Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research

Final Report

EDPS/2019/02-08

KU LEUVEN crids milieu

August 2021

This study has been prepared by Milieu under the lead of KU-Leuven under Contract No EDPS/2019/02-08 for the benefit of the EDPB.

The study has been carried out by researchers from KU-Leuven, with the support of researchers from Milieu and UNamur. The authors of the study are Els Kindt, César Augusto Fontanillo López, [redacted], Jan Czarnocki, and Olia Kanevskaia, from KU Leuven, and Jean Herveg from UNamur. Complementary national level input concerning Greece was provided by Aliki Benmayor from KU Leuven.

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be ; web address: www.milieu.be.

TABLE OF CONTENTS

EXECUTIVE SUMMARY **5**
1 INTRODUCTION **7**
1.1 Objectives and scope of the study 7
1.2 Study methodology 7
1.3 Scope and meaning of Article 89(1) GDPR 9
2 ANALYSIS OF NATIONAL LEGISLATION, GUIDELINES AND CODES OF CONDUCT **11**
2.1 GDPR implementing national legislation 11
2.1.1 Austria: Two sets of legislation and required safeguards 11
2.1.2 Belgium: a set of safeguards in the GDPR implementing Act 12
2.1.3 Bulgaria: no additional specifications 12
2.1.4 Estonia: broad notion of research and GDPR role for ethic committees 13
2.1.5 Finland: safeguards linked to derogations from rights and role for codes of conduct 13
2.1.6 France: safeguards linked to derogations from rights and SA-centric role for sensitive data 15
2.1.7 Germany: federal and state level legislation 16
2.1.8 Greece: specific safeguards for sensitive data processing without consent 17
2.1.9 Iceland: the need for appropriate security 17
2.1.10 Italy: reference to establishing codes of conduct 17
2.1.11 Norway: role of public interest and no exceptions to the rights of data subjects in case of legal effects 18
2.1.12 Poland: no additional legal requirements 19
2.2 National guidance documentation, codes of conduct and case law 19
2.2.1 Belgium: guidance by the SA and the national research council 19
2.2.2 Estonia: Code of Conduct for Research Integrity 20
2.2.3 Finland: limited concept of scientific research, detailed guidance by the Ombudsman, importance of the research plan and guidelines for higher education 20
2.2.4 France 22
2.2.5 Germany 23
2.2.6 Greece 23
2.2.7 Iceland 24
2.2.8 Italy 24
2.2.9 Norway 26
3 SECTORIAL LEGISLATION AND SOFT LAW **27**
3.1 Overview of EU sectorial legislation and soft law 27
3.1.1 Clinical Trial Directive and Regulation 27
3.1.2 Human tissue and cells Directive 2004/23/EC 28
3.1.3 Regulation (EC) no 223/2009 28
3.1.4 Proposal for Regulation on European data governance 28
3.1.5 Soft law instruments 29
3.2 Other legal instruments with influence upon European countries 30
3.2.1 International 30

3.2.2 The Council of Europe 30
3.3 Overview and legal analysis of national sectorial legislation and soft law .. 31
3.3.1 Austria 31
3.3.2 Belgium 32
3.3.3 Bulgaria 33
3.3.4 Estonia 34
3.3.5 Finland 36
3.3.6 France 37
3.3.7 Germany 38
3.3.8 Greece 39
3.3.9 Iceland 40
3.3.10 Italy 41
3.3.11 Norway 44
3.3.12 Poland 46
4 CONVERGING ELEMENTS AND TRENDS 48
4.1 Converging elements 48
4.1.1 General GDPR implementing legislation and soft law 48
4.1.2 Sectoral legislation and soft law 51
4.2 Trends 54
4.2.1 Research/Data Management Plan 54
4.2.2 Role for the DPO 54
4.2.3 Need for assessment or DPIA 55
4.2.4 Anonymisation or deletion requirement upon completion 55
4.2.5 Medical secrecy and confidentiality for medical research 55
5 DIVERGING ELEMENTS AND IMPACT 56
5.1 Divergences and variations 56
5.1.1 Divergences 56
5.1.2 Variations 59
5.2 Impact 61
6 AVENUES AND POLICY RECOMMENDATIONS 63
6.1 General recommendations 63
6.2 Specific recommendations 63
7 CONCLUSION 68
ANNEX 1 - ACRONYMS AND ABBREVIATIONS 69
ANNEX 2 – EXAMPLES OF DETAILED GUIDELINES - FINLAND AND FRANCE 71
ANNEX 3 – SOURCES OF INFORMATION 77
ANNEX 4 - QUESTIONNAIRE TO SAS– NATIONAL SOURCES OF INFORMATION 86

LIST OF TABLES

Table 1: Recommendation for safeguards for personal data use for scientific research in general 64
Table 2: Recommendations for safeguards for personal data use for scientific research in specific *sectors* 65

LIST OF FIGURES

Figure 1: Data protection roadmap for scientific research 71
Figure 2: Extensive list of the duties of controllers for scientific research 74

EXECUTIVE SUMMARY

This study analyses the appropriate safeguards for scientific research under Article 89(1) of the General Data Protection Regulation (GDPR). Appropriate safeguards in this context refer to the pertinent technical and organizational measures adopted by controllers and processors to protect the rights and freedoms of the data subject while conducting scientific research. To this extent, special relevance is given to those measures aimed at ensuring respect for the principle of data minimisation[1].

Scientific research as a legal concept is not determined. This study, however, contemplates it from a broad perspective[2], which encompasses, inter alia, technological development and demonstration as well as fundamental and applied research conducted both by public and private institutions[3]. In addition, the analysis of appropriate safeguards is based on the regulatory framework governing scientific research. It not only identifies appropriate safeguards stemming from the relevant sector-related methodological and ethical standards, in conformity with good practice[4], but it also takes into account the applicable legislation and data protection rules.

The methodology used in this study rests on a comparative analysis of appropriate safeguards implemented among a set of twelve European Economic Area (EEA) States, selected in agreement with the European Data Protection Board (EDPB). The countries included in the study are: Austria, Belgium, Bulgaria, Estonia, Finland, France, Germany, Greece, Iceland, Italy, Norway, and Poland.

The Supervisory Authorities (SAs) of the selected countries were asked to respond to a questionnaire on the implementation of appropriate safeguards in national and sectoral legislation as well as in other non-binding instruments and sources. Based on the replies and the additional research conducted, three groups of four countries were created according to the interest, language skills, and national legislation knowledge of the authors of this study. The responses were analysed and the relevant information was extracted in comparative tables, which allowed for an individual and collective examination of the appropriate safeguards at different levels. In this vein, Section 2 of this study concentrates on the analysis of national legislation, guidelines and codes of conduct; Section 3 focuses on sectoral legislation and soft law; Sections 4 and 5 highlight converging and diverging elements relating to the implementation of appropriate safeguards, and identify trends and similarities among the analysed national systems. Finally, Sections 6 and 7 provide for avenues, policy recommendations, and conclusions to contribute to a more uniform approach to the implementation of safeguards in the context of scientific research.

The results of this study show that certain harmonisation exists among EEA States with respect to appropriate safeguards for scientific research, as required by the GDPR. However, a conundrum of various bodies of law and (ethical) guidelines regulate scientific research in specific areas, such as biobanking, health, epidemiology, social benefits, artificial intelligence and statistics. In turn, this makes the legal framework for sectoral research to remain fragmented.

On a general note, the study reveals that the analysed national data protection laws differentiate between technical and organisational measures while conducting scientific research, thus mirroring the conceptual framework laid down by the GDPR. While technical measures are widespread in the EEA States, the positivation of organisational measures falls behind. In most of the analysed countries, technical measures concentrate on confidentiality, integrity, availability and resilience of the processing systems and environments where scientific research is being conducted. Confidentiality measures include, predominantly, access control procedures to prevent the intrusion of unauthorised persons in the systems. Integrity measures include encryption, pseudonymisation and anonymisation techniques to

[1] Art. 89(1) GDPR.
[2] Rec. 159 of the GDPR.
[3] *Ibidem.*
[4] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, 04.05.2020, Paragraph 153, viewed 5 August 20201, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

avoid the reading, copying, alteration or removal of information. Availability and resilience measures are in general poorly specified in national legislation. Primarily, countries make a direct reference to the GDPR in relation to the implementation of appropriate availability and resilience measures. Organisational measures are rather timidly addressed. Most prominently, specific measures relating to human resources and test, assessment and evaluation protocols and procedures have been incorporated into the national law of the analysed countries. Organisational measures relating to human resources tend to concentrate on ensuring that the persons authorised to process personal data have committed themselves to a duty of confidentiality. They additionally focus on instructing and improving the competence of the personnel involved in the processing operations by requiring specific trainings to raise awareness on hygienic data protection practices. Appropriate measures for test, assessment and evaluation include the regular monitoring and effectiveness of technical and organisational measures for ensuring the security of the processing.

The report recommends a reassessment of the appropriate technical and organisational measures, whether by binding or non-binding instruments, with special consideration to the measures relating to data minimisation. The authors also consider that further efforts should be made to better harmonise the fragmented legislation for sectoral research. In particular, more robust legal frameworks should be developed to address the various types of research according to their respective risks to fundamental rights and freedoms. By the same token, the overall types of safeguards within each scientific domain should in addition be streamlined. Finally, an intensifying dialogue and closer alignment between the regimes of data protection and ethics to clarify their overlaps and distinctions in relation to the protection of the rights and freedoms of the data subject is recommended.

1 INTRODUCTION

1.1 OBJECTIVES AND SCOPE OF THE STUDY

This study on the appropriate safeguards for the processing of personal data for scientific research under Article 89(1) of the General Data Protection Regulation (GDPR) is submitted further to the framework contract (FWC) No. EDPS/2019/02. The study analyses at national level of 12 European Economic Area (EEA) States the specification and regulation of appropriate safeguards for the rights and freedoms of the data subject in relation to Article 89(1) GDPR. It focuses on explicit references to safeguards for the processing of personal data for scientific research purposes.

To achieve this goal, the study performs a scoping review of the safeguards required or in place in the selected EEA States, based upon the input received from the national data protection Supervisory Authorities (SAs). The aim of the study is thus preeminently practical, as it concentrates on the legal organisational and technical measures envisaged at national level. This research was accomplished by analysing the EEA States´ relevant national laws implementing Article 89(1) GDPR with regard to the processing of data for scientific research purposes as well as any other laws and/or guidelines specific for scientific research and/or codes of conduct, and certain sectorial laws with direct impact on data protection and the specification of safeguards.

1.2 STUDY METHODOLOGY

After consultation and suggestions of the European Data Protection Board (EDPB) 12 European Union (EU) and EEA States were selected[5]. The final list of the countries was then determined and fixed in common agreement with the EDPB, and consists of the following countries (in alphabetical order): Austria, Belgium, Bulgaria, Estonia, Finland, France, Germany, Greece, Iceland, Italy, Norway, and Poland.

The project team then drafted a questionnaire containing concrete questions on the implementation of Article 89(1) GDPR in the national and sectoral legislation as well as in other guiding instruments and sources (see Annex 4). The questionnaire was based on the study's requirements and was submitted to the SAs by the EDPB Secretariat to the contact points of the 12 selected countries. All SAs provided answers to the questionnaires. Based on the questionnaires' replies, groups of countries were created, which were allocated to the researchers, taking into account their interest, language skills and national legislation knowledge. In addition to the input received by the questionnaires, other relevant legislative sources were collected and analysed where possible and relevant.

For all 12 countries, the team analysed 1) national GDPR legislation provisions referring to and implementing Article 89(1) GDPR for scientific research, 2) sectoral legislation, both at national and international level, relating to scientific research and mentioning safeguards relating to the GDPR, and 3) other relevant sources, such as non-binding governmental documents, guidelines, opinions and decisions of the SAs, industry codes, rules of professional legislation, contracts and processing agreements between research institutions and individual researchers, etc. The sectoral analyses provided overall results in the following sectors (in alphabetical order): artificial intelligence, biobanks, (bio)medical research, clinical trials and clinical research, healthcare/epidemiological services, labour/unemployment/social benefits/investigation and statistics. These sectors are retained in this report and described for those countries when national and/or sectoral legislation provided information about safeguards for scientific research.

Based on the extensive analysis, comparative tables were set up, for both national legislation and sectoral legislation for the 12 countries for internal study and comparison purposes. On the basis of these

[5] The following selection criteria were used: 1) geographical distribution; and 2) language skills and national legislation expertise of the researchers involved in the study.

overviews, the team created a descriptive document describing the relevant aspects of the national and sectoral legislation. The compound version of this analysis is encapsulated in Sections 2 and 3. The project team then proceeded with extracting converging and diverging elements of national (sectoral) legislation and identifying trends and similarities between the examined national systems[6]. This analysis is encapsulated in Sections 4 and 5, where three types of elements: "converging elements", "trends" and "diverging elements" are differentiated[7]. The analysed similarities and variations in countries' approaches to legal and technical safeguards for scientific research should allow for possible harmonised approaches and enforcement of Article 89(1) GDPR to be assessed. As a last step, a selected list of recommendations is provided. This list is not exhaustive, but retains only some significant findings of this study. Some further caveats are at order for our findings:

Firstly, the findings do not represent the situation in all 27 EU Member States and all 30 EEA States. The findings for the 12 countries studied, however, already allow interesting observations to be made and best practices and tendencies to be identified, but also challenges of the current national (sectoral) implementation of Article 89(1) GDPR. Secondly, "scientific research" is understood as being conducted both by public and private entitities[8]. At the same time, scientific research for archiving purposes[9] and historical research purposes was – as discussed and agreed with the EDPB - not at the core or intended to be within the scope of this study. Nevertheless, some references are made where considered useful. Thirdly, this study focused on the implementation of Article 89(1) GDPR (safeguards) and did not tackle nor include the implementation of Article 89(2) GDPR (rights restriction). That being said, the interrelation between Article 89(1) and (2) should be kept in mind. Article 89(2) refers directly to the possibility to derogate from certain rights under the GDPR, namely Articles 15, 16, 18 and 21, provided that the conditions and safeguards of Article 89(1) are fulfilled[10]. Article 89(1) and (2) are hence intertwined and in some cases cannot be easily separated in a useful way[11]. At the same time, the focus of this study remains on Article 89(1) GDPR, and conclusions directly related to Article 89(2) therefore remain limited. Sections 2 and 3, and the related endnotes, indicate such cases.

