deadlines[61]. The controller shall take appropriate measures to provide the information required under the GDPR. In addition, the controller must take appropriate measures to provide communication in respect of the data subject rights relating to processing to the data subject, in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information should be provided in writing, or by other means, including, where appropriate, by electronic means.

59. Where the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In that event,

[60] Regulation, Article 89.
[61] Article 12 of the Regulation.

the data subject rights (Articles 15-20) shall not apply, except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification. In that case, the controller shall not refuse to act on the request of the data subject for exercising his or her rights[62].

60. The controller shall provide information on action taken on a request for the exercise of one or more data subject rights without undue delay and in any event within one month of receipt of the request[63]. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The data controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

61. The controller shall provide the information to the data subject free of charge and any actions to honour the exercise of the data subject right(s) shall be provided free of charge. Where the controller has reasonable doubts concerning the identity of the natural person making the request to exercise one or more of her data subject rights, the controller may request the provision of additional information necessary to confirm the identity of the data subject. Article 12(5) enables controllers to refuse to act on requests from data subjects that are manifestly unfounded or excessive or charge a reasonable fee. These concepts have to be interpreted narrowly, as the principles of transparency and cost free data subjects rights must not be undermined[64].

62. Controllers must be able to demonstrate to the individual why they consider that the request is manifestly unfounded or excessive and, if asked, explain the reasons to the competent supervisory authority. Each request should be considered on a case by case basis in the context in which it is made in order to decide if it is manifestly unfounded or excessive.

63. *Derogation.* The GDPR does not provide for any exemptions to the requirements of transparent information, communication and modalities for the exercise of the rights of the data subject, set forth in Article 12 of the GDPR.

64. *Notification obligation regarding rectification or erasure of personal data or restriction of processing.* Pursuant to Article 19 of the GDPR, the controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the data have been disclosed. As observed by the Opinion of the Advocate General in the above mentioned case RW v Österreichische Post AG, Article 19 of the GDPR requires the data controller to inform all recipients to whom it has transferred personal data of any request for the rectification, erasure or restriction of processing of those data with which the controller must comply. "Recipients so informed are then required immediately to rectify, erase or restrict the processing of the data, to the extent that they are still processing the data in question." In pursuit of the objective of ensuring a high

[62] Article 11 of the Regulation.
[63] Art. 12 (3)(4) Regulation of the Regulation.
[64] EDPB Guidelines 01/2022 on data subject rights - Right of access Version 2.0, Published April 17, 2023, para 175.

level of protection, Article 19 of the GDPR is intended to relieve data subjects who have requested information pursuant to Article 15(1)(c) of the GDPR of the burden of sending further corresponding requests for rectification, erasure or restriction of processing to the recipients concerned. Nonetheless, the data subject must be put in a position to verify that the rectification, erasure or restriction has actually been carried out following notification by the data controller. To that end, Article 19 of the GDPR therefore provides that the data controller must inform the data subject of those recipients if the data subject requests it."[65]

65. *Derogation.* A derogation from this notification obligation could apply when the controller proves that performance of this obligation is impossible or involves a disproportionate effort[66]. The controller shall inform the data subject about those recipients if the data subject requests it[67]; article 19 GDPR does not provide for an exemption to this latter requirement.

[65] Opinion of Advocate General Pitruzzella, delivered on 9 June 2022 (Case C-154/21 RW v Österreichische Post AG (Request for a preliminary ruling from the Oberster Gerichtshof (Supreme Court, Austria)), paragraphs 31-33.
[66] Article 19 GDPR, first paragraph.
[67] Article 19 GDPR, second sentence.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

4. 2 National legal landscape

4.2.1 Introduction

4.2.1.2 The existing gap in cross-border processing of health data

There are many purposes for which data can be reused in the healthcare and genetic sector and thus the significance of the secondary use of data is increased (Martani et al, 2019). Alongside with many expected benefits of the reuse's impact, the full deployment of data in the healthcare sector also raises challenging legal, ethical and social implications (ELSI) and questions (Nuffield Council on Bioethics, 2015). A great deal of these is related to the high mobility of data that the genomic era has brought about (Brittain et al, 2017). Finding the right balance between protecting privacy and promoting beneficial use of data is particularly difficult in the case of secondary use, but it is fundamental for developing a well-functioning health data ecosystem (Iabob and Simonelli, 2020).

In light of the benefits to sharing healthcare and genomic data and the potential risks that they raise, clear and effective frameworks must be in place to enable the safe processing and management of data that preserves the privacy of individuals and enables valuable data sharing between organisations around the world (Herman, 2020). Many national and European projects and initiatives on genomic data sharing as well as public-private sectors have made considerable investments in data processing infrastructure. However, most of these efforts had as a result fragmented and overlapping investments in data management, because they are mostly independent and uncoordinated (Saunders et al, 2019; European Commission, 2021). Apart from the independency, these initiatives are mainly organised by one or a number of countries and thus differences in the context such as culture, community, health care system, legal structure, and geography are raised (Sielemann et al, 2020). For instance, across EU countries there are different data sources of health related data, different taxonomy and ontology codes to label the same condition and this makes comparisons and transferring of different datasets challenging. In order to give cross-border access to genomic data for research analyses and clinical applications, the ethical-legal standards of EU countries need to be adapted and re-designed focusing on covering a common European perspective.

Against the backdrop of an emerging EU infrastructure for healthcare and secondary use of healthcare data for scientific research purposes, the effect of divergences and further harmonisation potential across member states remains a crucial regulatory subject (Molnar-Gabor et al, 2021). Furthermore, differences in defining the appropriate safeguards, the legal basis and the derogations of data subjects rights when processing health and genetic data, especially in the context of retrospective research across EU Member States, have created an even more fragmented landscape across EU post GDPR (Tzortzatou et al, 2021). The absence of specific principles or a standardised framework that will guide the responsible sharing of genomic and health-related data is still remaining. Many countries refer to the need for the development of a common and universal ethico-legal framework that will facilitate compliance with the obligations and norms set by international and national law and policies (Branum & Wolf, 2015).

For these reasons, it is necessary to tackle the challenge of creating an integrated cross-border genome infrastructure that needs to overcome national differences. It is crucial to establish a harmonised ethico-legal framework to enable effective and responsible sharing of genomic and clinical data. This framework will be supported by policies for guidance in particular issues such as, but not limited to, ethical governance, privacy and security, and consent (Knoppers, 2014).

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

The establishment of this framework will increase international data sharing, the collaboration between different sectors, and good governance.

The initiative of a joint cross-border genome is complicated and characterised by overlaps, gaps and conflicts between EU and Member State laws and policies. It is indispensable, to establish an acceptable ELSI framework that can strengthen the secure sharing of genomics data across Europe, and bridge the above gaps. In order to tackle this challenge, in WP2 of Beyond One Million Genomes (B1MG) project, we navigated the heterogeneous ethico-legal landscapes and identified existing solutions and relevant stakeholders for input and feedback. We also focused on adapting and further developing existing ethical standards, analysing the legal landscape that affects a cross-border genome initiative and creating a pool of tools to centrally govern such infrastructure.

In order to deal with the above necessity to create an integrated cross-border genome infrastructure, we mapped the EU legal framework governing the data life cycle of a pan-European genome initiative with a specific focus on the challenges of making genomic data available across European Economic Area (EEA) countries. Specifically, we assessed how the General Data Protection Regulation (GDPR) has been implemented at national level regarding the processing of health and genetic data and thus we focused on applicable GDPR requirements for cross-border sharing, in order to assess the national derogations and divergence.

4.2.2 The goals and the implementation of the workshops

In order to collect data on national differences, four (4) workshops were organised within the B1MG project on the following subject: "Implementation of GDPR and secondary use of health and genetic data: The European countries approach". The aim of these workshops was to better understand the implementation of the GDPR and secondary use of health and genetic data in different European countries. The emerging challenges in this processing will in turn inform and contribute to the design of the best possible secondary use of data in order to develop the B1MG ethico-legal framework taxonomy. The Workshops were organised and chaired by Dr. Olga Tzortzatou, Principal Investigator on behalf of Biomedical Research Foundation of the Academy of Athens (BRFAA)- BBMRI.GR-Greece and working on WP2 of B1MG project.

In more detail, we focused on addressing issues immersing from the GDPR implementation legislation/regulations on a national level from namely the four following European regions: Nordic (Denmark, Finland, Norway, Sweden), South (Greece, Italy, Malta, Portugal, Spain), Central (Netherlands, Belgium, France, Germany) and Eastern (Estonia, Poland, Czech Republic, Latvia) European countries. The legal scholars were selected by the organiser of the workshops and the leaders of the WP2 of B1MG project. The main criteria for the selection of speakers were their expertise in the field of ELSI, health and genetic data processing in their countries. Participation was voluntary and participants were informed about the aims of the study prior to their inclusion in the workshops. Twenty (20) experts in this field in their country were invited to present a few details and examples by highlighting the current situation in their countries in order to proceed with the further development of B1MG project based on their opinions and remarks. In the Nordic and Central European countries workshops, four different speakers took part representing their country, whereas, in the South and Eastern European countries workshops, six speakers respectively were included. The countries and the speakers of the workshops are presented in Table 1 and Figure 1.

Each workshop lasted for 3 hours and each speaker had 20 minutes for the presentation and 10 minutes for questions and discussion. A 20-minute round table discussion followed after all invited speakers concluded with their presentations. The workshops took place online via Webex,

between February 2021 and February 2022. At the beginning of each workshop, all the participants consented to the video recording of the meeting.

In more detail, the workshops focused on the following issues:

- The legal basis for the secondary use of health and genetic data for scientific research purposes (art. 9 GDPR, Recital 51, 52, 53, 54 GDPR and art. 6 GDPR, Recitals 39-47, 50 GDPR).
- The ways that each national legislation system in the above countries has reacted to GDPR derogations (art. 89 GDPR, Recitals 156, 157, 159, 161 GDPR) with a particular focus on the derogations from the right to access (art. 15 GDPR, Recital 63, 64 GDPR), the right to rectification (art. 16 GDPR, Recital 65 GDPR), the right to restriction of processing (art. 18 GDPR, Recital 67 GDPR) and right to object to processing (art. 21 GDPR, Recital 69 GDPR)
- The specific safeguards in place (e.g. role of RECs etc) with particular focus on the issue of secondary use as the latest has been regulated (perhaps also by other legal instruments).
- The ethico-legal framework that is used in these countries to transfer:
  - health/genetic data within the healthcare setting
  - health/genetic data from healthcare to research setting
  - health data from the healthcare setting towards a genomic initiative
  - health/genetic data from research setting to the healthcare environment
  - health/genetic data from a genomic initiative to healthcare
- The set of legal instruments and soft law documents as well as the responsible committees/bodies, which are of relevance for the ethico-legal control and/or approval of the above mentioned data life cycle from healthcare to research settings and vice-versa.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

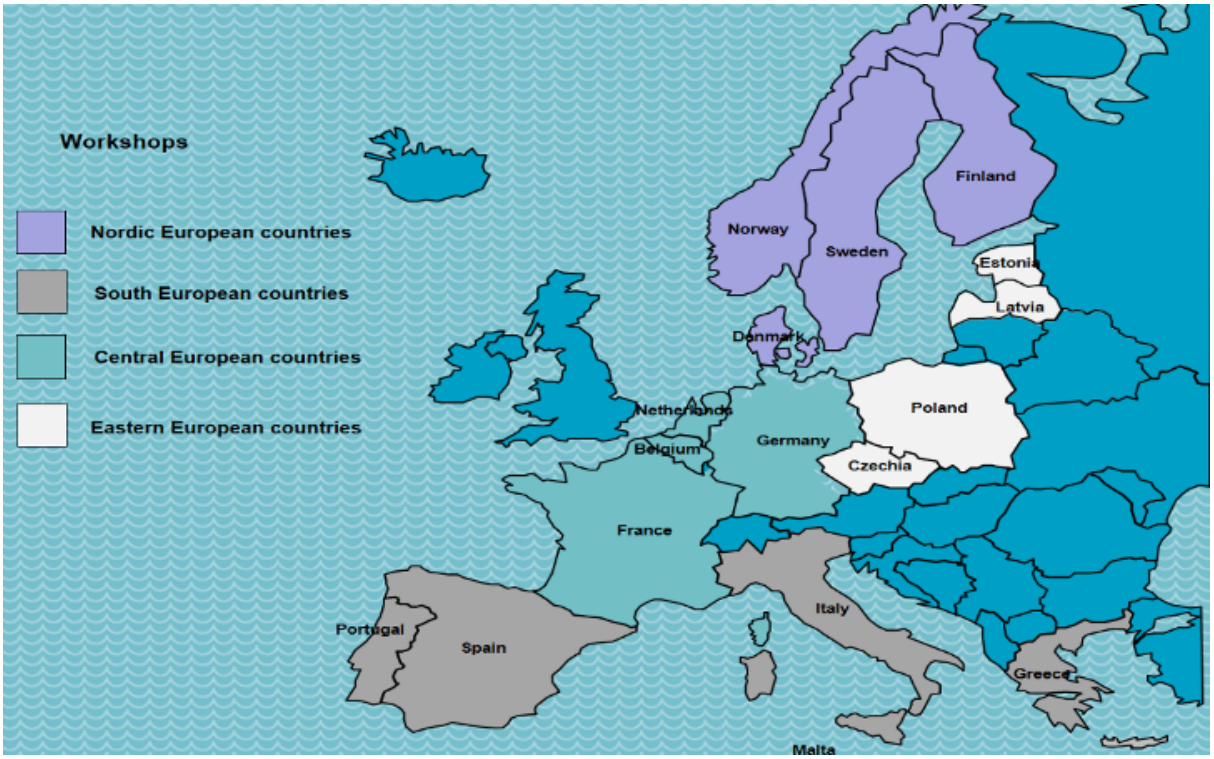

Figure 1: The participating countries in the workshops

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Table 1: The participating countries and speakers in the Workshops.

European regions	Countries	Legal scholars	Presentation's title
Nordic	Denmark	Prof. Mette Hartlev	Balancing of individual rights and research interests in Danish biobank regulation.
	Finland	Dr. Tom Southerington	GDPR implementation across Nordic countries: examples from Denmark, Finland, Norway and Sweden. GDPR implementation in Finland.
	Norway	Christine Dalebø Gjerdevik	Data Sharing during the Covid-19 Pandemic. Was Norway prepared to share health data collected for health care purposes for research purposes?
	Sweden	Prof. Jane Reichel	GDPR implementation in Sweden.
South	Greece	Dr. Olga Tzortzatou	Secondary use of health and genetic data under Greek legislation – GDPR implementation.
	Italy	Prof. Marialuisa Lavitrano Dr. Matteo Macilotti	B1MG - GDPR Implementation across South European countries research.
	Malta	Dr. Ruth Vella Falzon	Implementation of GDPR and secondary use of health and genetic data: The South European countries approach.
	Portugal	Prof. Carla Barbosa	The Portuguese Legal Framework for Research Activity – health data, biobanks, and reuse (secondary use) of data.
	Spain	Prof. Aliuska Duardo	The use of health-related data in scientific research: Impact of the GDPR on Spanish legislation.
Central	Netherlands	Dr. Susanne Rebers	The use of health/genetic data for research and health care in the Netherlands.
	Belgium	Teodora Lalova	Secondary use of health data for scientific research in Belgium.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

	France	Gauthier Chassang	French law, GDPR safeguards and derogations for the reuse of personal data in research.
	Germany	Dr. Fruzsina Molnár-Gábor	Implementation of GDPR and secondary use of health and genetic data: The Central European countries approach.
Eastern	Poland	Dorota Krekora- Zajac	Polish code of conduct for processing personal data for biobanks and secondary use of data.
	Czech Republic	Radek Halouzka	Secondary processing of health data: The Czech Legal Perspective.
		Jan Kuráň	
	Latvia	Santa Slokenberga	Primary and secondary use of health and genetic data for scientific research in Latvia.
		Signe Mežinska	
	Estonia	Silja Elunurm	Secondary Processing of Health and Genomic Data: The Estonian Legal Perspective.

4.2.3 The workshops

All legal scholars analysed the way GDPR was implemented in their countries with a focus on the secondary processing of health and genetic data. This section summarises the key points of the presentations of the 20 legal scholars of each workshop. The initial presentations can be found in B1MG common file https://drive.google.com/drive/folders/1vZguFmvDvYBxvsswTXxs2R2vp9RD__8F.