Article 89(1) also has a link with Article 9(4) GDPR, allowing EEA States to adopt national legislation

[6] We created two extensive Excel tables with each a schematic overview of safeguards taken in every country at the level of 1) national implementation of Article 89(1) GDPR and 2) sectoral legislation. The two Excel tables were configured on the basis of the general framework of research methodology as described in Bushan Mishra, S., Alok, S., 2011, 'Handbook of research methodology', Educreation Publishing. Certain adaptations were made for this report and the following stages of scientific research were considered for our comparative analysis of appropriate safeguards: 1) formulation and preparation of the plan, design, and methodology; 2) data collection; 3) data analysis: technical and organizational measures; 4) report, presentation of findings, data sharing; and 5) other: further processing, references to the GDPR, responses to the data subjects, etc. The document containing the descriptive analysis, as well as the two Excel tables, were intended for internal use only and allowed the finding of convergences and divergences, including references, and for making the legal analysis.

[7] We used the term "converging element" if a certain safeguard was present in more than six countries. We used the term "diverging element" when only one to three countries pursue a different approach. We used a looser yardstick for the term "trends," which we used to clarify emerging tendencies in multiple countries, further explained in Section 4.

[8] As laid down by Recital 159 of the GDPR, "*[f]or the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted* ***in a broad manner*** *including for example* ***technological development and demonstration, fundamental research, applied research and "privately funded research"****;* This open approach to scientific research is further supported by the EDPB in the Guidelines 05/2020 on consent under Regulation 2016/679, 04.05.2020, Paragraph 153. Please also note that the term "researcher" is a general notion used in this report, referring to the controller conducting the research, being in most cases an entity, institute, company or body, and in few cases individuals. The notion as such is not referring to any individual researchers, nor controllers, unless indicated otherwise.

[9] Some references to the use for archiving purposes may be included for some countries, because it is a domain which is well organized and exists since some time and which could therefore provide meaningful insights as to safeguards.

[10] In particular, such derogation should be possible when complying with those rights "are likely to render impossible or seriously impair the achievement of the specific purposes" and if the derogation is necessary for fulfilling the research purposes.

[11] Similarly, some EEA States, which are included in this study, have considered the two Articles together. Therefore, this study may, to some extent, for some countries, also include national measures and implementation of safeguards related to Article 89(2) in situations where a separation of the two would not be constructive for the nature of the national legislation in question or for the purpose of this study.

with further conditions for special categories of data. Safeguards could be considered as such further conditions. This link, and national implementation of Article 9(4) GDPR is also not within the scope. and therefore not explicitly further investigated in this study. Because of the limited time frame and means for this study, interviews with relevant stakeholders were not included. The questionnaires' responses and the background research already provided sufficient material to conduct an extensive comparative analysis on the subject matter and draw meaningful conclusions and recommendations.

1.3 SCOPE AND MEANING OF ARTICLE 89(1) GDPR

Article 89(1) GDPR states that personal data processing for archiving in the public interest, scientific or historical research purposes or statistical purposes (hereinafter together also referred to as 'scientific research') shall be subject to appropriate safeguards ***for protecting the rights and freedoms*** *of* the data subjects involved[12]. The safeguards have as an objective that *technical and organisational measures*[13] are in place *in order to ensure, in particular, the principle of data minimisation*. The aim of the safeguards, in other words, is (i) to protect rights and freedoms of the data subjects and (ii) to process personal data ***as little as possible*** *and only* ***as needed*** **to reach the objectives of the research**. By these means, scientific research shall consider data minimisation techniques, such as anonymisation and pseudonymisation, to achieve these purposes[14].

Furthermore, no fewer than eight recitals (recitals 156-163) relate to Article 89 GDPR. Recital 156, e.g., also adds to the data minimisation requirement that this requirement is 'in pursuance of the proportionality and necessity principles'. Some further additional explanations are contained in these recitals, including in relation to the *coupling information from registries*, personal data processing for scientific research and studies *in the public interest in the area of public health*, the interest of the Union *in achieving the European Research Area*, and with regard to ***statutory confidentiality of statistical authorities*** (recitals 162-163).

The *precise meaning* of Article 89(1) GDPR is, however, *debated* in some countries. Pointing to recital 156, as well as to the place in Chapter IX, one could argue that *Member States shall adopt* specific legislation specifying any own required safeguards[15]. Others defend that the same article imposes obligations for the researchers as *controllers* to implement safeguards[16]. Hence, in brief, it is important

[12] Article 89(1) GDPR sets out, that "processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be subject to appropriate safeguards". The safeguards shall be technical and organisational, and ensure in particular that the principle of data minimisation is observed. Article 89(1) also mentions pseudonymisation and anonymised data.

[13] About this notion, aimed to 'ensure a level of security appropriate to the risk', see also Article 32(1) GDPR.

[14] Discussion exists as to whether there should be an order of precedence for data minimisation techniques, i.e. if anonymisation is to be considered in the first place if the research objectives allow, as Article 89(1) GDPR *in fine* states that this 'shall be fulfilled in that manner' where the purposes of the research can be fulfilled 'by further processing'. See also case law, e.g., the CJEU *Huber* case, C-524/06, § 65, in which the Court stated that the statistical objectives of the processing relying on the German Central Register of Foreign Nationals could be reached with only the processing of anonymous data., as no more was 'necessary'. See also recital 156 GDPR. At the same time, the data minimisation requirements could also be fulfilled by *pseudonymisation*, as explicitly stated in Article 89(1) GDPR itself. Some authors also point to the need for privacy by design and by default. See Mondschein, C. F., and Monda, C., 2019, 'The EU's General Data Protection Regulation (GDPR) in a Research Context', in Kubben, P., Dumontier, M., Dekker, A. (eds.), Fundamentals of Clinical Data Science, Springer, pp. 55-74, viewed 5 July 2021, https://link.springer.com/content/pdf/10.1007%2F978-3-319-99713-1.pdf . See also some other authors have criticized the limited guidance in the GDPR about the required safeguards: see, e.g., Portmeister, K., 2017, 'Genetic data and the research exemption: is the GDPR going too far?', International Data Privacy Law, p. 139.

[15] See, e.g. in the Netherlands, Engelfriet, A., e.a., 2018, 'De Algemene Verordening Gegevensbescherming –Artikelsgewijze commentaar', Amsterdam, Ius Mentis, p. 289. See also the text of recital 156: '[…] *The further processing of personal data […] is to be carried out when* ***the controller has assessed the feasibility to fulfil those purposes*** *by processing data which do not permit or no longer permit the identification of data subjects […]. Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. […]*' (emphasis added).

[16] It shall also be noted that not respecting Article 89 GDPR will result in higher administrative fines (see Article 83(5)(c) GDPR).

to retain that discussion exists as to whether or not EEA States should adopt legislation imposing required safeguards for the processing of personal data for scientific research or if it is sufficient that controllers assess the feasibility to conduct the research respecting the data minimisation principle and providing for safeguards themselves, e.g., by means of codes of conduct.

Case law on safeguards for processing for scientific research purposes is overall very limited, both on the international and national level. At the same time, the highest international courts stress the importance of national law. The European Court of Human Rights (ECtHR) has for example stated repeatedly that

> *'[…] protection of […] data is of fundamental importance to a person's enjoyment of his or her right to respect for private life as guaranteed by Article 8 of the Convention. The domestic law must therefore afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article […]. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored, and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored […]. The domestic law must also afford adequate guarantees that retained personal data are efficiently protected from misuse and abuse […]. The above considerations are especially valid as regards the protection of special categories of more sensitive data' […] (emphasis added)'*[17].

The project team therefore argues that EEA States ***shall adopt national law*** specifying the safeguards when personal data is used for scientific research for securing the rights and freedoms of data subjects and to limit any risks after due assessment.

Furthermore, Article 89(1) GDPR covers a wide variety of diverse **science purposes and aims**. This study aims at finding convergences in this *large variety* with different aims and to link the safeguards identified to the type of scientific research and the risks for the data subjects, while not unduly restricting or prohibiting the use and free movement of the data[18].

[17] See ECtHR, P.N. v Germany, 11 June 2020, application no. 74440/17, §§ 70-71. The court further in these paragraphs referred to Article 6 of the Data Protection Convention; see also ECtHR in S. and Marper, § 103; M.K. v. France, § 35; and Peruzzo and Martens, § 42. The same development was made in ECtHR, 26 May 2020, application no. 1122/12, P.T. v La République de Moldavie, § 26. The first reiteration of the Court was in ECtHR, 25 February 1997, Z v Finland, application no. 22009/93, § 95 and followed by multiple references thereafter (e.g., in ECtHR., 27 August 1997, M.S. v Sweden, application no. 20837/92, § 41, ECtHR 17 July 2008, I. v Finland, application no. 20511/03, § 38.

[18] For example, processing for statistical purposes is characterised by bringing together elementary information from individuals making up the (specific) population to describe the characteristics of that population as a whole, while serving distinct purposes such as (i) establishing statistical knowledge as such, (ii) providing assistance to planning and decision-making and (iii) providing researchers with information contributing to understand epidemiology, economics, sociologie etc. Hence, for statistics, personal data used shall be rendered fully anonymous. At the same time, statistics operate on the principle that there should be minimum interference and intervention as to the individuals whose personal data are processed, which is quite different from for example of biological and human sciences, where much of the research is based on experimentation and hence personal intervention (see CoE, Explanatory Memorandum to Recommendation Rec(1997)18 on the protection of personal data collected and processed for statistical purposes, 1997, pp. 5-7). As a result, processing for statistical purposes, as they are totally incompatible with any scientific research relating to individuals or for taking measures in relation to individuals, shall lead in principle always to 'statistical results', and data minimisation should be understood as the statistical data at best not being linked/able or related to identified or identifiable natural persons.

2 ANALYSIS OF NATIONAL LEGISLATION, GUIDELINES AND CODES OF CONDUCT

This section briefly presents the national legislation implementing Article 89(1) of the GDPR as well as the relevant national guidelines and codes of conduct adopted in the selected countries. Section 2.1.1 focuses on national legislation encoding the specific elements of Article 89(1) of the GDPR. Section 2.1.2 addresses the case law of national courts and the related guidelines and codes of conduct.

2.1 GDPR IMPLEMENTING NATIONAL LEGISLATION

2.1.1 Austria: Two sets of legislation and required safeguards

Appropriate safeguards for scientific research purposes are regulated by the Austrian legislator in two main legal acts, namely the Austrian GDPR implementing Data Protection Act (*Datenschutzgesetz*, or *DSG*)[19] and the specific law for research **Austrian Research Organisation Act** (*Forschungsorganisationsgesetz*, or ***FOG***)[2021]. A dedicated national law hence covers research in various domains detailing safeguard requirements.

Article 7 *DSG* distinguishes two processing constellations for scientific research purposes, for which different safeguards apply. The first is processing of personal data for scientific research purposes *which are* ***not aimed at producing personal results***. In this case, the controller may process all personal data which: (i) are *publicly accessible*; (ii) have been *lawfully obtained* by the controller for other research projects or other purposes; or (iii) are *pseudonymised* and the controller cannot determine the identity of the data subject by legally permissible means. The second group encompasses processing for scientific research purposes ***aimed at producing personal results***. In that case, personal data may be processed only (i) in accordance with *special legal provisions* (e.g. the provisions contained in the *FOG*[22]); (ii) with the *consent* of the data subject; *or* (iii) with the *approval* of the Supervisory Authority (SA)[23]. Safeguard requirements hence depend upon aim and effects for the data subjects.

Where the processing of personal data for research purposes is permitted in a form which allows for the identification of the data subject, appropriate normative safeguards include the application of *pseudonimisation* techniques for personal data and *encryption* without delay of the direct references to the data subject should remain possible to identify the individual by legally permissive means. Further safeguards entail the *anonymisation* of personal data as soon as it is no longer necessary for the scientific research, unless otherwise expressly provided by the Austrian law.

Further to the *FOG*, which considers scientific research in a broad manner[24], all personal data may be

[19] *Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten* (*Datenschutzgesetz – DSG*) StF: BGBl. I Nr. 165/1999, viewed 15 December 2020, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597.

[20] *Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation* (*Forschungsorganisationsgesetz – FOG*) StF: BGBl. Nr. 341/1981 idF BGBl. Nr. 448/1981 (DFB), viewed 17 December 2020, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009514.

[21] The *DSG* establishes the general provisions for the processing of personal data for scientific research purposes, which may be superseded, in some cases, by the application of *lex specialis*, such as the *FOG.*

[22] Article 2d(7) of the FOG.

[23] Section 7(3) of the DSG sets forth the conditions for the granting of authorisation by the SA, *i.e.* the impossibility or disproportionate effort of obtaining the consent of the data subject, the public interest of the project, and the demonstrated professional qualification of the data controller. In case special categories of data are to be processed, the concurrence of an "important" public interest is required as well as the occurrence of the processing shall be made at the premises of the controller by persons subject to a statutory obligation of confidentiality or whose reliability is credible.

[24] Scientific research institutes under Article 2(b)(12) of the FOG means natural persons, associations and legal entities pursuing purposes in consonance with Article 89(1) GDPR, irrespective of whether said purposes are *charitable or not* and *irrespective of whether they are accomplished in universities, business or non-university contexts*.

processed in all domains[25], in particular special categories of data, if: (i) instead of the name, **area-specific personal *identifiers*** or other unique identifiers are used for allocation; or (ii) the processing is carried out in ***pseudonymised* form**; or (iii) the processing is carried out ***without publishing* the data**, or publishing the data only in anonymised or pseudonymised form, or publishing the data without names, addresses or photographs; or (iv) the processing is **carried out *exclusively for the purpose of anonymisation* or pseudonymisation** and no disclosure of direct personal data to third parties is involved[26]. Moreover, the FOG recognises 'broad consent' for the processing of special categories of personal data[27]. Other appropriate measures include the establishment of access and logging registries; the respect of the duty of confidentiality; and the avoidance of any disadvantage for the data subjects. Also, controllers need to make *publicly available on the Internet the use of their legal basis*; *delete the name details* in any case if the data are provided with specific personal identifiers; appoint *a data protection officer (DPO)*; arrange *organisational measures*[28].

2.1.2 Belgium: a set of safeguards in the GDPR implementing Act

The GDPR implementing national Act of 30.7.2018[29] specifies the general safeguards (Article 191). In general and overall, the Act states that anonymous data shall be used, and only if the research purpose *cannot be met*, pseudonymous data, and only if the research purpose cannot be met with pseudonymous data, non-pseudonymised data (Article 197) ('waterfall system'). Other safeguards include : (i) the ***appointment of a DPO*** in case of a likely high risk (see Article 35); (ii) specific ***motivation in the records why pseudonymised data is (not) used***; (iii) ***why the rights of the data subjects may endanger or render the purposes impossible***; and (iv) a **data protection impact assessment (DPIA)** in case of use ***of 'sensitive' data*** (besides specific requirements for use for archiving in the public interest as well).

In the case of direct collection, **the data subject *shall also be informed*** whether ***data are anonymised*** or not and why the rights of the data subject may endanger or render the purposes impossible (Article 193). Noteworthy is that in case of indirect collection and re-use, the controller needs ***to conclude an agreement*** *with the initial controller*, safe exceptions[30] to be added to the records (Article 196). This agreement contains the contact details of the controllers and why the rights of the data subjects may endanger or render the purposes impossible (Article 195). Belgian law requires a detailed agreement between the initial controller and new controller for secondary processing for research. The remaining articles contain further *specific requirements for pseudonymisation* (Articles 198 – 204), and *for dissemination and publication* (Articles 205-208).

2.1.3 Bulgaria: no additional specifications

The GDPR implementing national Personal Data Protection Act[31] provides that personal data may be processed for purposes other than (i) National Archive Funds, (ii) scientific research, (iii) historical

[25] In particular in the context of Big Data, personalised medicine, biomedical research, biobanks and the transfer to other scientific institutions and processors, according to Article 2(d)(2)(1) of the FOG. It is also stated that further processing of personal data for scientific research purposes do not constitute unlawful purposes, its storage can be made without restriction and, if necessary, otherwise processed, provided that no time limits are stipulated by law.
[26] Article 2(d)(2)(1) of the FOG.
[27] Article 2(d)(3) of the FOG. In this case, the purpose is replaced by one or several fields of research or certain research projects or parts of them.
[28] These include explicitly defining the distribution of tasks and authorised orders for processing; *instructing* every employee about the organisational obligations under *FOG* and data protection framework, including data security regulations; implementing access control procedures, mechanisms and areas; incorporating input control mechanisms and documentation measures to preserve evidence; completing a signed declaration as regards confidentiality and responsible use and access of the personal data by authorised persons; and deleting named data after transmission when the purposes pursuant to Article 89(1) GDPR have been achieved.
[29] Act of 30.7.2018.
[30] In particular if (i) the data were made public or (ii) law provides a mandate for doing research, and (ii) re-use for other purposes is forbidden. The initial controller shall be informed if such exception applies: see also art. 194.
[31] Personal Data Protection Act (*Закон за защита на личните данни*), viewed 5 July 2021, https://www.cpdp.bg/en/index.php?p=element&aid=1194.

research, or (iv) statistical purposes. Article 25m stipulates that the controller shall apply appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject. The provisions further refer to Article 89(1) of the GDPR. Bulgaria's national implementing legislation hence does not contain additional specifications.

2.1.4 Estonia: broad notion of research and GDPR role for ethic committees

The GDPR implementing the national Estonian Personal Data Protection Act[32] requires verification of compliance prior to conducting studies for the purpose of scientific research and policy development by the relevant ***ethics committee*** **or the** ***Estonian Data Protection Inspectorate (SA*****),** depending on **whether** ***sensitive data*** **is processed**[33]. Ethic committees hence have an explicit GDPR role. Prior to its transmission to the researcher, personal data that is processed for the purpose of scientific and historical research and official statistics *without consent* of the data subjects should be **pseudonymised, or processed using "*a format which provides equivalent level of protection*"**[34]. However, processing *in a format that enables identification* without the consent of the data subject is also allowed when *three cumulative* conditions are met, namely: (i) 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; (ii) there is *overriding public interest* for it; and (iii) 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[35]. In addition, Estonian law **permits de-pseudonymisation** (changing the information "back-wards", and thereby enabling identification of persons) "*for the needs of additional scientific and historical statistics or official statistics*" in this case, data processors must **designate the specific person who has access** to the information which allows pseudonymisation[36].

Research carried out for the *purpose of* ***policy development*** by the executive power (i.e. the Government, meaning the Prime Minister and ministers) **falls within** the definition of "*scientific research*"[37], which allows the executive power to request and, subsequently, process personal data from controllers' or processors' databases. Estonia hence maintains a broad notion of research.

2.1.5 Finland: safeguards linked to derogations from rights and role for codes of conduct

The GDPR implementing national Finnish Data Protection Act[38] does not define "scientific" or "historical" research. However, it is suggested that "scientific research" should be understood in the way it is *perceived by the general public* and *fulfil general criteria for what constitutes scientific* research[39]. Pursuant to the preparatory works, the freedom to conduct scientific and historical research, including

[32] Personal Data Protection Act, 12.12.2018, viewed 5 July 2021, https://www.riigiteataja.ee/en/eli/523012019001/consolide.
[33] Section 6 of the Personal Data Protection Act. The purpose of scientific research requires verification by the relevant ethics committee or by the SA. For policy development, verification by the SA is required, unless otherwise provided by law. See Section 6(5) of the Personal Data Protection Act: Unless the objectives of the intended study and the scope of processing of personal data for its purpose derive from legislation, the Estonian SA shall verify the compliance with Section 6 of the Estonian Data Protection Act prior to the beginning of the "specified processing of personal data". See also Section 6(4) of the Personal Data Protection Act: For the processing of personal data of specific categories, an ethics committee of the concerned domain or, in case such a committee does not exist (e.g., for personal data retained at the National Archives, the National Archive functions as the ethics committee) the Estonian SA will verify compliance with Section 6 of the Personal Data Protection Act (Note that the English translation of the Act uses the wording "verify compliance with the terms and conditions provided for in this section").
[34] Section 6(1) of the Personal Data Protection Act.
[35] Section 6(3) of the Personal Data Protection Act.
[36] Section 6(2) of the Personal Data Protection Act.
[37] Section 6(5) of the Personal Data Protection Act.
[38] Data Protection Act (1050/2018, *Tietosuojalaki*), viewed 5 July 2021, https://www.finlex.fi/fi/laki/kaannokset/2018/en20181050.pdf (unofficial translation). This act implements GDPR.
[39] As described in the preparatory works to the Personal Data Protection Act, Hallituksen esitys HE 9/2018 vp, available at https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_9+2018.aspx (Finnish and Swedish only).

the right to choose freely the research subjects and research methods, is protected by the Finnish Constitution[40]. Regarding the legal basis for processing personal data for scientific, historical or statistical research purposes, the preparatory work refers to Article 6(1) GDPR and states that such legal basis can be either consent or legitimate interest. As regards the purpose limitation, personal data can be processed if necessary and proportionate to the general interest pursued, and the *data controller* must be able to prove that these criteria are met[41]. However, since it is not always possible to identify the purpose of processing personal data for scientific research purposes while collecting the data[42], the data subject should be able to consent *to certain areas of scientific research*, where *acknowledged ethical standards* for scientific research are observed.

In order to benefit from the exceptions for scientific, historical research or statistic purposes, the data controller needs to draw up a *research plan*[43]. The Finnish legislation also allows for the processing of *sensitive data* for the purposes of scientific research[44]. However, when sensitive data is concerned, the research in question shall fulfil generally approved *ethical principles for science*. Furthermore, when processing the *national identification number*, which is a special type of personal data, for scientific research purposes, an effort should be made to obtain *consent* of the data subject[45]. The Act further *enables derogations from Articles 15, 16, 18 and 21 of the GDPR* when personal data is processed for scientific research[46]. The *safeguards required in this case are very similar to those when processing sensitive* data, and when relying on Article 9.2(j) GDPR (see below). One could say that in Finland, the required *safeguards are largely linked to data subject rights* (and the derogations thereto).

In addition to the extensive data protection mechanisms of the GDPR[47], the safeguards for processing of *special categories of personal data*[48] and personal data relating to criminal convictions and offences[49], Section 31(3) sets *specific requirements*[50] and requires in addition *either* carrying out a DPIA[51], which must be submitted in written to the Finnish SA, the Data Protection Ombudsman[52], 30 days prior to the processing. *Alternatively*, compliance with *codes of conduct* that take into account derogations of Section 31(1) of the Finnish Data Protection Act must be ensured[53]. In Finland, for sensitive data, controllers shall hence choose between submitting for review to the SA or abiding by a code of conduct.

[40] *Hallituksen esitys HE 9/2018 vp*, viewed 7 July 2021, https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_9+2018.aspx (Finnish and Swedish only). The Finnish Data Protection Act preserves this approach, and should hence be seen as completing the GDPR within the discretion of the EEA States.
[41] *Highlighted in HE 9/18 vp*, p. 50, also referring to Article 5(2) of the GDPR.
[42] The preparatory work also references Recital 33 GDPR in this regard.
[43] Section 31(1) of the Data Protection Act.
[44] Section 6, point 7 of the Data Protection Act. The Finnish Data Protection Act allows for processing of personal data of special categories for scientific and historical research or statistics. In such cases, Article 9(1) of the GDPR is not applied.
[45] HE 9 /2018. National identification numbers can be processed, if it is necessary for the historic, scientific research or for statistics to "uniquely identify" the data subject. See Section 29 of the Data Protection Act.
[46] This requires that (i) the processing is based on an appropriate *research plan*; (ii) a person or group *responsible* for the research has been designated; and (iii) the personal data are used *and disclosed only for scientific* or historical research purposes or for other compatible purposes, and the procedure followed is also that data concerning a given individual are *not revealed to outsiders*. See Section 31(1) of the Data Protection Act. Exceptions from this provision are justified when exercising the rights would jeopardise the specific purpose of the research or make it too hard to fulfil it, when such exception is needed to achieve the purpose of research. For example, the preparatory works mention a situation where data is fully pseudonymised and the data controller is not in possession of the data key. In such a case, the data controller should assess, on a situation-based approach, whether it is necessary to use the exception.
[47] Also extensively described by the Data Protection Ombudsman on the webpage, viewed 23 March 2021, https://tietosuoja.fi/en/rights-of-the-data-subject-in-scientific-research.
[48] Article 9(1) GDPR.
[49] Article 10 GDPR.
[50] Section 31(3) Data Protection Act.
[51] Article 35 GDPR.
[52] All the duties of the Data Protection Ombudsman are described in detail at https://tietosuoja.fi/en/duties (mostly compliance with data protection legislation and imposition of admin sanctions).
[53] See also Article 40 GDPR. Those codes of conduct must appropriately take into account the rights of the data subjects, as described in Articles 15,16, 18 and 21 of the GDPR. See also Section 31(3) Data Protection Act.

For relying on Article 9.2(j) GDPR for the processing of sensitive data[54], scientific safeguards include (i) an appropriate confidential[55] *research plan*[56] (i.e. to ensure that the processing takes place for *scientific* research) for research that fulfils state-of-the-art, general research *ethical principles* (especially for processing of special categories of data); (ii) a designated (group of) *person(s) responsible for the research*[57]; and (iii) for the personal data to only be disclosed for historic or scientific research purposes and *not to be revealed to outsiders*[58].

2.1.6 France: safeguards linked to derogations from rights and SA- centric role for sensitive data

Article 4 of the French GDPR implementing national act[59] states that further processing for scientific research is deemed to be compatible with the initial purposes if: (i) compliant with the GDPR and the French GDPR implementing law and (ii) is *not used to make decisions about the data subject*[60].

Article 78 of the same act further states that a decree issued after consulting the French Supervisory Authority (*Commission Nationale de l'Informatique et des Libertés* or *CNIL*) shall determine under what conditions and guarantees the rights provided for in Articles 15, 16, 18, and 21 GDPR may be waived for processing for scientific research purposes. France hence links the safeguards with the data subjects' rights. Article 116 of the implementing decree n°2019-536 of May 29[61] states that the data resulting from processing for scientific research purposes - kept by the controller or his or her subcontractor, **can only be accessed or modified by authorised persons**. These people must *respect the rules of* ***ethics applicable to their sectors of activity***. Further, personal data for the above-mentioned purposes **cannot be disseminated** without having been **previously anonymised** unless the interest of third parties in this dissemination prevails over the interests or fundamental rights and freedoms of the person concerned[62]. The dissemination of personal data appearing in documents from public archives can only take place after **authorisation from the archives' administration, after agreement of the authority from which the documents are issued, and after the opinion of the statistical confidentiality committee.** In France, the general required *safeguards are linked to the derogations from data subject rights.*

Processing of **sensitive data** necessary for public research is allowed, if conditions from Article 9(2) GDPR and Article 44.3 and 65 of French Data Protection Act[63] are met. This means, for example, either an **explicit consent**, or a prior **opinion/authorisation[64] of the CNIL** about particular processing[65]. Such an exemption from the prohibition on collecting sensitive data, provided for in Article 44.6 of the French Data Protection Act, is limited to public research (and therefore cannot be evoked for private research). Other prerequisites from Article 9.2 GDPR are also applicable, such as when data is clearly made public by the data subject or for reasons of public interest on the basis of text of national law.

[54] Section 6(1) of the Finnish Data Protection Act.
[55] Section 24, point 21 of the Act on the Openness of Government Activities, 621/1999, as amended by 907/2015, viewed 5 July 2021, https://finlex.fi/en/laki/kaannokset/1999/en19990621_20150907.pdf (unofficial English translation).
[56] Section 31(1) of the Finnish Data Protection Act.
[57] Idem.
[58] Idem. According to the Data Protection Act, a later use of the data is only allowed for historical or scientific research, or other appropriate purposes, such as statistical purposes.
[59] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés..
[60] See also Article 4.5: For scientific research, the storage limitation principle applies according to the purpose of the research.
[61] Article 116 - Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - Légifrance (legifrance.gouv.fr), viewed 7 July 2020.
[62] For research results, this dissemination must be necessary for its presentation. The data disseminated must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.
[63] Article 44.3, Article 65 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[64] See further page 76 the topic about CNIL methodologies for health and medical research.
[65] Article 44.6 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

French Law distinguishes between scientific research for health purposes[66] and for other purposes[67]. This distinction has direct consequences on data subject rights. For example in health research the data subject can oppose without giving a motive)[68]. Moreover, different requirements apply to health research (further explained in the next part of the report).