4.2.3.1 Nordic Countries workshop main points and outcomes

Date: 5th of February 2021

Speakers: Prof. Mette Hartlev (Denmark), Dr. Tom Southerington (Finland), Christine Dalebø, Gjerdevik (Norway), Prof. Jane Reichel (Sweden)

In ***Denmark,*** there is an unknown number of biobanks (clinical, research, donor, commercial) which differ by size, category and location. The legal framework governing biobanks is articulated in three Acts. First, the Health Act includes a number of patients' rights. According to the Health Act, informed consent is necessary for the collection of samples. It has specific provisions on self-determination regarding the retrieval and destruction of data, while it also establishes a right to opt out for non-treatment related use of samples. Second, the Danish Data Protection Act, which implements GDPR, applies in all parts of processing samples and has a specific provision covering the use of data (including samples), for research purposes. Section 10.1 stipulates that data mentioned in art. 9(1) and 10 GDPR, may be processed where the processing takes place for the sole purpose of carrying out statistical or scientific studies of significant importance to society and where such processing is necessary in order to carry out these studies. This provision applies also to tissues. Section 10.2-4 provides a list of specific safeguards, which mostly concern the

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

further use. The main rule is that these data are not to be subsequently processed for any purpose other than scientific or statistical purposes. Also, the disclosure of data to third parties requires a prior authorization from the supervisory authority when the disclosure 1) relates to data that will be processed outside the territorial scope of GDPR, 2) relates to biological material or it is made for the purpose of publication in a recognised scientific journal or similar (Section 10.3 Danish Data Protection Act). The supervisory authority may lay down general terms for the disclosure of data (Section 10.4 Danish Data Protection Act). Third, the Act on Research Ethics Review of Health Research Projects applies when samples of research participants are collected, requiring their informed consent.

This Act has also specific provisions for cases where someone can conduct their research on tissue samples from biobanks (biobank research) without having research participants included. Such research also needs REC authorisation. Although normally it would be necessary to obtain the informed consent of the donor, it is possible to derogate from this requirement in case there are no health risks or burden affiliated with the research project or it is impossible or disproportionately difficult to obtain informed consent. Usually, the derogation prevails, but in cases of very comprehensive genetic analysis and very sensitive issues, the REC would in some situations refuse to derogate, in which case researchers will need to go back and obtain the donor's consent. Data subjects may opt-out of the use of samples from clinical biobanks, in contrast to samples from research biobanks. The research that is based on tissue samples collected directly from research participants needs both informed consent and REC authorisation.

The Danish legislation enables the easy transfer of data and tissue samples from clinical to research settings. Generally, there are no consent requests. There are some opt-out options for use of tissue samples taken in a clinical situation, and this option also applies to genetic data, which should be stored in the National Genome Centre (Section 29 Health Act). It is necessary to obtain REC approval for research on tissue samples and a few selected data. In the context of transferring data and tissue samples from research to clinical settings, the main rule is that it is prohibited (Section 10 Danish Data Protection Act). However, there are some derogations from the prohibition, including situations of secondary findings, especially with genetic research, and exceptional cases of life threatening or serious, infectious diseases. Feeding back is also possible for supporting clinical assessment and decisions. This applies in situations where clinical assessment of a specific patient can profit from information about other patients (Section 42a.6 Health Act).

Research that is based exclusively on personal data (including health data and genetic data) will normally not need consent from the data subject or authorisation from REC. However, according to the new legislation (section 21a-21b Act on Research Ethics Review of Health Research projects), REC authorisation is required for data-based research projects generating risks of secondary findings. The more specific conditions regarding the obligation to report the secondary findings to patients are laid down in the executive order no 965 of 21 May 2021. Additionally, in an effort to facilitate research, there are derogations from all data subject rights laid down in GDPR.

In ***Finland***, the Finnish Data Protection Act (2018) complements GDPR. Section 4 of the Finish Data Protection Act stipulates that the processing of personal data is lawful under art. 6(1) e GDPR, when it is necessary for scientific research purposes and proportionate to the aim of public interest pursued. Section 6 of the Finish Data Protection Act provides that the prohibition of processing special categories of personal data under 9(1) GDPR, does not apply if the data are processed for scientific research purposes. Although not specifically mentioned in the Act, this provision is based on art. 9(2)j GDPR. When special categories of data are processed, the data controller and data processor must take suitable and specific measures to safeguard the data subject rights. In that respect, the Finnish Data Protection Act provides a list of 11 specific safeguard examples, adopting a risk-based approach. Section 31 of the Finnish Data Protection

Act prescribes some derogations from data subject rights, namely right of access (art. 15 GDPR), right to rectification (art. 16 GDPR), right to restriction of processing (art. 18 GDPR) and right to objection (art. 21 GDPR), when personal data are processed for scientific research purposes. These rights can be derogated when needed if three requirements are fulfilled; 1) the processing is based on an appropriate research plan, 2) a person or group responsible for the research has been designated, 3) personal data are processed only for scientific research purposes or other compatible purposes and the data about a given individual are not revealed to outsiders. There are further requirements for the special categories of data, such as conducting a Data Protection Impact Assessment (DPIA) and providing the results to the supervisory authority or complying with GDPR compatible codes of conduct. In Finland, there is a sector-specific legislation governing access to health data for secondary purposes, including the Act on the Secondary Use of Health and Social Care Data (2019), and the Biobank Act (2012). A Genome Act is under drafting and might in the future affect the use of genetic data for research purposes. The Act on the Secondary Use of Health and Social Care Data applies to scientific research among several other purposes. From an ethics point of view, there is neither an obligation for securing consent, nor an obligation to actively inform the data subject or obligation to publish the results. While social and health care data have been widely available for research already earlier, the Act created a centralised permission procedure and established a new permissions authority (Findata), which is competent in cases where data from several data from public social or health care providers (data controllers) or from private social and health care providers are needed. One of the security measures provided under the Act is that the data, except for anonymous aggregated statistical data, are only available to processing environments, whose security is confirmed by approved investigation bodies, primarily Findata's own environment. The Act also prescribes the process of returning incidental findings through health care, providing the possibility of opting not to know.

The Biobank Act covers biological samples governed by the biobank and related data. Consent is not considered a legal basis for the processing of personal data, but rather as a safeguard. This is something that is expected to be clarified in the new Biobank Act that is currently being drafted. The legal bases for processing special categories of personal data are in the Biobank Act itself and based on important public interest. Donors have broad rights, including the right to get health-related results analysed from their samples and receive an explanation of their significance. The Biobank Act provides safeguards, such as the requirement of a material transfer agreement or data transfer agreement and pseudonymization. Identifiers can be processed if it is needed eg. to combine other data to biobank material. Additionally, the Genome Act, that is currently being drafted, may establish another data-type-specific public authority to advise on, collect and control the use of genetic data.

In Finland, the professional secrecy rules concerning patient records seem to block using one patient's information for the benefit of another. Changes to the rules are in drafting, but the draft proposal seems to confirm this. It seems that this issue may be touched upon in the next phase of renewing the rules.

In ***Norway***, a new Personal Data Act which incorporates GDPR into Norwegian legislation was adopted by the Parliament in June 2018, and took effect on 20 July 2020. It did not bring substantial changes to existing laws, which include the Health Registries Act and the Act on Medical and Health Research (Health Research Act).

One of the main changes brought by GDPR for the secondary use of health data, is the non-requirement of the supervisory authority's pre-approval for processing sensitive personal data for secondary use. Also, a pre-approval from REC does not constitute a condition for processing sensitive personal data in health research. However, the REC's ethical assessment remains unchanged.

In Norway, the legal basis for processing health data for research purposes will vary according to the source from which the data are collected. In the context of health data from patient records or health registries, the legal basis for the processing will lie on the administrative decision on exception from the rule of professional secrecy made by the REC (para 29 Act on Health Care Professionals). This was expected to change in summer 2021, where a National Service for Health Data would be established, and would be competent to assess all the applications for data coming from patient records and health registries. In that case, the REC will only be competent for the ethical assessment. In the context of health data from National Health Registries, the legal basis for the processing is the Section 20 in the Personal Health Data Registries Act which constitutes the legal basis for processing indirectly identifiable health data in case of derogation from professional secrecy. If the data are collected from other sources, then the legal basis is found in para 9 of the Personal Data Act which requires that the processing must take place in accordance with art. 89 GDPR and that a Data Protection Officer (DPO) consultation must precede. If health data are processed for purposes other than research related ones, e.g. improving the quality of healthcare, health analysis and administrative purposes, there is no big change in the legal basis. The only thing that changes is the actor that makes the decision on the exception from professional secrecy, that is the Director of Health in this case. However, this was expected to change in summer 2021 with the national service data.

Norway has not included a list of specific safeguards in Norwegian law. The reason why is that the Ministry of Justice and Public Security has interpreted art. 89 GDPR as a duty of the controller and not one of the national authorities. Another reason is that the safeguards could change with the new technical measures. However, this does not entail that there are no safeguards. Indicatively, some safeguards include the prior consultation with the DPO before the decision for exception from professional secrecy, requirements for encryption of directly identifiable data in health registries etc. Also, derogations from rights to access (art. 15 GDPR), right to rectification (art. 16 GDPR) and right to restriction (art. 18 GDPR) are implemented under certain conditions (para 17 Personal Data Act). The derogations do not apply if the processing has legal effects or direct actual effects for the data subjects.

Health data can be disclosed from the patient record only if the patient consents or if there is an administrative decision for exception from the rule of professional secrecy, or if there is a legal basis in law. For other secondary use of health data (not research purposes), the legal authorities are following the same process according to the national health registries.

Research biobanks have their legal basis on the Health Research Act and have to be approved by the REC. There is a proposal on interpreted genetic variants and the proposition for the act was expected to take place in June 2021.

As far as the research on Covid-19 is concerned, the four regional RECs set up a fast-track system for research on Covid-19. In most of the projects, consent is the legal basis, as they also collect biological material from the patients. If it is not possible to take the patient's consent or the next of kin's consent, research can be conducted only upon fulfilment of strict conditions laid down in the Health Research Act (para 19). All biobanks require approval from REC.

Sweden has a long tradition of access to official documents and population based registries. Access to official documents can only be limited by the Public Access to Information and Secrecy Act (PAISA), not by GDPR. Specifically, on the access to health and genetic data in research, ethical approval is a condition for, but not a guarantee according to PAISA. Generally, health data are confidential. However, their release can only be possible if it is clear that the information can be disclosed without harm to the individual or someone close to them (Chapter 25(1) PAISA). Information may be disclosed with reservations: confidentiality, pseudonymization etc (Chapter 10(14) PAISA) and individuals may waive confidentiality (Chapter 12(2) PAISA). For private health care institutions, confidentiality is regulated in the Patient data Act and the Patient Security Act. As far as the secondary use of health and genetic data in research is concerned, the public

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

interest is the default legal ground for processing personal data in publicly-run research ((art. 6(1)e and art. 9 GDPR), but it can also be the legitimate interest in case of private research institutions (art. 6(1)f GDPR). With regard to art. 89 GDPR and the safeguards provided therein, ethical approval is required for every research on sensitive data, regardless of where these are collected (Section 6 Ethical Review Act). Consent is normally required by REC as an additional safeguard, but it may be waived in individual cases, if the risk of privacy intrusion is considered low.

In Sweden, there is no specific legislation on derogations from the exercise of data subjects' rights in the context of research. According to the preparatory work though, GDPR exceptions should be directly used. With regard to the secondary use of health and genetic data for other purposes, the Patient Data Act provides a legal basis for processing personal data in public and private health care and national quality registries. The permitted purposes are the patient's own health care, administration, statistics, national quality registries, etc (Chapter 2(4) Patient Data Act). In regards to the care of patients other than the data subject, informed consent would be needed. There is a separate section prescribing that other purposes require explicit informed consent (Chapter 2(3) Patient Data Act). In the context of biobanks, there is no possibility to waive the consent of person providing a sample, which is needed for storing and further use. This may hinder the research.

4.2.3.2 South European Countries workshop main points and outcomes

Date: 26th May 2021 Speakers: Dr. Olga Tzortzatou (Greece), Prof. Marialuisa Lavitrano and Dr. Matteo Macilotti (Italy), Dr. Ruth Vella Falzon (Malta), Prof. Carla Barbosa (Portugal), Prof. Aliuska Duardo (Spain)

In ***Greece***, there is a set of laws for regulating health data processing for research and healthcare, the most important being Law 2619/1998 ratifying the Oviedo Convention, the Code of Medical Ethics/Deontology (Law 3418/2005) and more specifically art. 24(2)d requiring that the research project is approved by the competent administrative authority, following a favourable opinion of the competent Scientific Council of the hospital and/or the Ethics Committee, the Regulation (EU) No 536/2014 on clinical trials of medicinal products for human use, the Ministerial Decision DYG 3/89292/2003 implementing Directive 2001/20/EC, Law 4386/2016 on Regulations for Research and other provisions, regulating administrative aspects of research, as well as the data protection legislation, that includes some provisions of pre GDPR Law 2472/1997 and Law 4624/2019, which transposed GDPR in the Greek legislation.

The most significant change brought by Law 4624/2019 is that the pre-approval from the Hellenic Data Protection Authority for processing sensitive personal data is no longer necessary. Also, Law 4624/2019 provides that the data controller must anonymise the data as soon as scientific or statistical purposes permit so, unless this is contrary to the data subject's legitimate interest (art. 30(3) Law 4624/2019). The Greek law provides an additional safeguard according to which, until anonymisation takes place, features that can be used to correlate details of personal or actual situations of an identified or identifiable individual must be stored separately.

Additionally, Law 4624/2019 has introduced a number of extra safeguards including among others, the pseudonymization and encryption of personal data, the appointment of DPO, measures to increase awareness of the staff and measures to ensure the capacity, confidentiality, integrity, availability and durability of processing systems and services related to the processing of personal data, including the ability to quickly restore availability and access in the event of a physical or technical incident.

In regards to the processing of genetic data, there is no specific genetic data legislation per se in Greece. Art. 23 Law 4624/2019 strictly prohibits the processing of genetic data for health and life insurance purposes pursuant to art. 9(4) GDPR, unless the data subject gives their informed consent.

With regard to the secondary processing of health data for other purposes, art. 22(2) Law 4624/2019 provides that public authorities may process health and genetic data for other purposes than that originally collected if it is necessary for the public interest given that one of the art. 9(2) GDPR legal bases applies. Also, art. 26 Law 4624/2019 enables the transfer of health data from public entities to private ones, under the above conditions.

Informed consent is still the main legal basis for processing health data for research, even in the case of pandemic. The Greek law allows derogations from data subject rights, namely the right to access (art. 15 GDPR), the right to rectification (art. 16 GDPR), the right to restriction of processing (art. 18 GDPR) and the right to object (art. 21 GDPR) in accordance with art. 89(2) GDPR. The derogations are allowed on condition that exercising these rights may render impossible or seriously impair the purposes of scientific or historical research. In the absence of specific guidelines, the assessment of whether the exercise of rights seriously impairs the purposes of scientific research is quite challenging and burdens the REC.

In Greece, there is no legislation specifically prescribing the use of one patient's health data for the healthcare of another patient. It can take place on a case by case basis, on condition that consent has been granted.

In ***Italy***, the legal framework on the use of samples and personal data for hospital-based biobanking for research consists of GDPR, the Legislative Decree no 196/2003 on the implementation of internal rules to GPPR (as modified by Legislative Decree no 101/2018) and the Provision of the Italian Privacy Authority no 146/2019.