2.1.7 Germany: federal and state level legislation

At the federal level[69], the German GDPR implementing national Federal Data Protection Act (*Bundesdatenschutzgesetz*, or *BDSG*)[70] provides for general rules and requirements for the processing of personal data for scientific research purposes in the public and the private sector. Article 27(1) *BDSG* allows for the processing of special categories of data without the data subject´s explicit consent if the processing is necessary for the purpose of scientific research and the interests of the controller in processing "substantially" outweigh those of the data subject. However, the controller shall take, in any case, appropriate and specific measures to safeguard the interests of the data subject, in accordance with Article 22(2) of the *BDSG*. These measures explicitly include the **encryption and pseudonymisation** of personal data, but also cover the general **technical and organisational** measures laid down by Article 32 of the GDPR[71]. In addition, Article 27(3) *BDSG* imposes **anonymisation** of *special* categories of personal data processed for scientific research purposes ""as soon as the research purpose allows", except when this conflicts with legitimate interests of the data subject. Until such time, the *BDSG* requires the characteristics enabling information concerning the individual be **stored separately**, and only be combined to the extent required by the research purpose. Lastly, Article 27(4) of the *BDSG* establishes *prior consent* from the data subject as a requirement for the **publication** of personal data[72].

At *Bundesländer* level, Article 24(1) of the Hessian Data Protection and Freedom of Information Act (*Hessisches Datenschutz- und Informationsfreiheitsgesetz* or *HDSIG*)[73] excludes the term "substantially" when assessing the interest of the controller against the data subject for the processing of special categories of data without the data subject´s consent. Although this may imply more lenient requirements in the *Bundesland* of Hesse, said article further introduces **additional safeguards** as to the start of the research project. The draft of a **"data protection concept" (*Datenschutzkonzept*) prior** to the outset of the research project is required and shall be submitted to the responsible SA upon request. Other divergencies with respect to Article 27 of the *BDSG* include the moment in which the **separate** storage of characteristics relating to the data subject shall occur[74]. Germany attaches importance to a 'data protection concept' plan.

[66] Article 72 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[67] Article 78 and 79 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[68] Input from the French SA.
[69] The German federal system provides for a top-down implementation of the GDPR into the national legislation. Legislative competences pertaining to the appropriate safeguards required by Article 89(1) of the GDPR are split up into a multiplicity of federal (*Bund*) and state (*Bundesland*) provisions. At state level, each *Bundesland* has its own general data protection act, which may modify or extend the safeguards provided by the BDSG.
[70] Recht, G.: Bundesdatenschutzgesetz (BDSG): G. Recht, 2014, viewed 20 December 2020, https://www.gesetze-im-internet.de/bdsg_2018/.
[71] These include in particular measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services, the designation of a DPO; the arrangement of personnel training; the setting of test, assessment, and evaluation processes for ensuring security; and the introduction of rules of procedure for data transfers and further processing.
[72] There is, however, an exception to this rule, namely when the publication of such data is indispensable for the presentation of research findings on contemporary events.
[73] Hessischen Gesetzes zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit vom 3. Mai 2018 (GVBl. S. 82), viewed 14 January 2021, https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHEV1IVZ.
[74] Here, Article 24(3) HDSIG provides that separate storage is made "as soon as the scientific research purpose permits", thus deviating from the more stringent criteria included in Article 27(3) of the BDSG, where the separation of such characteristics is made "until" the time in which the special categories of data can be anonymised. Notwithstanding the previous, the HDSIG raises the legal bar again by including, at the end of said Article, a supplemental duty to delete the characteristics as soon as the scientific research purpose permits.

2.1.8 Greece: specific safeguards for sensitive data processing without consent

Article 30 of the Law 4624/2019[75] introduces a derogation from the prohibition of processing special categories of data without the data subject´s consent where the *processing is necessary for scientific research purposes and* ***the interest of the controller overrides the*** **interest** of the data subject. Suitable and specific measures to protect the data subject´s legitimate interests shall be in place, such as in particular, (i) *access rights restrictions* to controllers and processors; (ii) *pseudonymisation* of personal data; (iii) *encryption* of personal data; and (iv) *designation of a DPO*. In addition to these measures, *anonymisation* of special categories of personal data where processed for scientific research purposes is to be implemented as soon as the scientific purpose allows, unless it is contrary to the legitimate interest of the data subject[76]. Greece hence imposes specific safeguards including anonymisation in case of processing without consent for necessity for scientific research and a controller's overriding interests.

Article 30 of the Law 4624/2019 further specifies that the controller may be allowed to *publish* personal data processed in the context of research, if the data subjects have given their *consent* "in writing" or the publication is *necessary* for the presentation of the results of the research. In the latter case, it is provided that the results shall undergo *pseudonymisation* before being published.

2.1.9 Iceland: the need for appropriate security

Article 18(1) of the Icelandic GDPR implementing national Data Protection and the Processing of Personal Data Act No.90/2018[77] largely follows the wording of Article 89(1) GDPR and prescribes appropriate safeguards for processing for scientific or historical research purposes, such as technical and organisational measures[78]. Only *data minimisation* is explicitly mentioned as one of such safeguards. While the Act provides that the data cannot be kept in a form which allows identification of the data subject for longer than is necessary considering the purpose of processing, archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are excepted from that main rule, provided that "***appropriate security***" is considered[79]. The same reference to appropriate security is also included in the provision on purpose limitation[80]. Iceland points mainly to the need for appropriate security.

2.1.10 Italy: reference to establishing codes of conduct

Appropriate safeguards relating to scientific research purposes is regulated in Title VII, Chapter III of

[75] Law 4624/2019 Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions, Government Gazette (137/A/29-08-2019), viewed 23 January 2021, https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF.

[76] Article 30 also requires that until that moment, the characteristics that can be used to match individual details of the data subject must be stored separately, and only be combined if required for research purposes.

[77] Article 18(1) of Act No. 90/2018 on Data Protection and the Processing of Personal Data (2018 *Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga*) , viewed 5 July 2021, https://www.personuvernd.is/media/uncategorized/Act_No_90_2018_on_Data_Protection_and_the_Processing_of_Personal_Data.pdf.

[78] See also the mentioning that derogations from some GDPR rights are allowed: the right to access, to rectification, restriction of processing and the right to object to the processing shall not apply where personal data are only processed for scientific or historical research purposes or for archiving purposes, to the extent that the rights would make it impossible or seriously impair the achievement of the purposes of the research. See Article 18 of the Act on Data Protection and the Processing of Personal Data.

[79] Article 8(5) of the Act on Data Protection and the Processing of Personal Data.

[80] Further processing for historical, statistical or scientific purposes is not considered incompatible with the initial purpose for which is was collected, "provided that appropriate security is taken into consideration". See Article 8(2) of the Act on Data Protection and the Processing of Personal Data. Interestingly, the wording of the provision seems to suggest, that the consideration of security is conditional for whether the processing is compatible with the purpose limitation in Article 8(2) and (5).

the GDPR implementing Personal Data Protection Code (*Codice in materia di protezione dei dati personali* or *PDPC*)[81]. Article 105 PDPC establishes the duty on "controllers or others" to unambiguously *specify* the purposes of the scientific research as well as *to make them known* to the data subject in accordance with Articles 13 and 14 of the GDPR. Said article also imposes a *prohibition to process personal data for decision-making purposes* on the data subject or else with a view to processing data for different purposes. Article 106 PDPC puts additional onus on the Italian SA (*Garante*) to ***encourage the adoption of rules of conduct*** *by the private and public entities* that are involved in processing data for scientific research purposes. The Rules of Conduct shall comprise specific measures[82], which have to be interpreted against Articles 99, 107, 110, 110-a of the PDPC. The Rules of Conduct have been adopted and attached to the PDPC. Among them, a set of rules concerns the processing of personal data for scientific research purposes[83] and another set of rules concerns the processing of personal data for the provision of Official Statistics[84]. Compliance with such rules is a fundamental precondition for the processing of personal data. Italy hence encourages and emphasises the development of codes of conduct for research.

2.1.11 Norway: role of public interest and no exceptions to the rights of data subjects in case of legal effects

The Norwegian GDPR implementing national Data Protection Act[85] allows personal data to be processed on the basis of Article 6(1) GDPR for the purpose of "*public interest, purposes related to scientific or historical research or statistical purposes"* and in compliance with 89(1) GDPR and its rights and principles[86]. Article 8 of the Act also serves as a legal basis to pass national laws related to the processing of personal data for the aforementioned purposes. The Act further states that the processing for the aforementioned purposes must provide the necessary guarantees as stated in Article

[81] Personal Data Protection Code containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, as amended by Law No 160 of 27 December 2019, viewed 24 January 2021, https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/.

[82] These measures include (i) the prerequisites and procedures to demonstrate and verify that the data are processed for *appropriate scientific research purposes*; (ii) storage period specification, the information to be provided to data subjects in respect of the data collected also from third parties, communication and dissemination of the data, the selective criteria to be implemented in processing identification data, the specific security measures and the mechanisms to amend the data as a result of the exercise of data subjects' rights, by taking account of the principles laid down in the relevant Council of Europe's Recommendations; (iii) the means that can reasonably be used by controllers or others in order *to identify* a data subject; (iv) the safeguards to be complied with *if the data subject's consent is unnecessary*, by having regard to the principles laid down in Council of Europe´s Recommendations; (v) simplified arrangements for the consent of the data subjects as regards *special categories of data*, where required, *e.g.* the data subject's consent shall not be required for scientific research purposes for reasons of *public interest in the area of public health the medical, bio-medical or epidemiological sectors* if a DPIA is carried out and published, it shall also not be required if informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or if it *is likely to render impossible or seriously impair the achievement of the research purposes*, subject to the *positive and reasoned assessment of the research project by the competent ethics committee* as well as the *prior consultation of the Data Protection Authority* in accordance with Article 36 of the GDPR; (vi) the fairness rules applying to data collections and the arrangements for the processing of data by persons under the authority of the controller or processor; (vii) the measures to be adopted in order to promote *compliance with the data minimization principle* and the technical and organisational measures referred to in Article 32 of the GDPR, particularly by having regard to access control mechanisms to avoid unauthorized access and data transfers; (viii) security and confidentiality measures of authorized and non-authorized processing; (ix) measures for minimization and anonymization of the data in case further processing of personal and special categories of data by third parties is allowed by the *Garante*; (x) compliance measures in relation to Article 89(1) of the GDPR where the processing of personal data is terminated and such data is *kept or transferred to another data controller* for scientific research purposes.

[83] Annex 5 of the PDPC.

[84] Annex 4 of the PDPC.

[85] Data Protection Act (*Personopplysningsloven*), LOV-2018-06-15-38, viewed 5 July 2021, https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysning.

[86] Unofficial English translation of Paragraph 8. The relevant Norwegian Ministry has noted in the preparatory works of the Data Protection Act that it is not "*practical to try and specify these guarantees further*" in the Act, while the processing must, however, be in accordance with the GDPR's other provisions, including its principles. See reply by the Norwegian SA and the information provided in the questionnaire to the EDPB.

89(1) of the GDPR, but the Act does not provide any specifications and/or references to additional safeguard other than those of Article 89(1) GDPR.

The processing of **special categories** of personal data *without* consent is only permitted if it is necessary for archiving purposes in the public interest, purposes related to scientific or historical research or statistical purposes[87]. and if the public interest "*clearly outweighs the inconveniences for the individual*". Prior to carrying out such processing, the controller *is **required to consult** with the DPO* or another party which fulfils the requirements set out in Article 37(5) and (6) and Article 38(3) GDPR regarding compliance of the planned processing with the GDPR requirements as well as with other relevant provisions of the Norwegian Data Protection Act[88]. Such consultation is ***not* required in case a DPIA is carried out**. The consultation obligation also applies to the processing of personal data of special categories, *even if the processing is based on consent of the data subject*[89]. The *SA can further grant **permission** to process special categories of personal* data for "the sake of important public interests"[90]. (Important) public interest hence plays an important role in Norway. In that case, the SA shall establish conditions for safeguarding the data subject's fundamental rights and interests[91]. The Act further also provides *exceptions to data subject's rights* when processing personal data for scientific purposes with reference to Article 89(1) GDPR[92]. Interestingly, these exceptions to the rights of data subjects do not apply in situations **where the processing has legal effects** of direct actual effects for the data subjects[93].

2.1.12 Poland: no additional legal requirements

In the GDPR implementing Personal Data Protection Act[94], Poland does not provide any additional safeguards, except those already present in Article 89(1) GDPR, which means **pseudonymisation** and **data minimisation** where possible. Poland stipulates no additional requirements in framework legislation.

2.2 NATIONAL GUIDANCE DOCUMENTATION, CODES OF CONDUCT AND CASE LAW

We hereunder describe national guidance documentation, codes of conduct and case law where these are defining appropriate safeguards in the different countries. National guidance documentation refers to non-binding governmental documents, including guidelines, opinions, decisions of SAs, as well as notices and communications, and non-governmental regulations or documentations (industry codes, research institute's guidelines), if any. This section is based on the input received in the questionnaires and limited desk research. In case of absence of sufficient relevant information, the country is not mentioned.

2.2.1 Belgium: guidance by the SA and the national research council

In general, there is discussion as (i) to whether or not EEA States should adopt legislation imposing required safeguards for the processing of personal data for scientific research (see above) and as (ii) to the reach of the national provisions with regard to the safeguards mentioned in Article 189 et seq. Act

[87] Paragraph 9, referencing Article 9(1) GDPR.
[88] Section 9(2) of the Norwegian Data Protection Act.
[89] Section 10 of the Norwegian Data Protection Act.
[90] Section 7 of the Norwegian Data Protection Act.
[91] Idem.
[92] The exceptions only apply if the burden caused by providing is disproportionate or the right to access is likely to make it impossible / seriously prevent objective of the research. See Section 17 of the Norwegian Data Protection Act.
[93] Section 17(2) of the Norwegian Data Protection Act.
[94] Act of 20 July 2018 The Law on Higher Education and Science, viewed 7 July 2021, act-of-20-july-2018-the-law-on-higher-education-and-science.pdf (konstytucjadlanauki.gov.pl).

30.7.2018[95]. The Belgium SA[96], the advising *Conseil d'Etat*[97] and some scholars are of the opinion that the obligation to implement safeguards is (directly) imposed upon the controllers. The argument is that if one would require national legislation specifying safeguards, this would imply that, in absence thereof, no research would be possible.

Further guidance was given by the SA under the previous regime under the Data Protection Directive 95/46/EC, including by brochures. In the domain of **higher education,** the **National Research Council** developed guidance for use of data in research, including personal data, for research and how to develop a *data management plan* to researchers when using personal data. This requirement is aligned with the guidance on European level by Science Europe (see below).

2.2.2 Estonia: Code of Conduct for Research Integrity

In the domain of **higher education**, the Estonian **Code of Conduct for Research Integrity** is set up by Estonian universities and developed in cooperation with the Estonian Academy of Science, the Estonian Research Council and the Estonian Ministry of Education and Research[98]. It addresses a wide variety of topics related to research, including privacy and data protection. The Code of Conduct requires that *prior, informed consent is always requested in immediate studies of people* and when personal data are collected from them[99]. If it is necessary for the aim of the research, consent can also be requested after the collection of the data. In that case, the potential harm of the collection of data for the data subjects needs to be considered, and the researcher *needs prior approval of the ethics committee*. The researcher also has extensive obligations to *inform* the data subject about his/her rights[100]. The Code of Conduct also requires *records* of the collection and the analysis of the data[101]. The researcher needs to adhere to principles and regulations regarding the protection of personal data, but the researcher should also ensure *broad access to the data whenever possible*[102]. Additionally, personal data (cf. "personalised" data) should be *stored for as long as possible*, taking into account the interest of the data subjects and the research[103]. Finally, the researcher must ensure *integrity and safety* when storing data (not only personal). This also entails *proper destruction* of data when needed[104].

2.2.3 Finland: limited concept of scientific research, detailed guidance by the Ombudsman, importance of the research plan and guidelines for higher education

The Finnish Data Protection **Ombudsman** provides extensive guidance[105] on scientific research and data protection. The *characteristics and* ***the needs to meet the concept of scientific research*** is detailed

[95] De Bot, D., 2020, 'De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit', Mechelen, Wolters Kluwer, pp. 351-353.
[96] SA, Advice 33/2018, § 272.
[97] The *Conseil d'Etat*, when providing its comments to the proposed Act of 30.7.2018, stated that the GDPR does not allow EEA States to provide a general deviating regime for personal data processing for scientific research: Adv. RvS, N°63.192/2 of 19 April 2018, 442.
[98] Estonian Code of Conduct for Research Integrity, viewed 5 July 2021, https://www.eetika.ee/en/ethics-estonia/estonian-code-conduct-research-integrity.
[99] Point 2.1.2 of the Estonian Code of Conduct for Research Integrity, viewed 5 July 2021, https://www.eetika.ee/et/2-conduct-research#11.
[100] For example, what data (and in which form) is being collected and its access regime, the right to withdraw consent, the risk and the benefits of the study, the data storage period and any other aspect which may have an impact on the decision to participate: see Points 2.1.3 and 2.1.4 of the Code of Conduct for Research Integrity.
[101] Point 2.2.3 of the Code of Conduct for Research Integrity.
[102] Points 2.2.5 and 2.2.6 of the Code of Conduct for Research Integrity.
[103] Point 2.2.7 of the Code of Conduct for Research Integrity.
[104] Point 2.2.9 of the Code of Conduct for Research Integrity.
[105] See the Finnish Data Protection Ombudsman website, viewed 5 July 2021, https://tietosuoja.fi/en/scientific-research-and-data-protection.

by the Ombudsman, with consequences for the needed legal basis as well[106]. In this context, the importance of *the research plan* is highlighted as a possibility to demonstrate that the data processing is indeed for scientific or historical research purposes[107]. The Data Protection Ombudsman further points out the importance of *following methodological and ethical standards* when evaluating the scientific nature of a research project as well as for the research in general. This is especially important for when personal data of special categories are processed. In practice, *ethical evaluation and ethics committee opinion* is needed *before* launching a research project[108].

The Data Protection Ombudsman draws up *inter alia a data protection roadmap* for the scientific research in great detail, sets out the required *technical and organisational safeguards specific* for research, also at *the end of the research*, and also listed in detail the duties especially of the controller, while highlighting the need *to define the responsibilities of different data processing partners* (data controller and processors, sub-processors)[109]. The **Administrative Supreme Court** denied access to confidential information possessed by the Social Insurance Institution of Finland (Kela) on medical prescriptions for scientific research data[110]. Kela had previously denied a request based on shortages in the research plan[111]. Due to these shortages in how the research was to be carried out and the doubts as to the scientific nature of the research, the Supreme Administrative Court concluded that the decision to deny access to the information was duly motivated[112].

In the domain of **higher education,** guidance also exists on the homepages of the different universities and other public institutions.

[106] The Ombudsman states: "*Scientific and historical research entails an **expectation of increasing the amount of information available to the public**. For example, by combining data from different data files, scientists can obtain valuable **new information** on things like endemic diseases, such as cardiovascular disorders, cancer and depression. Research results obtained from data files offer reliable knowledge that can serve as a basis for drafting and implementing **informed policies**, **improve the lives** of many individuals and increase the **effectiveness of services.**"* As to the need for a different legal basis, see also below, footnote 302.

[107] Please note that in Finland, not all research is considered scientific research. The Data Protection Ombudsman point out the importance of *following methodological and ethical standards* when evaluating the scientific nature of a research project as well as for the research in general. This is especially important for personal data of special categories. See also above about the concept of scientific research in the guidance by the Ombudsman.

[108] *Ibid.* This is considered as an evaluation of the ethics, and not a data protection audit or a basis for processing personal data.

[109] See also in more detail Annex 2 by way of illustration.

[110] Supreme Administrative Court decision 22.11.2013/3651 KHO:2013:181, viewed 5 July 2021, https://www.finlex.fi/fi/oikeus/kho/vuosikirjat/2013/201303651. A company engaged in medical-epidemiological research had applied for a research permit as per the Act on the Openness of Government Access (see Act on the Openness of Government Activities, 621/1999, as amended by 907/2015, viewed 5 July 2021, https://finlex.fi/en/laki/kaannokset/1999/en19990621_20150907.pdf (unofficial English translation)) in order to be able to use information possessed by the Social Insurance Institution of Finland (Kela) on medical prescriptions. The request was made specifically to have the information in an anonymised form.

[111] The research plan did in itself fulfil the qualitative requirements which could be expected from an appropriate research plan and the researchers had sufficient competence to do research. Nevertheless, some unclarities remained regarding the scientific nature of the research, especially since the company financing the research would be able to collect substantial information about the buying patterns and the use of medications. The possibility of the company to influence the publications following the research was also not completely ruled out. It was not possible to determine that the purposes of the research were merely scientific.

[112] It is interesting to note, that as such, the research plan as well as the competence of the researchers was considered sufficient. The information was also requested in an anonymised format. In access to the information possessed by the public authority, the doubts to the scientific nature overruled those formal safeguards taken.

2.2.4 France

The French SA, the CNIL, provides guidelines about the security of personal data[113], anonymisation[114] and about passwords[115] and rules for the protection of personal data in general, also applicable to processing personal data for the purpose of research. The Centre National de la Recherche Scientifique (CNRS) or the **Scientific Research National Center** also provides in its Research Guide additional safeguards in the domain of research[116]. The guidelines underly that protecting access to the database, in which personal data are stocked, is a basic precondition for its safety[117]. The data in the research project shall have *a defined life*-cycle, determined by the purposes for which they were collected[118]. However, if data are needed to be archived and used for research, and for this reason cannot be deleted once used, they should be *archived in three steps*. The first step concerns the processing data during the research project. The second phase is intermediary archiving of personal data, with restricted access to it, provided that it is justified in the context of research and data subjects' rights are respected[119]. The third phase relates to data, which cannot be deleted, in the context of the research project, and has to be kept. In certain cases, these data **shall be archived** and processed according to the rules in Chapter 2 of Code du Patrimoine[120]. Archiving the personal data shall not be done in the laboratory, where research projects have been conducted. The process should be conducted with the help of relevant local or national authorities, and **in compliance with the Code du Patrimoine**. The time of archiving the personal data should be defined and stated in a transparent manner, for all potentially concerned.

If research is about to be undertaken with *external partners, a contract should be signed*[121]. Universities issued guidelines as well, such as the Universite Paris Nanterre, Universite Paris Lumiere, and Universite Paris 8[122].

---

[113] CNIL, Guide sécurité des données personnelles, viewed 5 July 2021, https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf. Guidelines provide measures and safeguards such as: (i) educate and make processors sensitive to security issues, also introduce procedures of exploitation of data, and classification of data processed, where people processing data contractually oblige themselves to preserve their confidentiality; (ii) establish identifiers and passwords for those, who are permitted to access personal data, where passwords need to be complicated, robust enough and stored securely, as to protect the access to personal data; (iii) limit and manage access to personal data for each person allowed only to those data that is necessary for the research; (iv) trace the access to personal data, through proper software and documentation; (v) secure places, where data can be accessed, through state-of-art antivirus software, good quality hardware, and against fraudulent physical access; (vi) secure the servers, on which data reside; (vii) secure the websites, through which databases can be accessed; (viii) archive data not necessary for everyday use in a secure way: (ix) manage properly risk related to cooperation with sub-contractors, and sharing data with third parties; (x) evaluate constantly the level of security of the whole system.

[114] CNIL, L'anonymisation de données personelles, see in L'anonymisation de données personnelles, www.cnil.fr/fr/lanonymisation-de-donnees-personnelles, , viewed 8 August 2021.

[115] CNIL, Authentification par mot de passe: les mesures de sécurité élémentaires, viewed 5 July 2021, https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires.

[116] CNRS, Les sciences humaines et sociales et la protection des données à caractère personnel dans le contexte de la science ouverte, Guide Pour la Recherche, viewed 5 July 2021, guide-rgpd_2.pdf (cnrs.fr).

[117] Idem, Section 2.2. In order to protect the database, the guidelines propose that: (i) there should be a way to identify people accessing the database, through numeric certificates and passwords; (ii) only people appointed by the research leader shall have access to the database; (iii) devices on which database is, or through which it can be accessed shall be protected by the password; (iv) internal informatic system shall be duly protected; (v) as well as the exchange of data between researchers.

[118] Idem, Section 2.4.

[119] Intermediary archiving usually shall be done for no longer than two years, after the publication of the results of the research.

[120] Act of 20 February 2004 Code du patrimoine, viewed 7 July 2020, Légifrance - Droit national en vigueur - Codes - Code du patrimoine (legifrance.gouv.fr).

[121] It has to define the people responsible for data processing, and who has access to personal data. The contract shall permit the role of each researcher in the project to be identified and if it can access personal data, which is subject to the research. In such a project also the main person responsible for the whole project shall be assigned.

[122] Règlement général pour la protection des données, viewed 5 July 2021, https://www.u-plum.fr/wp-content/uploads/2019/09/Guide-RGPD-2019-web.pdf. The guidelines state that the data should be anonymised in a way that does not permit individual recognition of a person, through isolation, finding a correlation, and inference. They also prescribe specific technical and organisational measures, like setting up passwords and storing in dedicated devices, as well as using encryption, when sending data, to protect it. They also indicate that appointment of a responsible project leader, whether it is a collaborative project, with third parties or not, shall be appointed.

2.2.5 Germany

The German Federal Constitutional Court (*Bundesverfassungsgericht* or *BVerfG*) lays down the specific determination and interrelationship between the concepts of "science", "research" and "teaching" in BVerfG 35, 79, 112 f.[123] and BVerfG 47, 327, 367[124]. As such, research is defined as "*the intellectual activity with the aim of gaining new knowledge in a methodical, systematic and verifiable manner*", which makes science advance and which constitutes the necessary prerequisite for ensuring the character of teaching as the "*scientifically based transmission of the knowledge gained through research*".

Additional guidelines on the interpretation of the term "certain areas of scientific research" in Recital 33 of the GDPR and on safeguards and measures for the purposes of scientific research have been provided in the Decision of the 97th Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder[125]. This Decision aims at narrowing down the specific measures applicable to the use of broad consent where the purpose limitation principle for ""concrete data processing" remains problematic. As such, the Decision provides for corrective measures to compensate the lack of purpose specification by ensuring the (i) transparency, (ii) confidence-building and (iii) data security of the research. As regards transparency safeguards, the Decision emphasises the use of a *research plan* that is accessible to the data subject including the methods and the questions to be addressed by the research; a detailed explanation on the lack of purpose specification at the onset of the research project; and the establishment of an Internet presence through which participants can be informed about ongoing and future studies. In relation to confidence-building, the Decision requires *the affirmative vote of an ethics committee* prior to processing for research purposes, as well as the analysis of the applicability of dynamic consent and the respective granting of the withdrawal of consent to the data subject prior to processing for other purposes. Applicable security safeguards encompass the prohibition of data transfers to third countries with a lower level of data protection; the separate commitments to data minimisation, encryption, anonymisation or pseudonymisation; and specific rules for limiting access to the collected data.

Another relevant guideline in the area is the Memorandum of the German Research Foundation on "Safeguarding Good Scientific Practice"[126]. The Memorandum echoes a variety of ethical and legal safeguards for ensuring the highest standards of research practices. Relevant measures include the organisational responsibility of heads of research institutions and heads of research work units to promote good research practices; the appointment of an independent ombudsperson to whom questions relating to good research practices can be addressed; the examination of allegations of misconduct in strict confidentiality; and the adherence to the presumption of innocence by responsible bodies at research institutions to protect both the complainant and the respondent.