In Italy, informed consent is the general legal basis for research on health and genetic data and samples even in medical research. Art. 110 of the Legislative Decree 196/2003 introduces exceptions to the rule of informed consent for scientific research purposes in the medical, biomedical or epidemiological sphere. In particular, according to art. 110(1), the consent of the data subject is not necessary when the research is carried out based on provisions of law or regulation or the law of the European Union in accordance with art. 9(2)j GDPR, including the case in which the research is part of a biomedical or health research program regulated by art. 12-bis of the Legislative Decree no 502/1992 (Italian National Plan of Research), and a DPIA is conducted and made public pursuant to art. 35 and 36 GDPR. According to art. 110bis (1) of the Legislative Decree 196/2003, consent is also not necessary when, due to particular reasons, informing the data subject is impossible or involves a disproportionate effort, or it can make it impossible or seriously affect the achievement of the purposes of the research (eg. large number of participants). In such cases, the data controller takes appropriate measures to protect the rights, freedoms and legitimate interests of the interested part in accordance with art. 89(2) GDPR. The research program is subject to the favourable opinion of the local ethical committee and the prior consultation of the Italian Privacy Authority in accordance with Article 36 GDPR. According to art. 110bis (2), the Italian Privacy Authority communicates the decision on the request for authorisation within forty-five days, after which failure to pronounce equals to rejection. Together with the authorisation provision or even subsequently, the Italian Privacy Authority establishes the conditions and measures necessary to ensure adequate guarantees for the protection of data subjects in the context of further processing of personal data by third parties.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Another exception to the rule of consent is that the processing of health and genetic data by the Scientific Institutes for Research, Hospitalisation and HealthCare (IRCCS) does not constitute further processing by third parties. This exception takes effect in case of hospitals that have a dual aim, namely providing healthcare and conducting research. In that case, they can use the data that they collected in the care process for research purposes without the patient's consent (art. 110 bis(4) Legislative Decree 196/2003).

There are also specific requirements relating to the further processing of health and genetic data for scientific research purposes according to the Provision of the Italian Privacy Authority, no 146/2019. According to art. 4(5), informed consent is the general rule, but there are some exceptions. More specifically, the biological samples and the genetic data collected for health protection purposes can be stored and used for scientific or statistical research purposes without the patients' consent in case a) of statistical surveys or scientific research provided for by European Union law, by national law or, in the cases provided for by law, by regulation or b) when the scope is limited to the pursuit of further scientific and statistical purposes directly connected with those for which the informed consent of the interested parties was originally acquired (art. 4(11)3 Provision of the Italian Privacy Authority, no 146/2019). Other exceptions cover cases where despite all reasonable efforts, consent could not be obtained for the conservation and further use of biological samples and genetic data for research programs other than the original one, on condition that the further processing does not allow the identification of data subjects or the research program has received a prior favourable opinion by the local Ethics Committee and is subjected to prior consultation with the Italian Privacy Authority in accordance with art. 36 GDPR.

With regard to health data, the rules are less strict. Consent is not necessary when the research is carried out on the basis of legal or regulatory provisions or European Union law (art. 5(3) Provision of the Italian Privacy Authority, no 146/2019). In other cases, when it is not possible to obtain consent, the data controllers in the research project must document the existence of exceptional reasons for which informing the interested parties is impossible or involve a disproportionate effort, or risks making it impossible or seriously jeopardising the achievement of the purposes of the research. The reasons can be: 1) ethical, where the interested party ignores their condition and the revelation of information could cause material or psychological damage, 2) organisational, where the non-inclusion of the interested parties who cannot be contacted would have serious repercussions on the study, including alteration of the results, 3) health-related, where the seriousness of the interested party's clinical state renders them unable to understand the given information and give valid consent.

In Italy it is possible to use one patient's health data for the healthcare of another person without the consent of the patient, but only for healthcare reasons. In that case, security measures must be respected.

In ***Malta***, apart from GDPR, which has been transposed into Maltese law by means of the Data Protection Act, there are no specific laws regulating research, except for some references in the Clinical Trial Regulation and laws regulating higher education and health.

Consent is the legal basis for the processing of personal data for research purposes. Despite the possibility of derogations for research purposes, Malta refrained from prescribing further derogations in the Data Protection Act. Also, there are no changes to the national data protection legislation governing the processing of special categories of data in the field of scientific research. The Act prescribes further obligations for data controllers and rights of data subjects when derogations from the data subjects' rights occur. It provides that processing for scientific or historical research purposes shall be subject to appropriate safeguards for data subjects' rights

and freedoms, including pseudonymization and other technical and organisational measures, to ensure respect for the principle of data minimization. Controllers must consult with and obtain prior authorization from the Office of the Information and Data Protection Commissioner (IDPC) when they intend to process genetic data, biometric data, or data concerning health for statistical or research purposes in the public interest. The Commissioner must, in turn, consult with a REC.

Malta enacted the secondary processing (health sector) regulations on the 8th of October 2019. With regard to the processing for scientific research purposes, personal data may be processed where the research activities are in the public interest. Where such processing cannot be conducted using anonymised data, it is only permissible under specific conditions. In particular, in the case of research activity conducted by the Ministry of Health or its partners, such research can be carried out upon the approval of the Health Ethics Committee within the Ministry of Health and after obtaining prior authorisation from the IDPC. In the case of research activity conducted by academics or students or NGOs having the remit to assist patients in need in the health sector, such research can be carried out following approval of any other ethics committee and after obtaining prior authorisation by the IDPC. In such cases, personal data must be pseudonymised, however, if this is also not possible, appropriate measures should be taken to safeguard the rights and freedoms of data subjects by ensuring that the personal data are anonymised as soon as it is no longer required to be identifiable for the purpose of carrying out research or statistical studies. Also, no specific derogations for rights to access (art. 15 GDPR), right to rectification (art. 16 GDPR) and right to restriction of processing (art. 18 GDPR) are included.

A research team from the Centre for Molecular Medicine and Biobanking at the University of Malta has created a blockchain solution for dynamic consent in biobanking called Dwarna, which acts as a hub connecting the different stakeholders of the Malta Biobank: biobank managers, researchers, research partners, and the general public. The portal stores research partners' consent in a blockchain to create an immutable audit trail of research partners' consent changes.

Moreover, the Maltese Government has set up an ad-hoc task force to propose a regulatory framework for biobanks in Malta which is in progress. This is considered to be an important step, as there is no Biobank Act in place in Malta at the moment.

As a final note, the Maltese law is silent on the use of health data of one patient for the healthcare of another patient.

In ***Portugal***, Law 12/2005 limits the establishment of biobanks to the purposes of healthcare provision or applied health research. Law 58/2019 is the law that implements GDPR in the Portuguese legal framework. Although Law 58/2019 does not specifically refer to the protection of personal data in the context of scientific research, it provides that the processing of data, in this case, should comply with the data minimization principle, and anonymization or pseudonymization should be sought, provided that the objectives can be achieved. Also, according to art. 31(2) Law 58/2019, the rights to access (art. 15 GDPR), rectification (art. 16 GDPR), restriction of processing (art. 18 GDPR) and object (art. 21 GPDR) can be derogated from when their exercise is impossible. The national law states that the general rules on consent, as provided in GDPR, also apply to the processing in the context of scientific research considering that consent may cover several research areas, and the ethical standards must be complied with. It is noted that Portuguese law does not make any distinction between public and private sector.

Art. 31 Law 58/2019 provides that the further processing for scientific research purposes is not considered to be incompatible to the initial purpose in accordance with art. 89(1) GDPR. Also, taking example from art. 5(1)e GDPR, the storage of data for longer periods is allowed on

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

condition that appropriate technical and organisational measures to safeguard the rights and freedoms of the data subjects are in place.

Law 58/2019 does not establish any additional rules with regard to the processing of special categories of data, such as genetic data. The rules provided in Law 12/2005 continue to apply.

The Portuguese national law also does not have specific provisions on the reuse of data. However, Deliberation 227/2007 of the National Data Protection Commission is still relevant. When it comes to the retrospective scientific investigation of health information extracted from personal data other than samples (e.g. clinical records), in the absence of consent under the terms indicated, the data controller must carefully weigh whether to grant authorization for the processing of personal data or not. In these cases, it is necessary to obtain a REC favourable opinion, in the lack of which there can be no authorization for reuse.

According to art. 19(6) Law 12/2005, in the case of retrospective use of samples or in special situations, it must be fully detailed and demonstrated why it is impossible to obtain consent. Also, the public interest of the study or research in question must be unequivocally demonstrated and pursued immediately and directly by the result of the investigation.

The use of one patient's health data for the healthcare of another is partially covered by Law 12/2005. More specifically, in special circumstances, where the information may have relevance for the treatment or prevention of the recurrence of a disease in the family, that information may be processed and used in the context of genetic counselling, even if it is no longer possible to obtain the informed consent of the person to whom it belongs (art. 18(6) Law 12/2005). All relatives in direct line of ascent or descent, as well as second degree relatives, can have access to a stored sample of genetic material, provided that it is necessary to obtain a better knowledge of their own genetic status (art. 18(7) Law 12/2005). However, this provision does not allow them to know the genetic status of the person to whom the sample pertains or of other family members.

In ***Spain***, the applicable regulatory framework for the use of health-related data in research includes art. 44(2) of the Spanish Constitution, the Organic Act 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (Spanish Data Protection Act), which transposed GDPR in Spain, the Act 14/2007 on Biomedical Research, the Act 14/1986 on general health, the Act 41/2002, which is the basic law regulating patient autonomy and rights and obligations regarding clinical information and documentation as well as the Royal Decree (RD) 1716/2011, which established the basic requirements for biobanking. GDPR did not alter the regulatory framework in force in Spain in relation to the processing of data in the context of biomedical research. Such data continue to be processed under the terms established in the Biomedical Research Act.

There are parts in the Spanish Data Protection Act that are specifically linked to the use of personal data in the context of research. Except for the additional provision 17 on the processing of health data, the Act includes some additional parts specifically linked to the use of personal data for research. According to additional provision 17 of the Spanish Data Protection Act, the legal basis for processing health-related data in the context of research is reflected in the provisions of art. 9(2) GDPR, including consent (art. 9(2)a GDPR), reasons of public interest in the field of public health (art. 9(2)i GDPR), archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (art. 9(2)j GDPR) and reasons of essential public interest (art. 9(2)g GDPR). As far as consent is concerned, it can be broad, meaning that it may not be limited to specific research. Research can be implemented without consent for public interest in the field of public health. This provision applies only in cases where the research is carried out by the health authorities and public institutions competent in public health matters and only in extraordinary situations, of special relevance and seriousness. Also, it is possible to

proceed with the use of pseudonymised personal data for research without obtaining the consent of the data subject, provided that appropriate technical measures are implemented to prevent the re-identification of the source subject. In that respect, it is necessary to obtain a prior favourable opinion by the competent REC (art. 2(g) additional provision 17 Spanish Data Protection Act).

In the context of secondary use of data, art. 2(c) of the additional provision 17 of the Spanish Data Protection Act provides that the processing of data for health or biomedical research purposes is considered to be compatible when the latter are relevant to the area of study for which the data were initially collected and for which consent has been granted. Spanish authorities have chosen to use Article 9(4) GDPR by introducing a limitation to the processing of genetic data or data relating to health. The secondary use of data is only possible when the corresponding REC issues a prior favourable report.

When personal data are processed for health research purposes, and in particular biomedical research, for the purposes of art. 89(2) GDPR, the rights of data subjects provided for in art. 15, 16, 18 and 21 GDPR may be waived only under 3 specific conditions: a) the aforementioned rights are exercised directly against researchers or research centres that use anonymised or pseudonymised data; b) the exercise of these rights refers to the results of the research; and c) the research is in the essential public interest related to state security, defence, public safety or other important objectives of general public interest, provided that in the latter case the exception is expressly provided for by regulation with the status of a law (art. 2(e) additional provision 17 Data Protection Act).

Finally, when processing is carried out for public health research purposes and, in particular, for biomedical research purposes, it will be compulsory: 1) to conduct a DPIA, 2) to apply the quality standards and, where appropriate, international guidelines on good clinical practice, 3) to adopt measures aimed at ensuring that researchers do not access data that identify the data subjects, and 4) in the case of clinical trials, to designate a legal representative established in the EU, in accordance with Article 74 of Regulation (EU) 536/2014 if the sponsor of a clinical trial is not established in the EU (art. 2(f) additional Provision 17 Spanish Data Protection Act). Also, a prior report of REC is necessary (art. 2(g) additional provision 17 Spanish Data Protection Act). In the absence of REC, the Data Protection Officer can issue this report.

4.2.3.3 Central European Countries workshop main points and outcomes

Date: 19th of November 2021

Speakers: Dr. Susanne Rebers (Netherlands), Teodora Lalova (Belgium), Gauthier Chassang (France), Dr. Fruzsina Molnár-Gábor (Germany)

In ***the Netherlands***, the relevant framework for the processing of health and genetic data for healthcare includes the Medical Treatment Agreement Act (1994) and other relevant legislation like the Dutch implementation law to GDPR and the Act of additional provisions for the processing of personal data in healthcare. There is a need to obtain informed consent to transfer health and genetic data for the healthcare of other patients. The same applies in the case of the transfer of health and genetic data from healthcare to a genomic initiative for healthcare use.

In the processing of data for research purposes, there is a Specific Act for trials, which concerns the most invasive research. Although there is no specific Act for observational research, some more general laws apply, including the Medical Treatment Agreement Act. According to the latter, in the context of processing identifiable data for research purposes, consent is a standard procedure, although an opt-out procedure is considered sufficient when consent cannot reasonably be requested or when asking consent is not reasonably possible and when certain

requirements are met, such that the research contributes to the general interest, the research is not possible without these personal data and the patient concerned has not expressly objected (art. 458 Medical Treatment Agreement Act BW7). In this context, informed consent is generally seen as 'ethical informed consent' as it does not fulfil the requirements of GDPR consent.

Given the lack of clarity, there is a Code of Conduct 2004 which had been adopted by hospitals and approved by the DPO based on the predecessor law of GDPR. It prescribes informed consent, unless it cannot reasonably be requested or when it is not reasonably possible. In practice, this means that hospitals use an opt-out procedure for large scale data, and it is up to each hospital whether the patients are sufficiently informed or not. A new Code of Conduct has been recently published. This Code of Conduct has a layered consent system for the re-use of health data. It acknowledges that GDPR consent may be deemed impossible in practice because of the demand for specificity, and in that case, hospitals can use the ethical consent concept based on the Medical Treatment Agreement Act. If consent cannot be reasonably requested or it is not reasonably possible to ask consent, there is an opt-out procedure. Also, according to the new Code of Conduct, 'separate' consent is needed for re-use of genetic data. In the Netherlands, there is a disagreement on whether reuse of genetic/genomic data can fall under broad consent.

There is also a new law for biosamples that is under discussion. This new law will require GDPR consent for research. For genetic data, it will require specific consent while additional provisions will prescribe whether a separate consent will be needed too. Generally, there is ongoing lobbying for a sectoral law that will cover both data and biosamples.

With regard to the use of one patient's health data for the healthcare of another patient, currently there is no such provision in the Dutch legal framework.

Belgium adopted the Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data, which transposed GDPR in the Belgian legal framework. In the biobanking field, the applicable framework includes the Law of 19 December 2008 on obtaining and using human body material (HBM) for human medical applications or scientific research purposes, the Royal Decree on biobanks of 9 January 2018, the Law of 30 October 2018 modifying the Law of 19 December 2008 as well as the Compendium on biobanks (20.07.2018), which was published by the Federal Agency for Medicines and Health Products (FAMHP) and will be adapted in the near future. An adaptation of the Belgian biobank law was recently approved (8 March 2022). The main changes are in the definition of biobank, the definition of transformation by artificial material and extracted material, and the exclusion of certain aspects of the law for artificial material and extracted material.

In the context of the primary use of personal data and HBM, the Belgian Biobank law is also applicable as it covers associated data too, e.g., personal data associated with tissues. The data protection framework and the biobank framework always apply together.

When it comes to the secondary use of data in Belgium, personal data can be further processed as far as the further processing is not incompatible with the original purpose (art. 5(1)b GDPR), on condition that there is consent, a provision under European Union or Member State law, a compatibility test assessment has been conducted (art. 6(4) GDPR) or there is a presumption of compatibility. Also, according to the Belgian Biobank Law, any re-use of HBM requires consent, understood here as the ethical requirement for consent, not as a legal basis under the GDPR. In case it is impossible to seek consent, or such a request would be exceptionally inappropriate, a positive opinion of an ethics committee is necessary (art. 20(1) Law of 2008 on HBM). In the context of the use of residual HBM for research purposes, consent is presumed unless the donor has announced their refusal prior to any operation with the material (art. 20(2)1 and Art. 20(1) in conjunction with Art. 4(1)1 Law of 2008 on HBM).