2.2.6 Greece

The **National Institute of Social Research (EKKE's) Ethics Committee** and the University of Macedonia issued guidelines on good practices on scientific research in respectively the Code of Ethics

[123] BVerfG 35, 79, 112 f., viewed 2 February 2021, https://www.servat.unibe.ch/dfr/bv035079.html.
[124] BVerfG 47, 327, 367, viewed 3 February 2021, https://www.servat.unibe.ch/dfr/bv047327.html.
[125] Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO 3. April 2019, viewed 4 February 2021, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/97DSK_BeschlussEG33.pdf;jsessionid=4EA01CC14D23EE86E1758E4A4EE2CF8C.intranet242?__blob=publicationFile&v=4.
[126] Deutsche Forschungsgemeinschaft, Guidelines for Safeguarding Good Research Practice Code of Conduct, September 2019, viewed 67 February 2021, file:///C:/Users/u0142276/Downloads/code_of_conduct_dfg%20(1).pdf.

and the Internal Rules of Procedure[127] and the Code of Ethics[128].

EKKE´s Code requires researchers *to duly inform* the data subjects about the goals of the research in a concise, complete, honest, adequate and understandable way. The informational duty comprises *the methodology of the study*, the purposes, and the hazards, burdens or discomfort in writing or by other means, including electronic means where appropriate.

2.2.7 Iceland

The Icelandic **SA** (*Persónuvernd*) issued **guidelines** for record keepers[129] for *access of researchers to public records* for the purpose of scientific research. The informative website contains a list of considerations that researchers preparing to make a request for access to records should take into account, as well as *guidelines for the record keepers for assessing these requests*[130].

The Icelandic Supreme Court further decided in a case concerning the rejection of the Medical Director of Health of a request by a data subject that health information from medical records concerning her deceased father should not be *entered into the Health Sector Database*[131]. The Court concluded that although the individual provisions of the Act No 139/1998 repeatedly stipulated that health information in the Health Sector Database should be non-personally identifiable, it was far from adequately ensured under statutory law that this objective would be achieved. The Court concluded that various forms of monitoring of the creation and operation of the database were no substitute in this respect without further foundation in law and concluded that the right of the individual in this matter had to be recognised[132].

2.2.8 Italy

Specific guidelines on appropriate safeguards are provided in the **Decision No. 146 issued by the *Garante*** on 5 June 2019 (Decision No 146)[133] as well as in **the Rules of Conduct** for the processing for statistical or scientific research purposes, published on 14 January 2019[134].

Decision No 146 issued by the *Garante* on 5 June 2019 contains additional requirements covering various types of research as well as the data processing for scientific research purposes in cases in which

[127] National Center for Social Research, Adoption of the Code of Ethics and Conduct Research Ethics and the Rules for the Application of Principles and Operation of the Committee on Ethics and Research Ethics Committee of the National Centre for Humanities and Social Research (NSCR), 2019, viewed 15 March 2021, https://www.ekke.gr/uploads/announcements/privacy_policy/fek_ekke_privacy_policy.pdf.
[128] Code of Ethics and Conduct of Scientific Research, University of Macedonia, Thessaloniki, January 2019, viewed 15 March 2021, https://www.uom.gr/ethics/kodikas-hthikhs-kai-deontologias-ths-episthmonikhs-ereynas.
[129] *Leiðbeiningar til skrárhaldara um afhendingu gagna*, published 3.12.2013, viewed 2 April 2021, https://www.personuvernd.is/personuvernd/frettir/nr/1741.
[130] The researcher must consider the fact that he or she may become the controller for the processing activities. The entity dealing with the access request should ensure that the researcher can only get access to the information to which access has been authorised, and not access to more information than the authorisation cover and what is necessary for the research; as well as consider whether access to information where the identities have been removed would suffice.
When assessing the request, the record keepers should make an independent decision on whether the access to personal data should be granted; evaluate whether the data requested is consistent with and appropriate for the purpose of the research; and whether the researcher has requested information that is more than necessary for the purpose of research.
[131] This database was envisaged by the now repealed Act No. 139/1998. See Case No. 151/2003 November 27, 2003, viewed 5 July 2021, https://www.haestirettur.is/default.aspx?pageid=347c3bb1-8926-11e5-80c6-005056bc6a40&id=cbcba31b-5dfb-4d90-a286-cedc5d095595.
[132] This was also in light of the obligations imposed on the legislature by Paragraph 1 of Article 71 of the Icelandic Constitution.
[133] Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510], viewed 20 March 2021, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510.
[134] Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069637], viewed 30 March 2021, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069637.

collecting the data subjects' consent is not possible for specific and exceptional reasons, as well as additional safeguards for the necessary processing of data for medical, biomedical and epidemiological research purposes, described *below*.

The **2019 Rules of conduct** contained detailed instructions. They apply to all processing carried out for scientific purposes **by universities, other research institutions and scientific societies, as well as researchers working within these universities, institutions, research institutes and members of these scientific societies**. They require, as prerequisites of the processing of personal data, a research project containing: (i) information aimed at documenting the scientific research; (ii) the measures to ensure compliance with the Rules of conduct and the data protection legislation, the identification of the processors, if any; (iii) a declaration of commitment to comply with the Rules of conduct signed by the persons for the processing; (iv) *the deposit of the project which is kept*, in confidential form[135], for five years from the scheduled conclusion of the research; (v) in the processing of data relating to health, authorised subjects shall observe the rules of confidentiality and security which are required for health professionals or comparable rules of confidentiality and security. The Rules of conduct further provide for a risk assessment on the identification of the data subject for *disclosure and dissemination* purposes, which shall be less than the established thresholds, when the statistical results do not reasonably permit the identification of statistical units or waived for the sole statistical results related to public variables[136]. Moreover, when informing the data subjects entails a disproportionate effort[137], the *Garante* allows that the controller can adopt appropriate forms of publicity, *e.g.* for processing involving large numbers of subjects distributed throughout the country, *insertion in at least one newspaper with wide national circulation or announcement on a national radio or television station*[138]. In the case of processing special categories of data and data relating to criminal convictions and offences for scientific research purposes, data, as a rule, must be *anonymised* and only processed by universities when the interested party has freely expressed consent and the consent has been given in writing, unless the latter becomes burdensome, in which case it can be documented in writing, provided that it is explicit and is kept by the controller for three years.

Also, special provisions exist *in relation to medical, biomedical and epidemiological research, where stricter requirements for consent are provided*. Control mechanisms cover the custody of the *research plan*, the assurance of the dissemination of and compliance with the Rules of conduct among the entities and persons involved in the processing, and the report to the *Garante* of any violations of the said Rules. As for data collection purposes, it is compulsory to pay specific attention to the selection of personnel responsible for data collection and in defining its organisation and methods; make known the identity, function and purpose of the collection by the authorised personnel; provide the required *information* to the interested party and any other clarification; to not carry out at the same time, on behalf of more than one data controller, activities of personal data collection from the same data subjects, unless expressly authorised; provide for the correction of errors and inaccuracies in the information acquired during collection; ensure particular diligence in the collection of the special categories of data and data relating to criminal convictions and offences[139].

[135] According to Section 3, paragraph 3 of the 2019 Rules of Conduct, consultation of the research project for the purpose of applying the data protection legislation is always possible.
[136] See Section 5 paragraph 1, lett. c) of the 2019 Rules of conduct.
[137] See Section 6, paragraph 3 of the 2019 Rules of conduct.
[138] Moreover, for processing concerning large groups of data subjects distributed on a regional area (or provincial), an advertisement in a newspaper of wide regional (or provincial) diffusion or announcement by a radio and television station of regional (or provincial) diffusion is required; for processing concerning groups of specific categories of data subjects, identified by particular demographic characteristics and/or particular training or employment conditions or similar, insertion in information tools of which the interested parties are normally the recipients is also possible.
[139] Note in addition that in the event of the exercise of the rights, if it is necessary to make changes to the data concerning the person concerned, the controller shall make a note of the changes requested by the person concerned in the appropriate spaces or records, without changing the data originally entered in the file. Lastly, for accountability purposes, authorised persons need to conform their behaviour to the following provisions: (i) respect for the purpose limitation principle; (ii) appropriate storage of the data; (iii) prohibition to disseminate and use for private interest or other the personal data and information not

2.2.9 Norway

The Norwegian Research Ethics Committees have published guidelines, which apply to different types of research, such as medical- and health research, science and technology, social sciences, humanities, law and theology[140]. In addition, general guidelines comprise a set of principles to be implemented when carrying out research, relating to respect for the individuals, striving for good consequences, fairness, integrity, voluntary informed consent and confidentiality. Apart from general guidelines, there are guidelines *for research ethics* in numerous different research fields[141]. Additionally, the **Research Council of Norway** also provides *ethical standards for those receiving funding*, such as the Guidelines of the Norwegian National Committees for Research Ethics[142].

The Norwegian Centre for Research Data (the NSD) *facilitates the sharing and reuse of data* and gives *advice* on data management and data protection in research[143]. It is a state-owned centre, and falls under the Ministry of Education and Research[144]. It is a *public actor responsible for archiving data and facilitating the reuse* for research purposes, with national competence for data protection in research and data management services[145]. The work of the NSD is broad, but includes among other things helping to ensure that data protection and secure *data management* is respected across all disciplines, and assists researchers with identifying a *legal basis*, guidance on how to create *a data management plan*, how to archive research data and give courses on data protection in research[146]. Whereas no general requirement for notification or pre-approval of research projects exists under the GDPR, many Norwegian research institutions voluntarily choose to report and seek pre-approval of relevant projects with the NSD[147].

available to the public; (iv) documentation of the work; (v) adaptation to the evolution of methodologies and techniques for data protection purposes; (vi) stimulus of the communication and dissemination of statistical results, in relation to the cognitive needs of the scientific community and the public, in compliance with the rules on protection of personal data; and (vii) report of behaviours violating the Rules of conduct to the controller or processor.

[140] The Norwegian National Ethics Committees, viewed 5 July 2021, https://www.forskningsetikk.no/en/guidelines/.

[141] Such as the social sciences, humanities, law and theology comprise for example respect for individuals, human dignity, privacy, duty to inform, consent and obligation to notify, confidentiality, limited re-use, storage of personal data, responsibilities of avoiding harm, respect for privacy and family life. See the National Committee for Research Ethics in the Social Sciences and the Humanities (NESH), Guidelines for Research Ethics in the Social Sciences, Humanities, Law and Theology, published 8 June 2019, viewed 5 July 2021, https://www.forskningsetikk.no/en/guidelines/social-sciences-humanities-law-and-theology/guidelines-for-research-ethics-in-the-social-sciences-humanities-law-and-theology/. The principles mentioned have been chosen in order to underline those related to privacy and data protection in the first place. In guidelines for science and technology privacy, the duty of care, information to participants, confidentiality and anonymity are mentioned, see the Norwegian National Committee for Research Ethics in Science and Technology, Guidelines for Research Ethics in Science and Technology, published 8 July 2019, viewed 5 July 2021, https://www.forskningsetikk.no/en/guidelines/science-and-technology/guidelines-for-research-ethics-in-science-and-technology/.

[142] The Research Council of Norway, viewed 5 July 2021, https://www.forskningsradet.no/en/Adviser-research-policy/Ethical-standards-in-research/.

[143] The Norwegian Centre for Research Data, viewed 5 July 2021, https://www.nsd.no/en/about-nsd-norwegian-centre-for-research-data/.

[144] Ministry of Education and Research, viewed 5 July 2021, https://www.regjeringen.no/en/dep/kd/organisation/kunnskapsdepartementets-etater-og-virksomheter/Subordinate-agencies/norwegian-social-science-data-services-/id440384/.

[145] NSD Strategy 2021-2021, viewed 5 July 2021, https://www.nsd.no/en/about-nsd-norwegian-centre-for-research-data/nsd-strategy-20212024.

[146] NSD, viewed 5 July 2021, https://www.nsd.no/en/data-protection-services.

[147] The Norwegian National Research Ethics Committee, viewed 5 July 2021, https://www.forskningsetikk.no/en/resources/the-research-ethics-library/legal-statutes-and-guidelines/the-personal-data-act/.

3 SECTORIAL LEGISLATION AND SOFT LAW

This section provides an overview and analysis of sectorial legislation and soft law at EU and national level. Section 3.1 describes EU sectorial legislation and soft law while section 3.2 points to other legal instruments at international or European level which have relevance in the identification of appropriate safeguards in the EU Member States and EEA States. Finally, section 3.3. discussed national sectoral legislation.

The below-mentioned legal instruments often refer to the GDPR, including to some mechanisms which could be seen as safeguards, for example, the need for consent. Depending on the type of instrument, such safeguards have been implemented in national law or in guidelines by the EEA States. Recommendations of the Council of Europe, e.g., are often reflected in sectoral legislation. This is visible in the sectoral legislation for various domains e.g., use of biological material, and in the guidelines and further analysed and explained below.

3.1 OVERVIEW OF EU SECTORIAL LEGISLATION AND SOFT LAW

Several legal instruments on EU level in specific domains provide references to safeguards when deploying personal data for research. We discuss hereunder the most important ones. Furthermore, this section discusses any other soft law instruments that have relevance in the identification of appropriate safeguards.

3.1.1 Clinical Trial Directive and Regulation

The Clinical trials on medicinal products for human use Directive No. 2001/20/EC (Clinical Trial Directive or CT Directive)[148] stated *the need for informed consent* to protect the data subjects, and also referred to *ethics committees*. The consent mechanism in the current Clinical Trial Regulation (EU) No 536/2014[149] is very similar to that of the CT Directive while aiming at protecting the integrity and dignity of the trial participants (see also recital 27 CT Directive).

The Clinical Trials Regulation is built on the definition of 'consent' of the GDPR. It leads some to conclude that such consent is the same document as the consent of GDPR and that it can be valid as a consent also needed under data protection legislation. This is, however, not correct as consent as a safeguard for participating in clinical trials (CT) should be seen as distinct from consent as a safeguard and ground for processing any other and additional personal data for scientific purposes. The EDPB attempted to clarify that if personal data from a clinical trial is processed for scientific purposes *within the clinical trial protocol*, various grounds for use of the personal data for scientific purposes can be used as set forth in the GDPR (including for reasons of public interest or legitimate interests). As for 'sensitive' data, scientific research purposes, besides (explicit) consent, is mentioned as a condition[150]. The need for consent should in addition follow the rules of the GDPR, such as ascertaining that there is no imbalance etc. This position has been criticized, such as because privately funded pharmaceutical

[148] Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the EEA States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, OJ L 121, 1 May 2001, p. 34, viewed 5 July 2021, https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-1/dir_2001_20/dir_2001_20_en.pdf.

[149] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, viewed 5 July 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0536-20140527 (consolidated version).