Pursuant to art. 89(2) GDPR, Belgium allows the derogation from the right of access (art. 15 GDPR), the right to rectification (art. 16 GDPR), the right to restriction of processing (art. 18 GDPR)

and the right to objection (art. 21) when it comes to processing of data for research purposes, subject to conditions and safeguards. The Belgian law divides the safeguards into those that are applied generally, both in the context of primary and secondary use, those that apply only when the data are directly collected from the data subject and those that apply only in the context of further processing. General safeguards include the designation of a DPO and addition of new elements to the record of processing activities (justification for the use of data, reasons why the exercise of data subject rights would make the scientific research impossible to achieve or would seriously hinder it and DPIA when processing sensitive data) (art. 190-191, 204 Law of 30 July 2018). When data are collected directly from the data subject, there is an additional information obligation to inform the data subject whether the data will be anonymized or not and explain the reasons why the exercise of the rights by the data subject is likely to make the achievement of the scientific research purposes impossible or seriously hinder it (art. 193 Law of 30 July 2018).

In the context of further processing of data, there is a plethora of obligations (art. 197 Law of 30 July 2018). The general rule is that only anonymous data should be used. If it is not possible to achieve the research purpose by processing anonymous data, then the data should be pseudonymised. Even if in that case too it is impossible to achieve the research purpose, non-pseudonymised data can be used. Also, there are additional safeguards when the data are shared with a new controller, including an obligation to sign an agreement with the original controller and more specific rules on anonymisation and pseudonymisation of data (art. 194-195, 198-203 Law of 30 July 2018).

There is no special provision in the Belgian legal framework regulating the use of one patient's health data for the healthcare of another patient.

In ***France***, the entry into force of GDPR led to the modification of the Data Protection Act, "Loi Informatique et Libertés" (LIL) in 2018 and 2019. The provisions of LIL on the processing of data of health research are further specified by the National Commission for Information Technology and Liberties (CNIL) methodologies of reference (MR) (CNIL deliberations) for each health research type defined by French health law. The applicable framework also includes provisions in the Public Health Code, the Civil Code and the Penal Code.

In the French legal landscape, health research is divided into two categories according to a risk-based approach; the research involving the human person (prospective health research) and the research not involving the human person (retrospective health research). However, whatever the type of research, personal data protection is a common obligation that must be met before, during and after the research.

By reference to art. 9 GDPR, data controllers can rely on the necessity for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (art.9(2)(j) GDPR) or consent (art. 9(2)a GDPR), which is not though preferred due to the constraints it implies. The LIL specifies that personal data processing in health research may be implemented only for public interest purposes, such as ensuring high standards of quality and safety of healthcare and medicinal products or medical devices (art. 66(I) LIL).

The safeguards for data subjects are distinguished into State-level and data controller and processor-levels safeguards. On the State level, RECs, namely the Committees of Protection of Persons (CPP) and the Ethics and Scientific Committee for Research, Studies and Evaluations in the field of Health (CESREES) as well as CNIL experts are involved, depending on the legal qualification of the research project for assessing and approving projects involving personal data processing. In the data controller and processor level, the safeguards take reference from art. 89(1) GDPR and include both organisational and technical safeguards. Organisational safeguards include among others DPO designation and monitoring, mandatory DPIA and accountable data management while technical safeguards take the form of obligation for data minimization and pseudonymization, developing strong authentication mechanisms to access health data,

ensuring the security of networks, workplaces, storage and archives assets and processes and respecting data protection by design and data protection by default.

With regard to the implementation of art. 89(2) GDPR, all the rights provided therein (right to access, right to rectification, right to restriction of processing, right to object), apply in the context of the CNIL MR. Derogations have an exceptional nature and they shall be reviewed by the CPP in the context of prospective health research, or the CESREES in the context of retrospective health research and they need to be further authorised by the CNIL. In France, it is also possible to derogate from the right of erasure on grounds of public interest in the area of public health in accordance with art. 17(3)d GDPR. French law also allows derogations to the right to data portability where data are processed in the public interest in accordance with art. 17(3) GDPR. As a general rule, in all derogatory cases, data subjects keep a right to be informed and to introduce a claim before the controller and the CNIL. The French law provides extended protection to data subjects in the context of health research.

The new bioethics law (Loi de bioéthique 2021-1017) specified the legal basis for processing data for health research. Consent is now only required for research on constitutional genetic data (for studying genetic characteristics of a person inherited or acquired at an early stage of prenatal development). In that case, consent must be written, specific, separated and potentially multilayered. However, opt-out is the general rule for research on somatic genetic data (for studying genetic characteristics of a person whose inherited or acquired characteristics are unknown [and not researched] as a first intention). Furthermore, opt-out is the rule for the reuse of biological samples for any genetic research. However, the data subject must have been informed about the research program for which the samples could be reused. Where the person cannot be found back or is unable to express their will, or in case of post-mortem samples processing, the research responsible must ask for prior CPP approval. Lastly, the new law inserted clear provisions regarding the communication of incidental genetic research results in healthcare where they are clinically validated and are considered to be useful for the health of the data subject or his family members (modified Art.16-10 Civil Code). The initial data subject can consent to the communication or refuse it by written, they can communicate the information by themselves or delegate the communication to the prescribing physician who will ensure data subject's anonymity. In any case, the person has a right not to know about such findings. The same modalities apply to the communication of incidental findings resulting from clinical genetic testing practices allowing then to share anonymised information from a patient to the benefit of another family member, ascendants, descendants and collaterals. Some other provisions from the bioethics law organize further the access to health data of a patient to the benefit of a family member based on solidarity principle. In particular, it clarifies that medical confidentiality does not prevent information concerning a deceased person which are necessary for the care of a person likely to be the subject of a genetic test for medical purposes from being delivered to the doctor providing this care, unless the person expressed a contrary wish before their death (modified article L.1110-4 and L.1111-7 Public Health Code). Similarly, it is now possible, based on opt-out, and in derogation of Article 16-10 of the Civil Code, that when the person is unable to express their wishes or when they are dead, a genetic examination be undertaken for medical purposes in the interest of the members of their family if a doctor suspects a genetic anomaly that may be responsible for a serious condition justifying preventive measures, including genetic counselling, or care. Where the person is deceased, the examination shall be carried out on samples of that person already preserved or taken in the course of an autopsy for medical purposes.

In conclusion, health research has been facilitated due to the more simplified procedures prescribed by the French law.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

In *Germany*, the applicable legal framework on the processing of health and genetic data includes the Patient Data Protection Act, the Genetic Diagnosis Act, State hospital laws, State data protection laws, the Federal Data Protection Act, Civil law provisions as well as the Professional secrecy rules. Thereby, reference should be made to the complexity of applicable law based on the federal state structure (federal level vs. state level), on general and specific laws (*lex specialis* vs. *lex generalis*) and particularly of existing specific laws. The Patient Data Protection Act regulates among others the further processing of data from electronic health records. The Genetic Diagnosis Act is a pre-GDPR framework and focuses only on the diagnostic issues related to genomics and genetics while it does not focus on scientific research. This entails that in case of processing genomic data for scientific research purposes, GDPR and data protection law would apply. State hospital laws and state data protection laws often apply jointly. Despite the wealth of applicable laws, there is no biobanking law in Germany.

In the context of scientific research, the legal basis can take many forms. Although broad consent, as provided under Recital 33 GDPR, is not detailed in German law, the conference of all state level data protection supervisory authorities has issued an opinion on broad consent in the context of scientific research, prescribing specific conditions, such as employment of additional safeguards and, emphasising the role of the ethical review. Another legal basis, which is debated though, is the public interest in the area of public health (art. 9(2)i GDPR). Additionally, scientific research constitutes another form of the legal basis, which is also hotly debated due to the balancing act that is implied through its application (art. 9(2)j GDPR). Federal and state level provisions based on Art. 9(2)j GDPR rely on its wording with some specification. In general, further rules list possible technical and organisational measures that can be applied corresponding to the risk assessment of the data processing.

The data subject rights provided in art. 15, 16, 18 and 21 GDPR, namely the right to access, the right to rectification, right to restriction and right to object respectively, shall be limited to the extent that these rights are likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes (for example, Section 27(2) Federal Data Protection Act). Also, within the scope of application of the Federal Data Protection Act, the right to be forgotten can be derogated from in accordance with Article 89(1) in so far as the right is likely to render impossible or seriously impair the achievement of the objectives of that processing (art. 17(3)d GDPR, Section 35(1) Federal Data Protection Act).

In Germany, the use of health data of one patient for the healthcare of another patient is allowed under certain conditions. It should be taken into account that whenever the data processing falls into the scope of application of the state hospital laws, the state hospital laws take precedence over the general data protection rules of the GDPR and the Federal Data Protection Act as a more specific law. For example, the Baden-Württemberg State Hospital Act states in § 45(1) LKHG BW that patient data may be collected and processed, if this serves to care for the patient or to settle the account for medical services. However, according to § 46 (1) no. 6 LKHG BW, transmission outside the hospital is possible if the transmission is necessary to avert a danger to the life, health or freedom of the patient or a third party if the threat to these legal interests outweighs the confidentiality interest of the person concerned and the danger cannot be eliminated in any other reasonable way. Additionally, according to Art. 27 (2) of the Bavarian State Hospital Act, patient data may only be collected and stored if this is necessary for the fulfilment of the hospital's tasks or within the framework of the hospital-medical treatment relationship, or if the person concerned has consented.

4.2.3.4 Eastern European Countries workshop main points and outcomes

Date: 21st of February 2022

Speakers: Santa Slokenberga, Signe Mezinska (Latvia), Dorota Krekora- Zajac (Poland), Radek Halouzka, Jan Kuráň (Czech Republic), Silja Elunurm (Estonia)

In ***Latvia***, the ethico-legal framework for scientific research appears to be quite fragmented. Latvia is a monistic country, consequently international treaties that have been signed and ratified can be invoked directly at the national level. The Convention on Human Rights and Biomedicine (Oviedo Convention) sets out the general requirements for scientific research, while the Law on the Rights of the Patients has provisions on the use of patients' data in scientific research (Section 10) as well as the patients' involvement in a clinical trial in general (Section 11). The Pharmaceutical Law and the Cabinet Regulation 289 of 23 March 2010 have more specific provisions on clinical trials of medicinal products. The Human Genome Research Law governs the human genome research while the data protection framework predominantly consists of GDPR and the Personal Data Processing Law, as well as the mentioned provision on the Law on the Rights of the Patients. For the moment, there is no comprehensive regulation governing health registries, linking data from different resources and biobanks. However, Latvia is currently working towards a secondary use of data law as well as Biobank Law.

Latvia has taken measures to adapt its legal framework on art. 9(2)j GDPR (Section 31 Personal Data Processing Law), but it has not taken advantage of art. 9(4) GDPR, which enables States to introduce further conditions for the processing of special categories of data. Although the adaptation to art. 9(2)j GDPR allows the use of non-consensual legal basis for scientific research, in practice, it is difficult to adopt it for primary research. In general, the scientific research regulation in Latvia is still in a pre-GDPR phase, where consent is the legal basis for use of personal data in research (Law on the Rights of Patients, Pharmaceutical Law, Cabinet Regulation 289 of 23 March 2010, Human Genome Research Law).

For the secondary use of health data from patient medical records in the context of scientific research, except for consent, health data can be further processed also without consent when a special procedure is pursued in accordance with Section 10 Paragraph 8 of Law on the Rights of the Patients. More specifically, there are five conditions that need to be fulfilled for this special procedure, namely 1) the research is carried out in the public interest, 2) it has been granted a special authorization by an authority in accordance with the Cabinet Regulation 446 of 4 August 2015, 3) the patient has not previously prohibited the transfer of their data to the researcher in writing, 4) it is not possible to obtain the patient's consent by reasonable means and 5) the benefit of the research for the benefit of public health is commensurate with the restriction of the right to privacy.

Although the Latvian Personal Data Processing Law (Section 31) allows the derogation from data subject rights under art. 15, 16, 18 and 21 GPDR, pursuant to art. 89(2) GDPR, the operationalization of this possibility is limited by old solid laws that set out specific requirements, including data subject rights.

With regard to human genome research, the Human Genome Research Law, which is quite old (2002), provides for genetic exceptionalism, in the sense that it attributes genetic data a *sui generis* status, that currently is unrealistic due to the diversity of omics that pose higher risks than genetic data. What is more, the Human Genome Research Law can be interpreted as giving the possibility to request broad consent in the case of biobanks. Also, it was emphasised that there is a lack of clear legal regulations enabling the secondary use of genetic data.

There is also a lack of a systemic approach with regard to the role of RECs. To begin with, except for the Biomedicine Convention, there is not a general national clause requiring scientific and ethical approval of scientific research. Nor there is a clear and uniform mechanism to fulfil Article 16.iii of the Biomedicine Convention. However, there are some laws in place stating that RECs ethics review should take place, e.g. in the context of clinical research regarding medicinal products. In particular, the ethics review of genetic research is specifically conducted by the Central Medical Ethics Committee, further fortifying the current status of genetic exceptionalism

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

in Latvia. RECs do not have a legally assigned role in evaluating retrospective research using health data. The only exception is the review of student research using data from medical documents which has to be reviewed by institutional RECs.

In general, there is a lack of clear and uniform requirements for data transfer within the clinical care, from the clinical to the research setting and from research setting to clinical care. As a general rule, under Section 10 of the Law on the Rights of the Patients, a medical treatment institution shall share patient data for the purposes of medical care with another medical treatment institution (Section 10 Paragraph 5 Clause 1). Some further data sharing aspects within medical care are regulated under the Cabinet Regulation No 134 of 11 March 2014, as far as information is part of the electronic information system of the health sector. However, in practice, the challenges attributed to the functionality of the system render data sharing rather challenging.

In ***Poland***, there is a lack of specific legal regulations on biobanking and conducting biomedical research. After GDPR, the data protection legal landscape in the context of secondary use of health and genetic data for scientific research purposes is not clear, as there is no special provision in the Personal Data Protection Act that transposes GDPR in the national legal framework. To tackle this, BBMRI-PL has started working on a Code of Conduct (art. 40 GDPR), which aims to adapt data processing standards in the Polish biobanks to GDPR as well as harmonise procedures among the members of the Polish Biobank Network. This Code of Conduct is expected to govern the secondary use of health data. Except for this Code, there are several other Codes of Conduct including one concerning data processing for healthcare and one concerning data processing by the Medical University. For the moment, only the first one has been approved by the Polish Data Protection Authority, but it is not applicable in case of data processing for scientific research purposes.

The Code of Conduct on biobanking consists of principles, explanations and recommendations. The guiding principle is that consent should be obtained for the secondary use of data for scientific research purposes. According to the Code, it is recommended that consent is granted in a written, electronic or documentary form. The Code recommends that consent to data processing should be obtained separately from the consent to other activities related to HBM. It is also recommended that biobanks obtain tiered or dynamic consent, enabling that way the expression or withdrawal of consent for various types of scientific research. The biobank should define the scope and means of sharing patient's/ donor's/ research participant's data as well as clearly indicate whether the data will be processed by commercial and foreign entities. Although consent is the main legal basis for the secondary use of data for scientific purposes, the Code prescribes that consent can be waived on condition that obtaining consent would be impossible or would require extraordinary measures. In this case, it is recommended to obtain the opinion of the competent Bioethics Committee.

With regard to derogations from the exercise of data subject rights pursuant to art. 89(2) GDPR, there is no particular provision due to the lack of specific regulation on processing personal data for scientific research purposes. However, derogations could potentially rely on general rules, including the Polish Constitution, the Act on the Patients' Rights and the interpretation of the Patient Ombudsman.

As a final note, Poland allows the secondary processing of health data of one patient for the diagnosis of another patient only in case of infection diseases and on condition that the processing is based on the patient's consent (Act on infectious diseases). In the absence of consent, the secondary processing can be based on a Court decision.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

In ***Czech Republic***, the processing of health data for healthcare is governed by the Act on Health Services. The legal basis can range between the legal obligation of data controller to keep medical records (art. 6(1) c GDPR) and the performance of contract between controller and data subject for the provision of healthcare (art. 6(1)b and 9(2)h GDPR). The patients' consent is not necessary for the processing of health and genetic data for the purpose of healthcare provision. The Act on Health Services also regulates the transfer of health and genetic data between healthcare providers.

Czech Republic does not have a specific regulation on the secondary use of health and genetic data and the legal landscape seems to be quite fragmented. In particular, the secondary processing of health data for medical research is mainly governed by GDPR and the Czech Personal Data Processing Act but there are also some provisions in the Act on Health Services. According to the Act on Health Services, healthcare workers or scientists can have access to a patient's medical records only upon obtaining the patient´s consent. It is not obligatory to obtain consent in a written form, but it is highly recommended. This type of consent can be interpreted as a broad one.

Although in the pre-GDPR era, consent was the only legal basis for the processing of health data for scientific research(except for situations when processing was necessary to preserve the life or health of the data subject and their consent cannot be obtained, in particular, due to physical, mental or legal incapacity), after GDPR, there are some exceptions including the protection of public health and scientific research (art. 9(2) j and 89 GDPR). Even though there is a presumption of compatibility of secondary processing of data for scientific research according to art. 5(1)b GDPR, the experts that made the presentation assume that it is still necessary to pass the compatibility test under art. 6(4) GDPR. In the experts' opinion, the secondary processing of data that were initially collected for the provision of healthcare, for the purpose of medical research, is compatible with the initial purpose and can be in most cases carried out without patient's explicit consent in cases where public healthcare providers were established also for purposes of conducting medical research (eg. Deed of Foundation issued by Ministry of Health or regional administration). In some cases, such as in the context of cooperation with commercial entities or in the absence of safeguards pursuant to art. 89 GDPR, explicit consent is required. As a general note, consent seems to prevail on a legal basis.

The Czech Personal Data Processing Act provides a demonstrative list of special measures that the data controller or the data processor shall take when processing health and genetic data for scientific research purposes pursuant to art. 9(2)j GDPR. Indicatively, such measures may include technical and organisational measures aiming at data minimisation, logging of at least all operations of collection, entering, alteration and erasure of personal data for a period of at least 2 years, provision of information to persons who process personal data concerning obligations in the area of personal data protection data, designation of DPO, special limitation of access to personal data at the controller or processor, pseudonymisation, encryption, measures for ensuring permanent confidentiality, integrity, availability and resilience of processing systems and services, process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, special limitation of transmission of personal data to a third country or special limitation of personal data processing for some other purposes (Section 16 Personal Data Processing Act). Another safeguard that is not mentioned in the Personal Data Processing Act, is the independent examination of interventional research projects by an Ethics Committee pursuant to art. 9 of the Additional Protocol of the Oviedo Convention concerning Biomedical Research. However, sometimes researchers submit a request for approval to ethics committees in case of non-interventional retrospective research projects as a means of providing appropriate safeguards. With regard to data transfers, while it is not obligatory to sign Material and Data Transfer Agreements, they are commonly used in the

scientific research setting as an additional safeguard. Additionally, the Personal Data Processing Act in its art. 16(3) allows for derogations from the exercise of data subject rights under art. 15, 16, 18 and 21 GDPR (Section 16(3)).

As a final note, the Act on Specific Health Services allows in its art. 28 (11) the secondary processing of health data of one patient for the diagnosis of another patient in the event that the genetic testing results in a diagnostic conclusion that can be expected to have an impact on the health of the patient, including future generations, or on the health of genetically related persons, the Provider shall recommend to the patient (or its legal representative – parent, custodian) and to the genetically related person the provision of genetic counselling. Genetically related persons are namely patient's direct relatives (such as grandparents, parents and their children) and indirect relatives, where the degree of this risk is determined by the degree of affinity and type of genetic disease.

In ***Estonia***, there is no specific regulation governing the secondary processing of health and genetic data. The legal framework is quite fragmented. Firstly, it should be noted that Chapter 5 of the Public Information Act provides the main rules of the establishment of public databases/registries. On the basis of that Act, the specific conditions and procedure for obtaining the approval of the Estonian Information System's Authority and the Data Protection Inspectorate and, where necessary, also the technical and organisational requirements for establishment and maintenance of databases are provided (there is a separate statute). All Estonian databases/registries are themselves part of the administration system of the state information system.

The Health Services Organisation Act regulates the primary processing of clinical data and provides the legal framework of the eHealth Information System (including the obligation to forward the data to the system, the access rights to the system and the functioning of REC that evaluates the need to issue personal data from the Health Information System for the purposes of scientific research and statistics and the justification thereof). The Statute of the eHealth Information System regulates in more detail the primary and secondary processing of health data taken from the eHealth Information System. In regards to the secondary use of data, the Health Services Organisation Act requires that personal data shall only be issued for the purposes of scientific or historical research and national statistics, provided that the issue or transmission of data from the Health Information System has been provided for in the law. Paragraph 6 of the Personal Data Protection Act provides the legal basis and the main requirements for the processing of personal data for scientific research or official statistics needs.

The Public Health Act regulates the establishment, purposes and access rights of the following national registries: Estonian Cancer Registry, Pregnancy Information System, Estonian Myocardial Infarction Registry, Estonian Tuberculosis Registry, Estonian Cancer Screening Registry. The Act on Narcotic Drugs and Psychotropic Substances and Precursors regulates the functioning of the Drug Treatment Database. The Establishment of Cause of Death Act regulates the functioning of Causes of Death Registry. The Communicable Diseases Prevention and Control Act regulates Estonian Communicable Diseases Register. All of them have also special statutes. Therefore, the regulation is fragmented and there is no "umbrella" act, besides Public Information Act that sets the main rules for the state databases/registries.

The Human Genes Research Act (HGRA) regulates the establishment and maintenance of the Estonian Biobank and also the research within the Estonian Biobank (Section 1 HGRA). The Estonian Personal Data Protection Act provides the statutory basis for the secondary processing of health and genetic data. Last, the Medicinal Products Act governs the clinical trials setting.

Estonia has established the Estonian Biobank, which is a central population-based biobank of the Estonian Genome Center, based at the University of Tartu. Although the secondary use of genetic data and biological material by the healthcare providers is not prohibited, there is no national dedicated legal framework, such as a Biobank law, that regulates genetic research taking place outside the scope of the Estonian Biobank. The HGRA regulates only the research in the Estonian Biobank. The Act establishes the concept of broad consent that must be given by the gene donor for their inclusion in the Estonian Biobank, the storing of their data and the disclosure for the data's use. Researchers can use the health and genomics data for various studies upon approval by the Estonian Committee on Bioethics and Human Research based on public interest. However, the latter generates a debate in Estonia as to whether the Act actually prescribes a public interest model or a consent model.. The HGRA also provides a set of safeguards, including the prohibition of using genetic data and biological material in the context of civil or criminal proceedings or for surveillance (Section 16 HGRA). Generally, the processing of the data included in the Estonian Biobank is only allowed for the purposes prescribed therein, otherwise, the data subject needs to grant their consent. Additionally, the HGRA enables re-contacting and interviewing biobank participants upon the approval of the Estonian Committee on Bioethics and Human Research.

The secondary use of genetic data generated in the healthcare setting for scientific research purposes is allowed upon obtaining informed consent according to the Oviedo Convention and the Personal Data Protection Act.

The secondary use of health data from the national health information system or from the national health registries is possible based on the provisions of the Health Services Organisations Act, the Public Health Act and the Personal Data Protection Act. The secondary use for the purpose of scientific or historical research or statistics, of these data requires the approval of an Ethics Committee. The inclusion of health data from the National eHealth database and the Health Registries to the Estonian Biobank is based on the law and it requires that data subject has not opted out from such inclusion with the initial consent.

In case a researcher wants to access the data and/or biological material stored in the Estonian Biobank, they need to make a preliminary request to the Estonian Biobank of the Institute of Genomics, at the University of Tartu, which is the data controller. Upon the evaluation, it is necessary to obtain the approval of the Ethics Review Committee on Human Research of the Ministry of Social Affairs. In case that the researcher requests to store and study biological samples outside of Estonia, then it is necessary to take the permission of the Senate of the University of Tartu. The last phase is the application for the release of the data and/or biological material from the Estonian Biobank which will lead to either an order for release in case the research will be conducted in the University of Tartu or a release contract with the applicant, in case the research will take place outside. In general, the Ethics Review Committee on Human Research of the Ministry of Social Affairs is reviewing all the research projects based on the data / biological material from the Estonian Biobank. The evaluation is based on the Personal Data Protection Act (Section 6) and the regulation issued by the Minister of Social Affairs on "Establishment of the Research Ethics Committee, its rules of procedure, number of members and procedure for their appointment, and fees for the examination of a research application".

As far as the transfer of data from the research setting to the clinical setting is concerned, only the doctor of a gene donor of the Estonian Biobank has the right to obtain the de-pseudonymised description of the state of health of the gene donor from the Biobank in order to treat the gene donor. Currently, there is no infrastructure or legal framework for the transfer of the genetic data from Estonian Biobank to the National Health Information System, however this will change with the personal medicine implementation project. It will be necessary

to submit an application for data portability based on art. 20 GDPR in order to transfer genetic data from the Estonian Biobank to the national genetic database for clinical use (it will be part of eHealth Information System).

There are many open questions with regard to the legal basis for the secondary processing of health data in Estonia. Health data can be processed without the consent of the data subject for scientific research purposes on condition that they are placed in a pseudonymised format or in a format that provides equivalent level of protection. The secondary processing of health data in a format that can identify the data subject, can take place without the data subject's consent on condition that 1) the purposes of data processing can no longer be achieved after removal of the data enabling identification or it would be unreasonably difficult to achieve these purposes; 2) there is overriding public interest for it in the estimation of the persons conducting scientific research and 3) the scope of obligations of the data subject is not changed based on the processed personal data or the rights of the data subject are not excessively damaged in any other manner (Section 6(3) Personal Data Protection Act). The secondary processing of health data for scientific research purposes requires the verification of compliance by the ethics committee (Section 6(4) Personal Data Protection Act). In the absence of ethics committee, the Estonian Data Protection Inspectorate can undertake the verification.

With regard to art. 89(2) GDPR, Estonia enables the derogation from the exercise of data subject rights under art. 15, 16, 18 and 21 GDPR as long as the objectives of the processing would otherwise be rendered impossible.

The Estonian legislation enables the secondary use of health data of one patient to inform the diagnosis of another patient, only when the initial patient is deceased and the patient who will benefit from the data is a direct relative (ascendant or descendant associated with the deceased person as well as a sibling thereof).

4.2.4. Results

This section summarises the key themes that emerged across the presentations of the speakers and during the workshops' discussions. The overall outcomes from each country are presented in Table 2. Also, the main points that were highlighted in each Workshop are presented in Table 3, through combining these results with the existence of the ethico-legal framework and conditions set out in each country.

According to the **Nordic countries workshop**, when examining the legal basis and conditions under which data can be used retrospectively for research, Nordic countries differ among them. A variety of legal instruments, including the national Data Protection Acts, interact between them alongside GDPR provisions making the legal landscape complex even at the national level (e.g. Biobank Acts, Health Act on patient rights, Acts on research ethics, Genome Acts etc). There are also differences in legal basis, safeguards and rights. Finally, the role of RECs as one of art. 89 GDPR safeguards has significantly changed after GDPR scrutinised complex data issues, such as GDPR compliance.

Additionally, as mentioned in the **South European countries workshop**, the legal basis and conditions under which data can be reused for research, South European countries do not differ among them. All countries use informed consent as a general rule. In the South European countries, similarly to the Nordic countries, the legal landscape is complex at the national level due to the variety of legal instruments (e.g. Biobank Act only of Spain, Health Act on patient rights, Acts on research ethics etc) which interrelate with the national Data Protection Acts and GDPR. However, there are differences between South European countries on safeguards and

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

derogations from data subject rights. The role of RECs as one of art. 89 GDPR safeguards has significantly changed after GDPR scrutinising complex data issues, such as GDPR compliance.

According to the **Central European counties workshop**, it was observed that there are differences among Central European countries on the secondary processing of health and genetic data in healthcare and research. A variety of legal instruments, including the national Data Protection Acts, interact between them alongside GDPR provisions and this adds to the complexity of the legal landscape in national level (e.g. Medical Treatment Agreement Act, Patient Data Protection Acts, Genetic Diagnosis Acts, Federal and State Data Protection Acts etc). Differences were also identified in the legal basis, safeguards and rights. Additional Acts are expected to organise further the implementation of data subject's rights (e.g. decrees) in the field of genetic research.

In the **Eastern European Countries workshop**, it was observed that all countries lack a specific regulation on the secondary use of health data for scientific research purposes. Their legal framework appears to be quite fragmented. All participating countries have enacted a data protection law that transposes GDPR in the national legal framework. Poland's Data Protection Act has not implemented the opening clauses for scientific research. Although consent is the main legal basis for the secondary use of health data for scientific research purposes, Estonia has started to drift away from this approach, enabling the secondary processing of health data in the overriding public interest upon the fulfilment of certain conditions. Also, all countries allow the derogation from the exercise of data subject rights pursuant to art. 89(2), based on either specific provisions in the law or general rules. The experts discussed extensively the appropriateness of using consent as a legal basis and commented that it requires the introduction of dynamic consent, which may lead to a consent fatigue. The experts also highlighted the critical role of transparency, which should be ensured even where consent is not the legal basis.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Table 2: Conclusions on secondary use for research per country

European regions	Countries	Conclusions on secondary use for research per country
Nordic	Denmark	Easy to transfer data from healthcare to research.
	Finland	Legislation is being renewed to further encourage the responsible secondary use of health data in research, but the laws are complex. The latest developments have received a lot of criticism for not meeting their objectives and actually making health research more costly and difficult, and there are fears that this trend may continue.
	Norway	Art. 89 a duty of controller not of national authorities; no specification of safeguards/constant update.
	Sweden	Access to health data for research purposes is permissive but complex. Access to health data for other purposes is simply complex.
South	Greece	Not possible to transfer data from research to healthcare and vice-versa unless informed consent. Even in the pandemic Act.
	Italy	Transfer of data from healthcare to research and vice versa without consent is possible but under specific conditions and safeguards.
	Malta	Personal data may be processed where the research activities are in the public interest. Where such processing cannot be conducted using anonymised data, it is only permissible subject to conditions.
	Portugal	Access to health data for research purposes with no consent is permitted if fully detailed and demonstrated.
	Spain	Biomedical research Act still applies as before.
Central	Netherlands	Data sharing is complicated because there are differences in the use of informed or GDPR consents in hospitals, universities, etc.
	Belgium	Complex interplay between data protection rules & biobanking law. Strong emphasis on the data minimisation principle is needed.
	France	Law apply to any research performed by a data controller established in France or using health data from French participants or health systems. Personal data protection is a common obligation that must be met before/during/after the research in every type of research or data source. The Health Data Hub allows centralised access to large health databases for scientific reuses.
	Germany	Complex interplay between state-level and federal laws, specific and general laws as well as specific laws. Various infrastructures are emerging, both for genomic data and within health care.
Eastern	Estonia	No specific regulation on secondary processing of health data. Estonia has drifted away from using consent as the main legal basis for the secondary processing of health data. The legal basis can be the overriding public interest on the condition that certain requirements are fulfilled.
	Czech Republic	No specific regulation on secondary processing of health and genetic data. The Czech Data Processing Act contains a demonstrative list of special measures to be employed when data are processed for scientific research purposes. Patient's consent with access to their medical records for scientific purposes is needed.
	Latvia	Consent is the main legal basis for the secondary use of health data, however, pre-conditions for the use of personal data in scientific research without consent are also envisaged. Latvia is working towards secondary data use law and Biobank law.
	Poland	Code of conduct on Biobanking under drafting process. Lack of specific data protection regulation in the context of scientific research purposes after the GDPR's entry into force. Consent is the main legal basis for the secondary use of health data.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Table 3: Main points of each workshop and the existence of ethico-legal framework in each country

Countries	Secondary use for public interest	Act on secondary use	Consent for health data to research	RECs for health data to research	Consent for research data to healthcare	RECs for research data to healthcare	Specific safeguards on DPA	Anonymization or pseudonymization	Attention to subjects' rights	Need of DPIA
Denmark				✓	✓	✓	✓	✓		
Finland	✓	✓					✓	✓	✓	✓
Norway		✓	✓	✓	✓	✓	✓		✓	
Sweden	✓		✓	✓	✓				✓	
Greece			✓	✓	✓	✓	✓	✓	✓	✓
Italy			✓	✓	✓	✓	✓	✓	✓	✓
Malta	✓				✓	✓		✓		
Portugal			✓	✓	✓	✓	✓	✓	✓	✓
Spain	✓		✓	✓	✓		✓	✓	✓	✓
Netherlands			✓	✓	✓			✓	✓	✓
Belgium	✓		✓	✓	✓		✓	✓	✓	✓
France	✓			✓	✓	✓	✓	✓	✓	✓
Germany	✓	✓	✓		✓				✓	
Poland			✓	✓ [1]	✓				✓	✓
Czech Republic	✓		✓	✓			✓	✓	✓	✓
Latvia	✓		✓	✓ [2]	✓					
Estonia	✓			✓	✓		✓	✓		

4.2.5. Discussion

Designing a supportive normative framework for the reuse of health data (art. 4(15) GDPR, Recital 35, 53 GDPR) and genetic data (art. 4(13) GDPR, Recital 34 GDPR) is of crucial importance for the development of the successful interaction of research and clinical care (Herman, 2020). In order to support this initiative and the creation of a joint genomic cohort across jurisdictions in the EU, a need of exploring legal interoperability across Europe is raised (González-García et al, 2021). To assess legal interoperability, we need to focus on the national legal differences and their impact and consequence in secondary use of health and genetic data (Tassé et al, 2016).