[150] EDPB Opinion 3/2019 concerning Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR). According to the EDPB Opinion, Article 9(2)(j) is not a legal ground but a cumulative (specific) condition which is required for the processing of particular categories of personal data along with an adequate legal ground under Article 6 of the GDPR.

companies would be able to re-use the data while the rights of data subjects are restricted[151].

3.1.2 Human tissue and cells Directive 2004/23/EC

The Human tissue and cells Directive 2004/23/EC[152] mainly addresses the need for protection when donating tissue and cells as required by protection of fundamental rights in the relevant treaties and the Oviedo Convention[153] when pointing to the consent requirements. This Directive does not set out requirements for further use of personal data and tissue and cells for scientific purposes, such as for example whether a broad consent would be possible. National regimes will therefore remain and play an important role, in particular by for example excluding consent or imposing specific conditions for confidentiality.

As regards especially health databases and biobanks used for research, which were also the subject of various international ethical approaches and declarations, there is emphasis on *governance agreements between stakeholders*, held accountable, such as the database owners and the parties requesting access to these databases for research. Ethical approaches such as pronounced by the World Medical Association in the 2016 Taipei Declaration on ethical considerations regarding health databases and biobanks[154] strongly believe in such governance agreements being safeguards for research, together with *consent and transparency* to the data subjects[155].

The Human tissue and cells Directive 2004/23/EC further stresses the need for complying with 'all mandatory consent requirements' stressing the need for '*informed consent*' for tissue donation and also requires taking into account *confidentiality laws*[156].

3.1.3 Regulation (EC) no 223/2009

The Regulation (EC) No 223/2009 of 11 March 2009[157] sets out the common framework for European statistics, governed by the European statistics programme.

3.1.4 Proposal for Regulation on European data governance

The recent proposal for Regulation on European data governance of 25 November 2020[158] provides for

[151] European Parliament, *How the General Data Protection Regulation changes the rules for scientific research. Study*, Panel for the Future of Science and Technology, July 2019, p. 38.
[152] Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells, OJ L 102, 7.4.2004, p. 48–58, viewed 5 July 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0023.
[153] Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo, 4.IV.1997.
[154] WMA Declaration Of Taipei On Ethical Considerations Regarding Health Databases And Biobanks Adopted by the 53 WMA General Assembly, Washington, DC, USA, October 2002 and revised by the 67 WMA General Assembly, Taipei, Taiwan, October 2016, accessed 7 July 2021, WMA Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks – WMA – The World Medical Association.
[155] For a comparison between the Taipei Declaration and the GDPR safeguards, see, e.g., Chassang, G. and Rial-Sebbag, E., 2018, 'Research Biobanks and Health Databases: the WMA Declaration of Taipei, Added Value to the European Legislation (Soft and Hard Law)', European Journal of Health Law, vol. 25, pp. 501-516.
[156] Articles 13 and 14 of the Human tissue and cells Directive 2004/23/EC.
[157] Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities, OJ L 87, 31.3.2009, pp. 164–173, viewed 5 July 2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009R0223.
[158] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767, Accessed 7 July 2021, EUR-Lex - 52020PC0767 - EN - EUR-Lex (europa.eu). See also EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data

the supply for the re-use of data within scope, which could also include personal data, including statistical data, as *public task* of *public sector bodies* covered. Recital 28 states that the proposed Regulation shall be without prejudice to the obligation of providers of data sharing services to comply with Regulation (EU) 2016/679 and the responsibility of supervisory authorities to ensure compliance with that Regulation.

3.1.5 Soft law instruments

3.1.5.1 Research in general

For research institutions, Science Europe developed a *Practical Guide to the International Alignment of Research Data Management*[159] in which the details of data management plan are further discussed.

3.1.5.2 Archives

The European Archives Group (EAG), an expert group of the EU Commission, published *guidelines for archives*[160] stating that personal data protection needs to be balanced against the right to justice, the right to the truth and the right to remedy and reparation for victims of gross violations of human rights. Because of the type and purpose of research (i.e. archiving), data minimisation *is often not possible*, and the *integral preservation* of documents containing personal data has been instrumental in restoring the rights of data subjects. Further, the guidelines state that '*pseudonymisation should be fully reversible'* and should be done in a way that does not endanger the evidential value of records. In case of personal data preserved for archiving purposes in the public interest, archive services *should store unaltered original data* in a *protected storage* facility and make a *pseudonymised copy of personal data for access* by researchers, if such purposes can be fulfilled in that manner[161]. As for *special categories of data,* access is *restricted*[162]. Other public and private bodies *should seek guidelines of their SA*. Additional precise safeguards are not specified. Relevant national codes exist in the United Kingdom and Italy.

3.1.5.3 Health - registries

The European Commission has supported cooperation and networks for scientific research in the context of specific programmes, such as for example **the European Network of Cancer Registries (ENCR**), which has been in operation since 1990. ENCR, e.g., established a *data submission portal* for its members (only), with support of the Joint Research Center. The ENCR was supported by the Joint Research Center for the *harmonisation of data and registration processes when submitting data to the European Cancer Information System (ECIS)*[163]. In this system, participating countries with varying data sources (cancer registries, national statistics, population register, epidemiological centres…)

governance (Data Governance Act), viewed 20 August 2021, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en.

[159] See Science Europe, Practical Guide to the International Alignment of Research Data Management – extended Edition, 27.1.2021, p. 29, viewed 5 July 2021, https://scienceeurope.org/our-resources/practical-guide-to-the-international-alignment-of-research-data-management/.

[160] See EAG, Guidance on Data Protection for Archive Services, EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector, 2018, viewed 5 July 2021, https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf.

[161] Ibid. pp. 12-13.

[162] As for the archive in National Archives of data relating to criminal convictions and offences, archive services can take measures such as *posting such documents on a restricted-access area* of their websites, or *redacting names*, pursuant the paramount principle of respecting and protecting the dignity of individuals. See Ibid. pp. 21-22.

[163] See, JRC Technical Reports, The European Cancer Information System (ECIS) web application, Computing and disseminating European statistics on cancer burden, 2018, p. 5, viewed 5 July 2021, https://encr.eu/sites/default/files/JRC113106_ecis_wa_guide_11_sept_2018_print-.pdf. One would expect also detailed guidelines as to how comply with data protection safeguards, to inter alia protect the privacy and data protection rights of individuals whose data may be directly or indirectly relied on for the registration.

extend beyond the European Union[164].

3.1.5.4 Biological material: guidelines and common practices

Some organisations in EEA States have tackled research specific questions in well researched **recommendations and guidelines** and **practices**. An example is '*Human Biological Material. Recommendations for Collection, Use and Storage in research* of the Irish Council for Bioethics[165], and which also reviewed practices in various EEA States. Another example are the practices adopted by the Biobanking and BioMolecular Research Infrastructure (BBMRI), a significant biobank network grouping researchers and biobanks of 20 countries. The degree as to how and how far these recommendations were adopted, however, remains difficult to assess. BBMRI would also have developed a draft code of conduct, which is however not made public (until approval).

3.2 OTHER LEGAL INSTRUMENTS WITH INFLUENCE UPON EUROPEAN COUNTRIES

3.2.1 International

In the guidance to States for adopting legislation, Unesco stated in the Universal Declaration on Bioethics and Human Rights of 2003[166], that **human dignity and the interests and welfare of the individual** *shall prevail over the interest of science and society* (Article 3).
In the specific domain of processing for **statistical purposes**, several initiatives have been taken at international, Council of Europe and European Union level, including the development by **legal norms**. Such legal norms, for example, see into guaranteeing *confidentiality, including* when statistical bodies communicate data to Eurostat.

3.2.2 The Council of Europe

3.2.2.1 Convention on Human Rights and Biomedicine, concerning Biomedical Research (1997) and Additional Protocol (2005) ('Oviedo Convention')

The Convention of Oviedo explicitly states that everyone is entitled to *know* any information collected about his or her health, but also that the wishes of individuals not to be so informed shall be observed (Article 10(2) and Article 27 Additional protocol). The Convention also contains a limitation as to the use of genetic information[167]. The Additional Protocol of 2005 imposes *a statutory confidentiality obligation* (Article 25) and requires *more extensive* information to be given to participants, including relating to access and potentially further use (Article 13[168]), and a *duty of care*, imposing a duty to return

[164] See https://ecis.jrc.ec.europa.eu/info/registries_encr.php.
[165] Irish Council for Bioethics, Human Biological Material: Recommendations for Collection, Use and Storage in Research 2005, Dublin, 116 p., viewed 5 July 2021, https://repository.library.georgetown.edu/handle/10822/1039512.
[166] United Nations Educational, Scientific and Cultural Organization (UNESCO), Universal Declaration on Bioethics and Human Rights, 19 October 2005, viewed 3 April 2021, http://portal.unesco.org/en/ev.php-URL_ID=31058&URL_DO=DO_TOPIC&URL_SECTION=201.html.
[167] See Article 12: "*Tests which are predictive of genetic diseases or which serve either to identify the subject as a carrier of a gene responsible for a disease or to detect a genetic predisposition or susceptibility to a disease may be performed only for health purposes or for scientific research linked to health purposes, and subject to appropriate genetic counselling*".
[168] Article 13 states as follows: "*The information shall cover the purpose, the overall plan and the possible risks and benefits of the research project, and include the opinion of the ethics committee. Before being asked to consent to participate in a research project, the persons concerned shall be specifically informed, according to the nature and purpose of the research: (i) of the nature, extent and duration of the procedures involved, in particular, details of any burden imposed by the research project; (ii) of available preventive, diagnostic and therapeutic procedures; (iii) of the arrangements for responding to adverse events or the concerns of research participants; (iv) of arrangements to ensure respect for private life and ensure the confidentiality of personal data; (v) of arrangements for access to information relevant to the participant arising from the research and to its overall results; (vi) of the arrangements for fair compensation in the case of damage; (vii) of any foreseen*

relevant information about 'the current or future health or quality of life of research participants', and such 'within a framework of health care or counselling' (Article 27) and to make results available, both to the participant , the ethics committee and the public (Article 28).

3.2.2.2 Health-related data

The Council of Europe also issued several recommendations in the domain of health-related data. The 2019 Recommendation[169] by the Council of Europe, which replaced Recommendation (97)[170] stated that not only healthcare professionals who are entitled to carry out their '**own medical research'**, **but also** '**other scientists in other disciplines**' could use the health-related data 'which they hold' for research purposes. The condition, however, is that the data subject has been *informed* of the possibility beforehand and appropriate safeguards are in place.

3.2.2.3 Biological materials of human origin

According to the Recommendation 2016(6) on research on biological materials[171], in which it is reminded that the interests and **welfare of the human being shall prevail over the sole interest of society or science,** the collection and storage of biological materials for future research can be based on either **consent or authorisation**, prior to which the individual concerned should be provided with comprehensible information (Article 10)[172]. If the attempt to contact the person is unsuccessful, an exception may be made where the research **addresses an important scientific interest** and is in accordance with the **principle of accountability** (Article 22(2)(b)(ii)).

3.3 OVERVIEW AND LEGAL ANALYSIS OF NATIONAL SECTORIAL LEGISLATION AND SOFT LAW

In this section, legislation and guidelines as well as other 'soft law' relating to specific sectors are described and analysed per Member State with a view of finding common approaches to safeguards. Not all sectors are equally covered in each country. The results of this section are based on the replies to the questionnaire and additional desk research covering available or otherwise researched legislation and soft law instruments.

3.3.1 Austria

Article 2 of the Austrian Act establishing the Austrian Health GmbH (*Bundesgesetzes über die Gesundheit Österreich GmbH*, or *GÖGG*) lays the groundwork for the creation of **Austrian Health GmbH**, a legal entity providing non-commercial services of *general interest* in the field of health care which is entitled to process personal data in stem cell registries[173] and quality registries for research purposes (e.g., clinical trials data). In this context, Articles 15a(6), (7) and (10) GÖGG stipulate the appropriate measures to guarantee a proper level of confidentiality and integrity, *i.e., encryption mechanism in place without delay*, for which *area-specific personal identifiers* are permitted for patient

potential further uses, including commercial uses, of the research results, data or biological materials; (viii) of the source of funding of the research project."

[169] Council of Europe, Recommendation CM/Rec (2019)2 of the Committee of Ministers to member States on the protection of health-related data.

[170] EDPB, EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, 2 February 2021, Paragraph 7.

[171] Council of Europe, Recommendation CM/Rec (2016)6 of the Committee of Ministers to member States on research on biological materials of human origin, which is a successor of Council of Europe, Recommendation Rec(2006)4 on research on biological materials of human origin.

[172] Note that biological materials can only be used in a research project if the latter is within the scope of the consent or authorisation given by the individual (Article 21(1)). For uses not in the scope of the original consent/authorisation, reasonable efforts should be made to contact the person concerned and obtain consent/authorisation (Article 22(2)(a)).

[173] Article 4a GÖGG.

identification with the condition of carrying out an irreversible deletion immediately after conversion. It is moreover required that any additional data is *pseudonymised* and *stored separately* as well as *deleted as soon as* they are no longer required for the scientific purposes[174]. Other safeguards in this area include the draft of a document containing all data security measures taken in accordance with Article 32 of the GDPR and the provisions of the Health Telematics Act (*Gesundheitstelematikgesetz* or *GTelG*) on the basis of an "IT security concept"[175]. This documentation must show that both access to and transmission of data are carried out properly and that the data are not accessible to unauthorised persons.

3.3.2 Belgium

The Act of 4 July 1962 on **public statistics** refers to the possibility of *certification of methodologies* for statistics (Article 13) and for separation, codification and *deletion of individual data if no longer necessary* (Article 17). The Act of 22 March 2006, modifying and updating the Act of 4 July 1962 refers to *confidentiality imposed by law* (and subject to criminal sanctions) on persons and entities responsible for statistical data (Article 18), requires the appointment of *a DPO*, controlling inter alia the use of the logical keys for re-identification (Article 17I*sexies*) and the appointment of *a person for deleting such keys* in time of war. Communications of statistical data to public authorities and researchers is subject to (i) *authorisation* of the Statistic Supervisory Authority (ii) a detailed *confidentiality agreement*[176] for the communication *for a specific statistical purpose* (purpose binding), and (iii) shall contain only *encoded data.* Further note that the Royal Decree of 13 June 2014 determines the conditions under which the **National Institute for Statistics** can act as an intermediary for further processing for statistical purposes. **Public archives** are governed by several *legal instruments*[177], providing in the *public task* and *legal basis* for specific public bodies. One of the most essential safeguards, is the '*public information statement'* with regard to the processing of personal data in the state archives[178].