In order to determine the challenges that can arise from cross-border processing and bringing genomic research data to the clinic across European countries, we organised workshops including representatives of the four European regions, Nordic, South, Central, and Eastern Europe. By organising these actions and analysing the specification of each national ethical-legal framework of the four workshops, we can delineate the implementation of GDPR regulations in these countries on secondary use of data and highlight the challenges arising from bringing

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

genomic research to healthcare. There is anecessity to move on sustainable governance structures for health and genetic data processing and transfer cross-border in order to ensure portability and interoperability of these data, and these results can be the first step in this direction.

According to recent studies and our results, GDPR helps simplify sharing of health and genetic data at the European level. However, EU member states and most countries of our workshops implement GDPR into national laws in a different way (Molnár-Gábor & Korbel, 2020). The representatives of the countries highlighted that the legislation and provisions differ depending on the source of data and the purposes of secondary use as well as on the type of stakeholders (data providers, data processors, data users). The major origins of national legal differences were focused on data protection related legislation (opening clauses of the GDPR; healthcare legislation, medical secrecy, patients' rights), genomics related legislation (genome initiative, genomic testing), and research ethics-related legislation.

One of the challenges identified by the participants was the lack of uniformity in different countries as to what "scientific research" concept entails. Given that research projects are no longer taking place only in one country, but increasingly involve cross-border projects, it is necessary to create a common understanding of the concept of scientific research (EDPB, 2021). GDPR does not define the concept of scientific research. Although Recital 159 provides that the processing of personal data for scientific research purposes should be interpreted in a broad manner, the European Data Protection Board (EDPB) stressed that the notion should not be stretched beyond its common meaning, but it should rather mean "a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice" (EDPB, Guidelines 05/2020).

Additionally, while the GDPR lays down horizontal directly applicable rules in all Member States, there remains variation in the range of national-level legislation linked to its implementation in the area of healthcare and genetics research (Chassang, 2017). The Directive 95/46/EC was the first EU data protection instrument that favoured the preservation of national regulatory autonomy in the scientific research context, further leading to the creation of a fragmented landscape (Slokenberga, 2021). It seems that GDPR does not substantially deviate from this direction. This, our participating speakers suggest, has led to a fragmented approach in the way that health and genetic data processing for health and research is conducted in European countries. These results are in line with the recent study published by the European Commission on the "Assessment of the EU Member States' rules on health data in the light of GDPR" (2021), which also underlines that this fragmented approach can negatively impact cross-border cooperation for care provision, healthcare system administration, public health or research. In that context, the EDPB has emphasised that despite the fact the GDPR provides leeway for derogations, it is necessary to embrace the idea that the derogations must only apply when it is strictly necessary (EDPB, Guidelines 03/2020). Given that the fragmentation of national legal frameworks can undermine the cross-border transfer of data for scientific research purposes, it is necessary to coordinate the monitoring of the different derogations and develop codes of conduct as a means to address the lack of harmonisation (European Parliament, 2019). The legal uncertainty and the fragmentation in the context of secondary use of health and genetic data, if not addressed properly, can lead to a proliferation of risks, especially if we take into account the increasing rise of Big Data (Iabob and Simonelli, 2020).

Another indication of legal fragmentation is found in the scope of consent. Although consent is the most common legal basis for the processing of health and genetic data, literature as well as the workshops showed that its scope differs substantially across European countries, and this can further hamper the cross-border transfer of data (Tzortzatou et al, 2021).

Shabani & Borry (2018) emphasise that the allowing Member States' to set further limitations on processing genetic data for research purposes may hamper cross-border processing of genetic

data and undermine the harmonisation of data protection within the European countries if those limitations and conditions vary. All speakers of our study highlighted this point and also that by listing all the different national provisions (which keep changing over time) and identifying different approaches, we will not need to know which country has which provisions and we will achieve harmonisation.

According to previous studies and the workshops, it was observed that despite the fragmentation in the national legal frameworks with respect to the secondary use of health and genetic data for scientific research purposes, the examined countries share the same converging safeguards that can form the basis for the creation of common minimum standards. Safeguards play a significant role in the context of scientific research and they should be understood as a form of compensation for providing more relaxed protection of data subject rights (Duguet. et al, 2021). In particular, some of the most significant converging safeguards pursuant to art. 89(1) GDPR (see also Recitals 156, 157) concern data minimization requirements, including anonymization and pseudonymization techniques, technical measures ensuring security management, confidentiality and integrity, such as encryption as well as safeguards for the disclosure of data and transparency (EDPB, 2021). Other identified trends include the designation of a DPO (art. 37 GDPR, Recital 97 GDPR) and the need to conduct a DPIA (art. 35 GDPR, Recital 75, 84, 89, 90-93 GDPR). Although anonymization (Recital 26 GDPR) and pseudonymization (Art. 4(5) GDPR, Recital 26, 28 GDPR) (see Working Party of Article 29, 2014) are considered to be vital safeguards for the protection of data subjects, it is necessary to find a balance with the interests of scientific research. In this vein, it is necessary to come up with more specific guidelines on the necessity and the procedural aspects of these measures with a view to enable bigger consistency among the European countries (EDPB, 2021).

In addition, recent longitudinal findings suggest that it is crucial to identify the key mechanisms for an effective framework for cross-border sharing of information that enables international collaboration for the purpose of improving health care while preserving human rights to privacy and autonomy (Herman, 2020; Sielemann et al, 2020). A particular focus of all speakers of the workshops has been also on data protection, as this is considered one of the main potential barriers to sharing, both for reasons of its complexity and its lack of a pan-European standard. They underlined that there is an increased need for an infrastructure that will explore the integration of privacy-preserving technology like standard authentication and access protocols, secure multi-party computation and encryption in order to ensure that the processing of data is privacy-protective, transparent, and accountable. Comply with applicable privacy and data protection regulations at every stage of data sharing, and be in a position to provide assurances to citizens that confidentiality and privacy are appropriately protected when data are collected, stored, processed, and exchanged. Privacy and data protection safeguards should be proportionate to the nature and use of the data, whether identifiable, coded or anonymized.

Given that most countries treat consent as the default or the safest legal basis for the secondary processing of health and genetic data, participants shared a common concern over the appropriateness of consent as a legal basis, as it entails a number of challenges that cannot be overlooked. First, when consent is the legal basis, data subjects must have the right to withdraw their consent. When a data controller receives a request for withdrawal, it should in principle delete the personal data straight away, and this could undermine the types of scientific research that are based on data that can be linked to individuals (EDPB, Guidelines 05/2020, Working Party of Article 29, 2018). Second, it is difficult to fulfil the requirements of valid consent under GDPR, according to which consent must be freely given, specific, informed and unambiguous (art. 4(11) GDPR) (Taylor and Whitton, 2020). Especially in the scientific research context, it is particularly challenging to obtain a specific consent from the data subject given that it is often difficult to fully identify the purpose of the data processing at the time of data collection. According to EDPB, although Recital 33 GDPR allows data subjects to give their consent only to certain areas of research or parts of a research project, it does not disapply the obligation to obtain specific consent (EDPB, Guidelines 05/2020). In the context of this discussion, the participants

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

emphasised that consent as a legal basis should not be confused with the consent that is requested as an additional safeguard, eg. as an ethical standard or procedural obligation, pointing out that it may be better to look for alternative legal bases. It has also been suggested in literature that researchers could ask for data subjects' consent as an additional safeguard, but use a different legal basis for the data processing, as a means to overcome the challenges that accompany consent (Dove, 2018). Participants also highlighted that it is necessary to employ measures that ensure transparency, not only in cases where it is difficult to obtain specific consent, but also at more general level (art. 13, 14 GDPR). Indeed, further research within the field suggests that the European legal framework governing the whole data life cycle needs to be characterised by transparency (Knoppers, 2014; Lamas et al, 2015, Altavilla et al, 2019). Transparency is of utmost importance as data subjects feel more in control over their data and their trust towards data controllers is increased (Verhenneman et al, 2019). Most speakers of participating countries in the workshops also emphasised the need to develop clearly defined and accessible information on the purposes, processes, procedures and governance frameworks for health and genetic data processing. Such information should be presented in a way that is understandable and accessible in both digital and non-digital formats. Provide clear information on the purpose, collection, use and exchange of genomic and health-related data, including, but not limited to: data transfer to third parties; international transfer of data; terms of access; duration of data storage; identifiability of individuals and data and limits to anonymity or confidentiality of data; communication of results to individuals and/or groups; oversight of downstream uses of data; commercial involvement; proprietary claims; and processes of withdrawal from data sharing. Implement procedures for fairly determining requests for data access and/or exchange. (Knoppers, 2014; Herman, 2020).

The results of these workshops are in line with the cumulated evidence regarding the challenges faced by each country in the cross-border process of genomic data (Knoppers, 2014; Herman, 2020; Sielemann, 2020; González-García et al, 2021). The main goals according to all speakers are to deal with all these challenges of cross-border processing of data and to move towards a more functional model that relies on agreements and legal sharing provisions that may safely remove barriers without endangering privacy.

4.2.6. Conclusions

The objective of this study was to examine and present, the legal landscape rules that govern the processing of health and genetic data in light of the GDPR, based on selected examples. The aim was to highlight possible differences and identify elements that might affect the cross-border exchange of health and genetic data in the EU from healthcare to research and vice versa in order to support health and genetic data use and re-use. The study is based on a series of expert workshops, organised in 2021 and the first months of 2022, with the participation of representatives of different countries across the EU from Nordic, South, Central and Eastern European regions. According to the analysis of the results, there are differences between EU countries in the implementation of the GDPR in the field of the secondary use of health and genetic data and the development of a common ethico-legal framework is indispensable.

4.2.7 Impact

European countries differ among cross-border processes of health and genomic data. The results of these workshops increase the better understanding of the implementation of the GDPR and secondary use in health and genetic data in different European countries. The emerging challenges of this process which were highlighted in the workshops will, in turn, inform and contribute to the design of the most applicable GDPR requirements for cross-border sharing and develop the B1MG ethico-legal framework taxonomy. A GDPR cross-border toolkit can be built in order to support the target groups of B1MG project, like scientists, technicians, clinicians,

regulators, policymakers, payers and patients to meet these requirements with due respect for national derogations and divergence. By focusing on the empowerment of data subjects under the GDPR, these results can contribute to the development of the legal specifications which can help build workable mechanisms to make these rights operational in close collaboration with WP3 and WP4.

4.2.8. Glossary of terms, abbreviations and acronyms

B1MG: Beyond One Million Genomes

CESREES: Ethics and Scientific Committee for Research, Studies and Evaluations in the field of Health

CNIL: Commission for Information Technology and Liberties

CPP: Committees of Protection of Persons

EDPB: European Data Protection Board

EEA: European Economic Area

EU: European Union

DPA: Data Protection Act

DPIA: Data Protection Impact Assessment

DPO: Data Protection Officer

GDPR: General Data Protection Regulation

FAMHP: Federal Agency for Medicines and Health Products

HBM: Human Body Material

HGRA: Human Genes Research Act

IDPC: Office of the Information and Data Protection Commissioner

LIL: Loi Informatique et Libertés

LKHG BW : Baden-Württemberg State Hospital Act

MR : Methodologies of Reference

NGC: National Genome Center

Oviedo Convention: Human Rights and Biomedicine Convention

4.2.9. References

Altavilla, A., Herveg, J., Giannuzzi, V., Landi, A., and Ceci, A. (2019). The Secondary Use of Paediatric Data under GDPR: Looking for New Safeguards for Research. *European Pharmaceutical Law Review (EPLR),* 3(4), 156-164 Branum, R., & Wolf, S. M. (2015). International Policies on Sharing Genomic Research Results with Relatives: Approaches to Balancing Privacy with Access. *The*

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Journal of law, medicine & ethics: a journal of the American Society of Law, Medicine & Ethics, 43(3), 576–593. https://doi.org/10.1111/jlme.12301

Brittain HK, Scott R andThomas E. (2017). The rise of the genome and personalised medicine. *Clinical Medicine Journal,* 17(6), 545-551. https://www.rcpjournals.org/content/clinmedicine/17/6/545

Chassang, G., (2017). The impact of the EU general data protection regulation on scientific research. *Ecancer Medical Science*, 11, 709. https://doi.org/10.3332/ecancer.2017.709

Dove, E. S. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *Journal of Law, Medicine and Ethics*, 46(4), 1013-1030

Duguet A. M. and Herveg, J. '*Safeguards and Derogations Relating to Processing for Scientific Purposes: Article 89 Analysis for Biobank Research*' in Slokenberga, S., Tzortzatou, O. and Reichel, J. (eds.), (2021). GDPR and Biobanking Individual Rights, Public Interest and Research Regulation across Europe , Springer, Law, Governance and Technology Series. https://link.springer.com/book/10.1007/978-3-030-49388-2

European Commission on the 'Assessment of the EU Member States' rules on health data in the light of GDPR' (2021) https://ec.europa.eu/health/system/files/2021-02/ms_rules_health-data_en_0.pdf

EDPB, 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' (21 April 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679 – Version 1.1' (4 May 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

EDPB, 'Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research', EDPS/2019/02-08, August 2021, https://edpb.europa.eu/system/files/2022-01/legalstudy_on_the_appropriate_safeguards_89.1.pdf

European Parliament, 'How the General Data Protection Regulation changes the rules for scientific research' (July 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf

González-García, J., Estupiñán-Romero, F., Tellería-Orriols, C. *et al.* (2021). Coping with interoperability in the development of a federated research infrastructure: achievements, challenges and recommendations from the JA-InfAct. *Arch Public Health*, 79, 221. https://doi.org/10.1186/s13690-021-00731-z

Herman, K. (2020). Governing cross-border sharing of genetic data: a new border frontier. https://dspace.library.uvic.ca/bitstream/handle/1828/11545/Herman_Katherina_MPA_2020.pdf?isAllowed=y&sequence=7

Iabob N. and Simonelli F. (2020). Towards a European Health Data Ecosystem. *European Journal of Risk Regulation*, 11(4), 884-893. doi:10.1017/err.2020.88

Knoppers B. M. (2014). Framework for responsible sharing of genomic and health-related data. *The HUGO journal*, 8(1), 3. https://doi.org/10.1186/s11568-014-0003-1

Lalova, T., Negrouk, A., Dollé, L., Bekaert, S., Debucquoy, A., Derèze, J.-J., Valcke, P., Kindt, E., Huys, I., *'An overview of Belgian Legislation Applicable to Biobank Research and its Interplay with Data Protection Rules',* in Slokenberga, S., Tzortzatou, O., and Reichel, J. (ed.), 2021, GDPR and Biobanking. Individual Rights, Public Interest and Research Regulation across Europe, Springer, Law, Governance and Technology Series. https://link.springer.com/book/10.1007/978-3-030-49388-2

Lamas E, Barh A, Brown D and Jaulent MC. (2015). Ethical, Legal and Social Issues related to the health data-warehouses: re-using health data in the research and public health research. *European Federation for Medical Informatics*, 210, 719-723. doi:10.3233/978-1-61499-512-8-719

Martani, A., Geneviève, L. D., Pauli-Magnus, C., McLennan, S., and Elger, B. S. (2019). Regulating the Secondary Use of Data for Research: Arguments Against Genetic Exceptionalism. *Frontiers in genetics*, 10, 1254. https://doi.org/10.3389/fgene.2019.01254

Molnár-Gábor, F. and Korbel, J. O. (2020). Genomic data sharing in Europe is stumbling-Could a code of conduct prevent its fall?. *EMBO molecular medicine*, 12(3), e11421. https://doi.org/10.15252/emmm.201911421

Molnar-Gabor F, Sellner J, Pagil S, Slokenberga S, Tzortzatou O, Nystr¨om K. (2021). Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: insights from Germany, Greece, Latvia and Sweden, *Seminars in Cancer Biology.* doi: https://doi.org/10.1016/j.semcancer.2021.12.001

Nuffield Council on Bioethics (2015). The collection, linking and use of data in biomedical research and health care: ethical issues. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf.

Saunders, G., Baudis, M., Becker, R., Beltran, S., Béroud, C., Birney, E., Brooksbank, C., Brunak, S., Van den Bulcke, M., Drysdale, R., Capella-Gutierrez, S., Flicek, P., Florindi, F., Goodhand, P., Gut, I., Heringa, J., Holub, P., Hooyberghs, J., Juty, N., Keane, T. M., Scollen, S. (2019). Leveraging European infrastructures to access 1 million human genomes by 2022. *Nature reviews Genetics*, 20(11), 693–701. https://doi.org/10.1038/s41576-019-0156-9

Shabani, M., and Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European journal of human genetics : EJHG*, 26(2), 149–156. https://doi.org/10.1038/s41431-017-0045-7

Sielemann, K., Hafner, A., and Pucker, B. (2020). The reuse of public datasets in the life sciences: potential risks and rewards. *PeerJ*, *8*, e9954. https://doi.org/10.7717/peerj.9954

Slokenberga, S. '*Setting the Foundations: Individual Rights, Public Interest, Scientific Research and Biobanking*' in Slokenberga, S., Tzortzatou, O. and Reichel, J. (eds.), (2021). GDPR and Biobanking Individual Rights, Public Interest and Research Regulation across Europe , Springer, Law, Governance and Technology Series. https://link.springer.com/book/10.1007/978-3-030-49388-2

Tassé AM, Kirby E and Fortier I. (2016). Developing an Ethical and Legal Interoperability Assessment Process for Retrospective Studies. Biopreservation and Biobanking, 14(3), 249-255. https://doi.org/10.1089/bio.2015.0122

Taylor, M. J., & Whitton, T. (2020). Public Interest, Health Research and Data Protection Law: Establishing Legitimate Trade-off between Individual Control and Research Access to Health Data. *Laws*, 9(1), 6. https://doi.org/10.3390/laws9010006

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Tzortzatou, O. et al '*Biobanking Across Europe Post-GDPR: A Deliberately Fragmented Landscape*' in Slokenberga, S., Tzortzatou, O. and Reichel, J. (eds.), (2021). GDPR and Biobanking Individual Rights, Public Interest and Research Regulation across Europe , Springer, Law, Governance and Technology Series. https://link.springer.com/book/10.1007/978-3-030-49388-2

Verhenneman, G., Claes, K., Derèze, J.J, Herijgers, P., Mathieu, C., Rademakers, F.E., Reydaa, R. and Vanautgaerdena, M. (2019). How GDPR Enhances Transparency and Fosters Pseudonymisation in Academic Medical Research. *European Journal of Health Law*, 27, 35-57. https://doi.org/10.1163/15718093-12251009

Working Party of Article 29, 'Opinion 05/2014 on Anonymisation Techniques' (10 April 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Working Party of Article 29, 'Guidelines on consent under Regulation 2016/679' (10 April 2018), https://ec.europa.eu/newsroom/article29/items/623051

[1]Poland: REC's approval is not required by law, but it is commonly used due to the requirements of institutions involved in scientific research.
[2] Latvia: RECs do not have a legally assigned role in evaluating retrospective research using health data. However, a prior REC approval is necessary for student research using data from medical documents.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

4.2 Transnational Code of Conduct

Transnational Data Protection Code of Conduct

intending the proper application of the EU General Data Protection Regulation, with a focus on data subject rights, to cross border analysis of human genetic data for purposes of scientific medical research within the European Union

Explanatory Note

1. Genetics research may benefit from providing researchers across the EU with access to genetic information stored across the EU. The provision of such access to genetic data of a data subject by a data controller in one Member State to a data user(s) from another Member State(s) ("Cross Border Access") is likely to involve the processing of (directly or indirectly) identifying data (personal data) and hence subject to the EU General Data Protection Regulation ("GDPR"). The GDPR defines "genetic data" as "[means] personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. As the provision of Cross Border Access involves the processing, on a large-scale, of special categories of data (i.e. genetic data), it is deemed by GDPR to be likely to result in a high risk to the rights and freedoms of the data subjects concerned.

2. Specifically, the leakage of identifying information derived from genetic and omics data has been established in many studies, with single nucleotide polymorphisms (SNPs) shown to carry a strong risk of reidentification for individuals and their genetic relatives. Additional risks include the sensitive nature of genetic data, the proposed repeated use thereof through Cross Border Access by multiple data users, from a variety of jurisdictions, each with their own rules and regulations, the resultant accumulation of meaning to be ascribed to the data, the possible requirement of feedback of results to the data subject and her family and the potential of this type of data and associated information being abused, whether or not by linking with other personal data, resulting in economic or social disadvantage, including discrimination and limitation or denial of access to private and public services, loss of autonomy, automated decision-making and coercive or mandatory medicines, for the data subject or her family.

3. To address these risks, processing these data within a Member State of the European Union (EU) is subject to the national legislation of that Member State, which includes but is not limited to the GDPR, as implemented in the Member State concerned. However, the processing of these personal genetic data across the borders of the Member States raises, inter alia, the following issues under the GDPR.

4. *Processing of special categories of personal data.* First, under the GDPR the processing of genetic data and data concerning health is prohibited[68]. This prohibition can only be lifted

[68] Article 9 § 1 of the EU General Data Protection Regulation (GDPR).

if one of the exceptions[69] listed in the GDPR applies and provided that the processing complies with all other requirements of the GDPR, including a legal basis for lawful processing[70].

5. *Member State conditions.* Second, the GDPR provides that Union law or Member State law may provide that the prohibition of processing genetic data under the GDPR may not be lifted by the data subject[71]. Also, Member States may maintain or introduce their own, national, conditions, including limitations, with regard to the processing of genetic data[72].

6. *Processing for purposes of scientific research requires appropriate safeguards.* Third, the GDPR provides that, regardless of the type of data, processing personal data for scientific research purposes must be subject to appropriate safeguards, in accordance with the GDPR, for the rights and freedoms of the data subject[73].

7. *Member State derogations to data subject rights.* Fourth, when personal data are being processed for scientific purposes, the GDPR allows the Member States, under certain conditions, to enact their own, national, derogations from certain data subject rights under the GDPR[74]. In brief, processing of personal genetic data for purposes of scientific research has not been harmonised under the GDPR.

8. *Accountability for compliance with GDPR - assignment of GDPR roles.* Fifth, the disclosure by transmission of genetic data by the primary collector (controller and custodian) of these data to one or more researchers established in one or more other Member State(s) raises questions about GDPR roles and responsibilities, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of the GDPR.

9. *Which national law applies?* Sixth, the transfer and subsequent processing of personal genetic data across the borders of the Member States raises the issue which Member State's national data protection law applies? The territorial scope of the GDPR is directly based on the GDPR[75]. However, this territorial effect does not apply to the territorial scope of the Member State law which is based on the GDPR. The territorial effect of such national laws depends on the national law of the Member State concerned.

[69] Article 9 § 2 of the GDPR.
[70] Article 6 of the GDPR.
[71] Article 9 § 2 GDPR.
[72] Article 9 § 4 of the GDPR ('Lawfulness of processing').
[73] Article 89 § 1 of the GDPR.
[74] Where personal data are processed for scientific or historical research purposes, Union or Member State law may provide for derogations from the right of access by the data subject (Article 15 of the GDPR), the right to rectification (Article 16 of the GDPR) the right to restriction of processing (Article 18 of the GDPR) and the right to object (Article 21 of the GDPR), subject to the conditions and safeguards referred to in Article 89 § 1 of the GDPR and in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purpose of the scientific research and such derogations are necessary for the fulfilment of this purpose (Article 89 § 2 of the GDPR).
[75] Article 3 of the GDPR.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

For example, a genetics researcher established in the Netherlands wants to process in the Netherlands not only personal genetics data from data subjects residing in the Netherlands, but would also like to use personal genetic data regarding data subjects residing in Sweden held by a Swedish researcher, and regarding data subjects residing in France held by a French researcher established in France.
This scenario is in practice likely to be further confounded in the event of a joint research project, when researchers established in different Member States want to join in the processing. Complicating the issue even further is the fact that each Member State will have its own provision for the territorial scope of its national data protection law and its own law on 'conflict of laws'. This may prevent the researcher in France, for example, from making the genetic data of the French data subjects available, as French law may provide for further conditions, including limitations[76] and/or have different derogations from their data subjects' rights with respect to the processing of these data[77].

10. *Processing genetic data may be subject to additional national specific sector laws.* Processing genetic data within a given Member State is not only subject to the GDPR but also to specific (health) sector national laws and human rights, such as patient confidentiality laws, criminal laws and associated national and institutional regulations. In addition, use of the data is in principle subject to informed consent and any limitations therein and subject to prior approval by an ethics committee and any conditions of such an approval. Compliance with these additional laws and conditions is typically the responsibility of the initial collector and controller of these data, in his or her role as custodian of these data. A siloed regulatory approach, focusing exclusively on the GDPR, would compromise compliance by this controller who is also the custodian of these data pursuant to related laws, regulations, conditions, codes and associated guidance, and case law.

11. *Transnational Code of Conduct.* It follows from the above, in brief, that processing of personal genetic data for purposes of scientific research has not been harmonised under the GDPR. As a result, the flow of human genetic data for purposes of scientific research among the Member States is hampered. One legal avenue, offered by the GDPR, to overcome the above issues of diverging national data subject rights and laws, is by the adoption of a pan European Code of Conduct by the pertinent sector of human genetic researchers, in conformity with Article 40 of the GDPR[78]. To that end, the sector of human genetic researchers, represented by the [Association (e.g. ESHG)] has prepared this Transnational Code of Conduct, in conformity with Article 40 of the GDPR. The Code cannot and does not aim to 'harmonise' any diverging national data protection laws of the Member States. Rather it intends to contribute to the proper application of the GDPR and to specify its application to Cross Border Processing of human genetic data for purposes of scientific research, with the aim to ensure the complete and effective protection of the data subjects concerned.

12. As additional benefits, the Code has been structured in such a way as to "double" as a joint arrangement required under Article 26 of the GDPR and both data providers and data users could use adherence to such a Code to demonstrate their compliance with their obligations under the GDPR and any national implementation thereof.

[76] Pursuant to Article 9 § 4 of the GDPR.
[77] Pursuant to Article 89 § 2 of the GDPR.
[78] European Parliament, 'How the General Data Protection Regulation changes the rules for scientific research' (July 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf.

13. As Cross Border Access relates to processing activities in several member states, the draft Code has been submitted to the Netherlands Supervisory Authority which, upon its review thereof and prior to its approval, has submitted the draft Code for advice to the European Data Protection Board (EDPB), which in turn has submitted its advice on the draft Code to the EU Commission, which has decided, by way of implementing act, that the Code has general validity.

14. Following below is the draft Code:

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Transnational Code of Conduct

intending the proper application of the EU General Data Protection Regulation to the processing of human genetic data, for purposes of scientific research, within the European Union

Section I – Purpose, parties & scope

Clause 1

Purpose, parties and scope

1. The purpose of this Transnational Code of Conduct is (i) to contribute to the proper application and to provide specification of the requirements of the GDPR[79] with respect to the processing of genetic data for purposes of scientific research across the borders of EU Member States, (ii) to clarify the roles and responsibilities of the controllers concerned, (iii) to address the issues triggered by the different Member State laws applicable to such processing.

2. The persons who can adhere to this Code of Conduct are (i) Data Custodian(s): natural or legal persons residing respectively established in a Member State of the European Union who have personal genetic data under their controllership and custody and (ii) Data User(s): natural or legal persons residing respectively established in a Member State of the European Union, who qualify as academic medical researcher(s) or academic medical research institution(s) and who are engaged in scientific genetic research.

3. This Code applies to the transnational processing, i.e. the 'making available' and 'use', of personal genetic data, as defined in the GDPR, for the purposes of scientific research across the national borders of the Member States ("Cross-Border Access" or "CBA").

4. The relationship between Adhering Persons with respect to the conduct of a scientific medical research project including Cross Border Access shall be governed by a contract to be entered into between the Adhering Persons, which shall deal with all matters non-data protection and not regulated in this Code, including but not limited to IP and publication matters (the Research Contract). For the avoidance of doubt, the Research Contract shall refer to and incorporate by reference the obligations of the Adhering Persons under this Code.

Clause 2

Interpretation & integration

1. Where this Code uses the terms defined in the GDPR, those terms shall have the same meaning as in the GDPR. This Code shall be read and interpreted in the light of the provisions of the GDPR. This Code shall not be interpreted in a way that conflicts

[79] Regulation (EU) 2016/97 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and the free movement of such data (General Data Protection Regulation or GDPR).

with rights and obligations provided for in the GDPR. All Annexes (I through ..) form an integral part of this Code.

Clause 3

Adhering Clause

1. Data Custodians and Data Users who wish to adhere to the Code shall provide the Association with an explicit declaration of adhesion in the form of Annex II, committing to comply with the obligations established therein and will so become Adhering Persons. This statement will include, along with their contact details, the interlocutor designated by the Adhering Person for the purposes of notifications related to the Code, the data protection officer (if one has been designated) and, in the event such a procedure is part of the Code, the interlocutors who will attend to the communications performed in extrajudicial dispute resolution procedures.

2. Adhering Persons will inform the Association of any changes in their contact data or the data of their representatives and contact persons, and in particular of the appointment of a data protection officer in the event that none was appointed at the time of joining.

3. The Association will maintain the list of Adhering Persons duly up-to-date, informing the competent Supervisory Authority of any modifications. This list will be made accessible to the public and available on the Association's website (www.[..]) or one that may replace it).

4. Adhering Persons may withdraw from the Code by notifying the Association in writing and expressly declaring their intention to withdraw, at least one month before the date on which they wish to withdraw. This notification must be signed by the Adhering Person or an authorised representative of the Adhering Person.

5. In any event, the withdrawal will not affect procedures in process on that date or that apply to events prior to the effective date of the withdrawal, which will continue until their completion, in accordance with the provisions of this Code.

Section II Specifying Data Protection Requirements

Clause 1

Designated Controller

1. In order to satisfy the GDPR requirements of 'accountability'[80] in general and of the 'transparent information, communication and modalities for the exercise of the rights of the data subject' in particular'[81], the party responsible for compliance of Cross Border Access with the obligations under the GDPR pursuant to Article 26 of the GDPR shall be the Data Custodian.

[80] Article 5 § 2 and Article 24 of the GDPR.
[81] Chapter III of the GDPR - Rights of the data subject, juncto Article 26 of the GDPR.

Clause 2

Cross Border Access subject to prior assessment by Access Committee

1. Cross Border Access requires the prior written assessment of the Cross Border Access Committee as per this Code. Applications for approval of Cross Border Access will be made conform the Cross Border Access Procedure of this Code.

Clause 3

Cross Border Access Procedure

Cross Border Access Committee

1. A Data Custodian shall have an independent Cross Border Access Committee (CBAC) in place to assess applications from Data Users to Data Custodians for Cross Border Access. A Cross Border Access Committee could be a stand-alone committee or form part of a Data Access Committee or a Medical Ethical Review Board, as appropriate and in accordance with applicable law.

2. The CBAC shall be comprised of an equal number of data subjects or their representatives, and experts in data protection matters.

3. The members of the CBAC shall be appointed for a term of 3 years, which may be prolonged once. The CBAC shall elect its chairman from among its members for a term of 3 years, which may be prolonged once. The chairman is qualified as a data protection expert.

4. Members of the CBAC shall not have financial or other interests which could affect their impartiality. They shall act in the interests of the data subjects and in an independent manner, and shall submit an annual declaration of any interests, financial or otherwise, conflicting with their membership of the CBAC, which shall be entered in a register held by the CBAC which is accessible to the public, on request, at the CBACs offices.

5. The CBAC's internal rules shall provide for the implementation of this paragraph with particular reference to the acceptance of gifts.

6. Members of the CBAC, and, if applicable, any rapporteurs and experts who participate in meetings of the CBAC shall declare, at each meeting, any specific interests which could be considered to be prejudicial to their independence with respect to the items on the agenda. These declarations shall be made available to the public.

7. The CBAC shall adopt rules to ensure the availability to the public of regulatory, scientific or technical information concerning the application for and the authorisation or rejection of Cross Border Access which is not of a confidential nature. The internal rules and procedures of the CBAC shall be made available to the public on its website.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

8. The CBAC shall set up and maintain a web-portal for the dissemination of information on Cross Border Access applications and authorisations. By means of that portal, the CBAC shall make public at least the following:
    (a) the names of members of the CBAC, together with their professional qualifications and with the declarations of any conflicts of interest;
    (b) the agendas of all CBAC meetings will be published 7 working days prior to the meeting;
    (c) The minutes of all CBAC meetings will be published in the week following their adoption by the CDAC;
    (d) a list of Cross Border Access applications, granted applications and rejected applications;
    (e) a list of data breach reports;
    (f) conclusions of the assessment of the application for CBA and the approvals, rejections or other decisions taken by the CBAC with regard to the application.

Application for Cross Border Access

9. Applications for approval of Cross Border Access will be made conform the Cross Border Access Procedure of this Code.

10. A Data User may apply for Cross Border Access from a Data Custodian by the submission of an application to the Data Custodian concerned.

11. Data Users must submit their application to the Data Custodian using an Application Form for Cross Border Access issued by the Data Custodian. The Data Custodian will forward a copy of all incoming applications for Cross Border Access to the Cross Border Access Committee for registration and advice.

12. Data Custodians may use their own Application form for Cross Border Access. However, their application form for CBA shall at a minimum contain the items listed in the template form attached to this Code in Annex 1. The application form will be signed by the legal representative of the Data User and by the Data User's data protection officer, and a copy of any applicable Research Contract or, where applicable, research consortium agreement concerning the proposed Cross Border Access.

13. The Data Custodian will consider applications that include named collaborators. Each collaborator must co-sign the application and be and continue to be an Adhering Person. In the event an applicant wishes to share the Cross Border Access with additional Data Users not previously approved by the Data CustodianC, these additional Data Users must make a separate application for the Cross Border Access concerned. In the event two or more applications overlap, the Data Custodian may propose the respective applicants to align their applications.

14. Applications seeking Cross Border Access for unspecified research goals will not be taken into consideration by the Data Custodian.

Assessment of application for Cross Border Access

15. The Cross Border Access Committee will assess each application for Cross Border Access to determine:
    (i) whether it has been submitted by one or more Data User(s) who is registered as an Adhering Persons;
    (ii) whether the nature of the funding of the application and of the applicant Data User is not for profit;
    (iii) whether the purpose of the application fits the scientific use purposes of the Data Custodian;
    (iv) whether the application has been peer reviewed and the outcome of this review;
    (v) whether the application fits the individual sample donor's consent, and is likely to be understood as such by the individual sample donor;
    (vi) whether it complies with the conditions or restrictions in any pertinent consent form and/or imposed by a medico-ethical review board;
    (vii) whether all required ethico-legal approvals, restrictions and commitments for the application have been obtained and adhered to;
    (viii) whether the application triggers any cross border data protection risks for the data subjects concerned.
    (ix) whether the application could have any adverse potential impact, specifically whether the proposed research could affect minorities and/or minors;
    (x) whether the application is, quantitatively and qualitatively, suitable and not excessive for the applicant's proposed research;
    (xi) whether there are any similar applications pending or granted;
    (xii) and to consider any other criteria which the Cross Border Access Committee deems necessary in the light of the pending application.

16. The Cross Border Access Committee will render its advice to the Data Custodian on an application within a reasonable period of time after it has received all pertinent information. The Cross Border Access Committee will render and motivate its advice, whether to approve, to approve subject to conditions or to reject an application, and will do so in writing.

17. When deciding on the application, the Data Custodian will take the advice of the Cross Border Access Committee into account and explain in writing if he chooses not to follow the advice. The Data Custodian may make an approval subject to further conditions. If the Data Custodian decides to approve the application, he will make Cross Border Access available to the Data User(s). The provision of Cross Border Access to the Data User will be administered by the Data Custodian and be notified to pertinent data subjects by the Custodian.

Clause 4

Data Protection Safeguards

1. To satisfy the GDPR principles of 'lawfulness, fairness, and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', 'integrity and

confidentiality' and 'accountability'[82] and as safeguard for the rights and freedoms of the data subject, the Data Custodian shall provide Cross Border Access by way of 'local analysis' of the Data Provider's research question, also known as decentralised, local (institutional) and non-disclosive analysis of the genetic data concerned. The Data Custodian will limit Cross Border Access for Data Users to the data concerned being analysed on the local servers in the Member State of the Data Custodian. Rather than the Data Custodian transferring his or her data subject's data to, one or more, Data User(s) in one or more other Member State(s), the Data User will bring his or her proposed analysis to the data held by the Data Custodian in the Member State of establishment of the Data Custodian.

2. The Data Custodian shall ensure that the genetic data under his or her controllership and custody that are subject to Cross Border Access, remain secure behind the firewalls on the systems and servers where they reside, under his or her control, custody and governance and that such Cross Border Access is at all times in compliance with pertinent GDPR, national and institutional technical and organisational data protection standards, codes and applicable laws. The Data Users shall comply with any request or instruction which the Data Custodian deems necessary to comply with his obligations hereunder.

3. The Data User acknowledges that the result of the local analysis he will receive (the Result) is anonymised and that the Data Custodian will under no circumstances provide the Data User with any means to identify any data subject. The Data User shall not use the Result to (try to) identify or contact individual data subjects. The Data User shall at all times, preserve the confidentiality of any data underlying the Result. In particular, the Data User shall not use, or attempt to use the Result to compromise or otherwise infringe the confidentiality of information on data subjects and their right to privacy.

4. The Data User shall use the granted Cross Border Access only for the purpose and project described in his application, as approved by the Cross Border Access Committee. The Data User accepts that the Data Custodian bears no legal responsibility whatsoever for the accuracy, completeness or comprehensiveness of the data that are the subject of the Cross Border Access and accepts no liability for direct, indirect, consequential or incidental, damages or losses arising from any use of the Result by anyone, including without limitation any clinical use and any commercial use thereof, or arising from the unavailability of these data for whatever reason.

Clause 5

Information, data subject rights and choice of law

1. The responsibility to satisfy the requirements under Articles 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), 13 (Information and access to personal data) and 14 (Information to be provided where personal data have not been obtained from the data subject) shall lie with the Data Custodian concerned. Specifically, the Data Custodian will inform the pertinent data subjects on all incoming applications by Data Users for Cross Border Access upon receipt of such an application and advise them of their rights. The Data

[82] Article 5

Custodian will provide the pertinent data subjects with a list of approved applications stating the names and contact details of the applicants.

2. The Data Custodian shall set up and maintain a web-portal for the dissemination of information on Cross Border Access applications. By means of that portal, the CBAC shall make public at least the following.. By means of that portal, the CBAC shall make public at least the following:

    a. a list of Cross Border Access applications;
    b. pending advices from the Cross Border Access Committee on such applications;
    c. the Data Custodian's decisions on such applications, whether it be an approval, a conditional approval, or a rejection. In the event of a conditional approval, the conditions imposed will be made public as well;
    d. a list of data breach reports;

3. Data Custodian(s) and Data User(s) shall comply with all applicable data subject rights of the data subject concerned, including both local derogations to data subject rights under the GDPR, and all further conditions, including limitations, laid down in the laws of the home state of the data subject concerned, and all rights of the person concerned under his or her national health-sector specific laws.

Clause 6

Data breach

1. The Data Custodian and the Data User concerned will promptly inform each other in the event they encounter a data breach in their respective conduct of Cross Border Access. The Data Custodian shall take appropriate measures to address the data breach, including measures to mitigate its possible adverse effects. Where appropriate the Data User will assist the Data Custodian in mitigating the breach.

2. In the event of a data breach concerning personal data accessed in the Cross Border Access concerned by the Data User, the Data User shall without undue delay and, where possible, within 36 hours after it became aware of the breach, notify the Data Custodian. If a data breach is likely to result in significant adverse effects, the Data Custodian shall, without undue delay after having been notified by the Data User, notify the competent supervisory authority of the Member State of the Data Custodian. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the data breach and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the Data User to provide the information to the Data Custodian at the same time, it may do so in phases without undue further delay.

3. In the event of a data breach concerning personal data accessed by the Data Custodian, the Data Custodian shall, if necessary in cooperation with the Data User, notify without undue delay the data subjects concerned of the data breach.

4. Both the Data User and the Data Custodian shall document all relevant facts relating to the data breach, including its effects and any remedial action taken, and keep a record thereof.

Clause 7

Supervision

1. The supervisory authority of the Member State where the data subject whose personal data are processed under this Code is located shall act as competent supervisory authority.

2. The Data Custodian and the Data User agree to submit themselves to the jurisdiction of the competent supervisory authority in any procedures aimed at ensuring compliance with this Code. In particular, the Data Custodian and the Data User agree to respond to inquiries, submit themselves to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. They shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Section IV – Monitoring & Complaints

Clause 1

General

1. This Section is without prejudice to the GDPR, meaning that any non-compliancy, non performance or violation of the provisions of this Code committed by an Adhering Person may also qualify as a non-compliancy, non performance or violation of the GDPR and might subject such Adhering Person to the remedies, liability and penalties provided for by the GDPR.

Documentation

1. The Adhering Persons shall be able to demonstrate compliance with this Code. The Adhering Persons shall make such documentation available to the competent supervisory authority on request.

Clause 2

Monitoring Body - Audits

1. The Adhering Persons shall mandate an annual audit of their compliance with the provisions of this Code by a monitoring body which has an appropriate level of expertise in relation to the subject matter of this Code and is accredited for that purpose by the competent supervisory authority (Monitoring Body).

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

2. In addition to the annual audit mentioned in paragraph (1), the Adhering Persons shall allow the Monitoring Body to schedule and carry out risk-based interim audits.

3. In order to enable the Monitoring Body to carry out its audit, the Adhering Persons shall make available to the Monitoring Body all information necessary to demonstrate compliance with the obligations set out in this Code and allow for and contribute to reviews of data files and documentation, or of any audits of the processing activities covered by this Code, in particular if there are any indications of non-compliance. The Monitoring Body may include in its audit inspections at the premises of the Adhering Person.

4. The Adhering Persons shall make the results of any audits, available to the competent authority.

Clause 3

Measures and sanctions

1. In cases of infringement of the Code by an Adhering Person, the Monitoring Body shall take appropriate action to stop the infringement and to avoid future recurrence, including but not limited to:
    a. a formal notice requiring the implementation of specific actions within a specified deadline;
    b. submit a proposal for temporary suspension of the Adhering Person from this Code until remedial action is taken, to the Association for the Association to be decided on;
    c. submit a proposal for permanent suspension of the Adhering Person from this Code, for the Association to be decided on.

2. In the event of a permanent suspension, the Monitoring Body shall inform the competent supervisory authority of such action and the reasons for taking them.

Section V – Final Provisions

Clause 1

Non-compliance with the Code and termination

1. An Adhering Person shall promptly inform the Association and the appropriate Adhering Person, if it is unable to comply with the Code, for whatever reason.

2. In the event that a Data User involved in a particular Cross Border Access has been found in breach of this Code or unable to comply with this Code, the Data Custodian(s) shall suspend the access of personal data to the Data User under this Research Contract until compliance is again ensured. The Data Custodian shall inform the competent supervisory authority of such non-compliance.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Clause 2

Governing law

1. This Code has been adopted pursuant to the GDPR and shall be subject to the GDPR accordingly. Any issues arising under this Code which are not governed by the GDPR shall be governed by the law of the Netherlands.

Clause 3

Choice of forum and jurisdiction

1. Any dispute arising under this Code shall be resolved by the courts of The Hague, including the Supreme Court, the Netherlands. The Adhering Persons agree to submit themselves to the jurisdiction of these courts.

2. Legal proceedings by a data subject against the Data Custodian and/or Data User may also be brought before the courts of the home Member State of the data subject.

Clause 4

Review of the Code

1. This Code shall be reviewed on a periodic basis and further as often as deemed necessary by the Association in view of legislative, regulatory or jurisprudential developments, including but not limited to the adoption of guidelines, recommendations, and best practices of the European Data Protection Board in order to encourage consistent application of the GDPR.

2. Any amendment or expansion of this Code shall be submitted to the Netherlands Data Protection Agency, pursuant to the Regulation, to provide an opinion on whether it complies with data protection regulations and, if the guarantees offered are considered sufficient, to approve the Code thus modified or extended.

3. Adhering Persons shall be informed of modifications to the Code. Adhering Persons shall have a period of one month to request the Association their withdrawal from it, if they so desire. If no such request is received, adherence to the Code shall be presumed to have been renewed.

Clause 5

Entry into force

1. This Code will enter into effect as from two months after the publication of the implementing act whereby the European Commission decides that the approved Code has general validity within the European Union.

Annex I Minimal Question set for Application form for Cross Border Access

Request to be filled in and submitted by Data User to Data Custodian

Instructions

To apply for permission for remote analysis by requestor of human genetic data held by Data Custodian, fill in the form below and send to [..]. Your request will be evaluated by the Cross Border Data Access Committee charged by Data Custodian to make such evaluation. If your request has been approved, you will be granted permission to conduct your thus approved remote analysis on the terms set forth in this Transnational Code. For the applicability of any other terms, specifically Publications and IP, please refer to those terms of the Data Custodian or the terms of any research, collaboration or consortium agreement to be entered in to between you and Data Custodian.

Applicant information

Enter information about yourself and all c-applicants (if applicable).

1. Name

2. Position

3. Affiliation [Enter employment information or affiliation with academic institution and name institution].

4. Co-applicants [include full postal and email address and name of academic institution for each co-applicant

Research Question

5. Title of the study

6. Study description
    a. Outline of the study design
    b. An indication of the methodologies used
    c. Description of remote analysis to be used
    d. Preceeding reviews and approvals of the study, methodologies and remote anlaysis to be used (if any).
    e. Specific details of what Data user intends to do with the results of the remote analysis
    f. Expected timeline from date of request until end of the study.
    g. Key references

Consent and approvals

7. Have you obtained all required consent and approvals to conduct your proposed research?
8. If yes, please specify official approvals:

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Data requested for your remote analysis

Indicate to which data you request access for your remote analysis:

Resources, feasibility and expertise

Have you secured funding for the conduct of your study?

Please describe your experience and expertise and that of your co-applicants and how this will be applied to your proposed study:

Recent publications

Please provide a list of recent publications:

Access for analysis conditions

Please declare that you are an Adhering Person to the Transnational Data Protection Code of Conduct to the processing of human genetic data, for purposes of scientific research, within the European Union.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

Annex II Declaration of Adhesion to the Code

[..].

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724

5. Conclusions

This part III builds a workable mechanism to respect and bridge national legal divergences while making data subject rights, as implemented in the national legislation and addressing not only GDPR but also other pertinent human rights and national sector specific safeguards operational in the form of a Code of Conduct for the cross-border sharing of genetic data. To that end, this part delivers an actual draft Transnational Code of Conduct intending the proper application of the GDPR to the cross border analysis of human genetic data for purposes of scientific research within the European Union. A competent (Dutch) Data Protection Agency has expressed its willingness to consider the draft for the formal approval process under Article 40 GDPR.

6. Next steps

Presentation of draft Transnational Code to pertinent categories of controllers (1+MG Controllers/Custodians), designation of Code Owner assembly to ensure periodic updates and continued approval, including representation of vulnerable citizens and minority groups, and consideration of submission of Code of Conduct to the competent Dutch Data Protection Agency to initiate process for formal approval.

B1MG has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 951724