For **health registries**, *national legislation*[179] obliges the registration of all new cancer diagnoses with the Belgian Cancer **Registry** (BCR)[180] which is in charge of inter alia *encoding* the patient's

[174] Further, the *anonymisation* of data is required when accessed by third parties. *Access control* mechanisms and availability measures are further contemplated in the text as well as organisational measures as to the documentation of access and transmissions of personal data and security management procedures. The federal Austrian Health Telematics Act (*Gesundheitstelematikgesetz* or *GTelG*), the subject of which is the transmission of electronic records of data concerning health and genetic data by healthcare providers, further requires that access control areas, procedures, and mechanisms are established, especially in the case of public health service authorities, which presumably also applies in case of research. As regards the confidentiality requirements, special measures include the necessity of establishing networks which are secure against unauthorised access, in compliance with the state of the art in network security. This includes measures by (i) securing the transmissions with cryptographic or structural measures and establishing network´s authentication and access control mechanisms to a definable user/group; or (ii) establishing protocols and procedures that provide full encryption of data and specified cryptographic algorithms. Other means to ensure confidentiality including encrypted storage of the data in cloud computing infrastructure with an as-need basis. This must show that both access to and transmission of data are carried out properly and that the data are not accessible for unauthorised persons.

[175] Article 8(1) GTelG.

[176] For the content, it shall state that (i) further transfer is not authorised except with authorisation of StatBel, which shall conclude a confidentiality agreement with the transferee; (ii) the receiver shall ensure the security and make sure individual data cannot be extracted from published results; (iii) audits; (iv) sanctions; and (v) duration of the agreement (see Article 18 of the Act of 22 March Act 2006).

[177] Including the Act of 26 July 1955 on archives for federal archive, as complemented with several royal decrees, the Ordonnance of the Brussels parliament of 19 March 2009 on archives, and the Decree of the Flemish parliament of 9 July 2010 on archives.

[178] See also Van Keer, E., De AVG en archieven: een bibliografische wegwijzer, p. 29, viewed 5 July 2021, http://www.arch.be/docs/20200528_Biblio_AVG-Archieven.pdf.

[179] In particular the Health Act of 13 December 2006, adding Article 45*quinquies* to the Royal Decree No 78 of 10.11.1967, and the Royal Decree on norms for oncological care programmes.

[180] The BCR is a national population-based cancer registry with the aim to also report on the survival of patients and to do research (case-control and cohort-studies). The Belgian Cancer Registry (BCR) receives analysis results from labs, data from hospitals, and data linked to sick funds ('mutualité') data. The BCR monitors the data protection, when hospitals, with an oncological care programme, and services for pathological anatomy, legally obliged to cooperate, share data. See Belgian Health Care Knowledge Centre (*Federaal Kenniscentrum voor de Gezondheidszorg* or KCE), Ten years of multidisciplinary teams, KCE report 239, 2015, p. 18, viewed 5 July 2021,

social security number and reviewing the *data quality*, and which may – *upon authorisation of the SA* - communicate the data for research to third parties (Article 3 and 9)[181]. The law setting up the **Crossroad Database for Social Security**, authorises the latter to communicate as an intermediary organisation *pseudonymous data* it has to third parties for *knowledge development for social security* purposes and *determining selection criteria for research participants*[182]. Further, a specific authority[183] is tasked with guiding and establishing 'good practices' with regard to specific personal data processing, in particular those concerning health and the federal government, including for the communication of '*anonymous data' by the governmental agencies and for determining the selection criteria for research participants*[184].

The Act of 19 December 2008 on **Human Body Material** (HBM), which also covers HBM for scientific research use, specifies some safeguards, in particular that a ***written agreement*** shall be concluded with the person or institution receiving HBM for research[185]. It should be noted as well that for secondary use, which is defined as "*any use of human body material other than that to which the donor has given his/her consent in the context of the collection*" in cases where it is impossible to seek consent, or where such a request would be exceptionally inappropriate, the (positive) ***opinion of an ethics committee*** would be sufficient to allow the collection of samples (Article 20(1) of the HBM Act). Further conditions are specified in a Royal Decree, including the obligation to declare to the **Federal Agency for Medicines and Health Products (FAMHP)**[186]. A new service with the **FAMHP** *advises* on accessing the biobanks.

3.3.3 Bulgaria

Access to health data is possible for purposes of public health and statistics. Based on Article 28 of the National Health Act, professionals with proven credentials, such as doctors, can access health data. The data have to be anonymised. The access applies to publicly funded organisations[187].

The National Centre of Public Health and Analyses (**NCPHA)** provides **statistical information** based on the Health Act (HA) and the Personal Data Protection Act. A written application should be made for access to data, but this is limited to public information.

Informed, **written consent** is required for **medical research**[188] and the taking of biological material for

https://kce.fgov.be/sites/default/files/atoms/files/KCE_239_team%20meetings_oncology_Report_2.pdf. A standard form is deployed, as set forth in the Offical Journal of 14.10.2010, and following ENCR guidelines. See also: https://kankerregister.org/Standard%20cancer%20registration, viewed 5 July 2021.

[181] The law imposes additional safeguards as well, such as drafting a security plan, appointment of a security adviser / DPO in charge of establishing minimum security measures, guaranteeing confidentiality and limited access (Article 4), which can be further completed by royal decree.

[182] See Article 5 of the Act of 15 January 1990 setting up the Crossroad Database for Social Security, as modified by Act of 5.9.2019 regarding ISCs (Article 11).

[183] This authority is called the 'information security comité' (ISC) and was set up by Act of 5 September 2018.

[184] See Act 5.9.2018, Article 39. These 'good practices' and also the ISC's opinions, which are required safe in particular cases, and the succinct annual reports, can be found at ehealth.fgov.be.

[185] ***Elements*** that shall be included in the written agreement include the ***topic*** of the scientific research for which the HBM is made available, the responsibilities ***for ensuring traceability***, the appropriate technical and organisation ***measures*** in the case personal data is also communicated and a ***coded copy*** of the consent of the donor (Article 22(2)(3) HBM Act). About this Act, see also 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, p. 187 *et seq.*

[186] See Royal Decree of 9 January 2018 on biobanks. See also https://www.famhp.be/en/news/new_royal_decree_on_biobanks, viewed 5 July 2021. Other conditions are relating to the collection, the reporting to the ethics committee, a register, the agreement with the recipients of the body material, encoding, traceability and identification.

[187] Article 28, National Health Act.

[188] Article 197 National Health Act.

genetic tests[189]. The consent has to be given after *information* of the research leader about the essence, importance, scope, and possible risks[190]. The statute underlines that such data are personal data and *should be not disclosed* to employers, health insurance organisations, and insurance companies[191]. Moreover, such research should be conducted ensuring maximum safety for the health of the person, and should not disclose his or her personal data.

3.3.4 Estonia

The **Official Statistics Act** (OSA) regulates statistics and scientific research conducted by the Statistical Office of Estonia[192] based upon (in principle voluntary) responses collected by a 'producer of official statistics' (producer)[193] after extensive *information* disclosure[194]. The producer of statistics is *allowed by law* to set up statistical registers of data by collecting data *from administrative records*, data bases and other types of data sources, and use these data for the production of (other) official statistics, *regardless of the initial purpose of collection*[195]. The OSA further contained detailed safeguards as that for example micro-data of a natural person should only be kept together with the personal identification code, until the validation of the micro-data has been completed[196], and the principles of protection of personal data and s*tatistical confidentiality* must still be complied with. The producer must ensure organisational, information technology related and physical protection of data for all statistical activities[197] as established by requirements of the Estonian government or the Bank of Estonia (Eesti Pank)[198]. *Dissemination* of confidential data is only allowed in a form that prevents to directly or indirectly identify the statistical unit, and should be otherwise disseminated with the consent of the data subject, unless the data are considered public according to national law, or the receiver is Eurostat, national statistical institutes or other EEA States[199]. In this case, the data are marked as confidential[200].

The **Archives Act** regulates archival research[201], including the management, appraisal and transfer of records, conditions preventing the unauthorised use of, damage to and destruction or copying of archival records. Access and use of archival records are unrestricted except when the provisions of GDPR and of the Estonian data protection legislation apply.

[189] Article 141 National Health Act.
[190] Article 199 National Health Act.
[191] Article 141 National Health Act.
[192] Official Statistics Act, passed 10.06.2010, RT I 2010, 41, 241, entry into force 01.08.2010, viewed 30 March 2021, https://www.riigiteataja.ee/en/eli/517122019002/consolide.
[193] Section 28 of the Official Statistics Act. With some exceptions or unless provided by law, submission of personal data is *voluntary* for natural persons. As for the exceptions: see Section 28(2) of the Official Statistics Act: "*Natural persons who own immovable property, buildings or parts thereof or own or possess agricultural land or farm animals or make international payments*". At the same time, producers should preferably use data which has already been generated/collected as a part of state and local government authorities' or legal persons in public and private law activities.
[194] For the collection and statistical processing of data, the producer *must inform* the respondents in advance about which data will be collected, the purpose for which the data will be used, the principles of statistical processing and how that data can be disseminated and the due date for when the data should be submitted, as well as provide the information of any liability for not complying with the submission requirements: see Section 30(1) of the Official Statistics Act. The right to rectification, erasure of data or the right to restrict the processing extend to personal data collected for the purpose of official statistics: see Section 31 (2)-(4)of the Official Statistics Act.
[195] Section 30(2) of the Official Statistics Act. With regard to the use, the producer has the right to use personal data for the production of official statistics (see Section 31 of the Official Statistics Act) and unlike it is the case for data collection, it is not required to inform the data subjects concerned.
[196] Afterwards, the personal identification code must be *stored separately* from the other data of that person. *Later linking* should, however, remain possible: see Section 32 OSA. In addition, persons who, due to the nature of their official duties, have access to data which allow for direct or indirect identification of individuals carry responsibilities for the use of the data, and must ensure that the data are only used for statistical purposes and prevent unlawful dissemination of such data: see Section 34(4) of the Official Statistics Act.
[197] Section 34(5) of the Official Statistics Act.
[198] Section 34(6) and (7) of the Official Statistics Act.
[199] Section 35 of the Official Statistics Act, requires provision by EU law.
[200] Section 34 of the Official Statistics Act, *data that allow direct or indirect identification of a statistical unit and thereby disclosure of micro-data*.
[201] Archives Act, viewed 30 March 2021, https://www.riigiteataja.ee/en/eli/521032019019/consolide.

Clinical trials are regulated by the **Medicinal Products Act**[202]. Clinical trials require (i) an approval requirement, unless the treatment and monitoring of the trial subjects remain unchanged and no new medicinal product is introduced[203]; (ii) are subjected to requirements regarding the quality of the medicinal products, the sponsor of the clinical trial, the planning and *publication* of the result and the persons conducting the research[204]. Furthermore, (iii) *consent* of the trial subject is required[205] and can only be given after the data subject has been *informed* of all facts related to the trial, and withdrawal must be possible at any time; and (iv) the *approval* of a medical *ethics committee* is required[206], with further requirements concerning its composition and due process[207]. In addition, (v) a written application must be submitted to the *State Agency of Medicines* at least two months before the beginning of the planned trial[208], *and authorisation* from the Agency, typically containing requirements for the quality of research, should be obtained[209]. The State Agency of Medicines can also immediately suspend or terminate the clinical trial if these circumstances become evident or, if the continuation of the trial does not pose a risk to life and health of the trial subjects, send a notice concerning the intention of suspension or termination. The liability for the compliance of all the aspects of the trial falls entirely on the sponsor of the clinical trials of medicinal products[210].

The **Human Genes Research Act** regulates the set up and the maintenance of the Estonian Gene Bank[211], the conditions for processing and composition of the data[212], the rights and obligations of gene donors, restrictions on the use of data and conditions for generic research relating to the Gene Bank and the organisation of its administrative supervision[213]. The Act contains also detailed provisions for **aggregating pseudonymised** data[214] and the **type of research** for which the Gene Bank can be used[215]. It also specifies, among other things, that (de-)pseudonymisation should be performed by **specific persons** appointed by the controller[216], and outlines *the role of the Data Protection Supervisory*

[202] Medicinal Products Act, passed 16.12.2004, RT I 2005, 2, 4, entry into force 01.03.2005,viewed 30 March 2021, https://www.riigiteataja.ee/en/eli/529122020002/consolide.The Act covers different types of medicinal products and the manufacturing and distribution thereof.
[203] Section 87(2) of the Medicinal Products Act.
[204] Sections 88-89 of the Medicinal Products Act.
[205] Section 91 of the Medicinal Products Act. In case of animal, the owner's consent is sought. There are special requirements for individuals with restricted legal capacity.
[206] Section 92 of the Medicinal Products Act.
[207] All requirements concerning the nature of the Medical ethics committee for clinical trials listed in Section 92 of the Medicinal Products Act.
[208] Section 95 of the Medicinal Products Act.
[209] Such authorisation can be denied if (i) the applicant does not comply with the requirements for clinical trials of medicinal products; (ii) the information or documents submitted by the applicant are incomplete or inaccurate; (iii) the trial protocol is unreasonable; (iv) the trial is of no scientific value or is likely to influence the use of medicinal products in the course of health care provision in an unreasonable direction; (v) the risk to the life and health of trial subjects is high: see Section 97 of the Medicinal Products Act. When it comes to veterinary medicinal products, such authorisation is granted by the Ministry of Rural Affairs.
[210] Section 99 of the Medicinal Products Act. Doctors, dentists or veterinarian conducting the trial are only liable in certain circumstances, where violations of their obligations occur or jointly with a third party (employer or other contractual party).
[211] Human Genes Research Act (13 February 20000) RT I 2000, 104, 685, viewed 30 March 2021,https://www.riigiteataja.ee/en/eli/508042019001/consolide.
[212] The Act establishes the rules for valid consent and for the rights to (take) samples, storage of tissue samples and destruction of data and records.
[213] Human Genes Research Act, Article 1(2).
The provisions do not apply to the processing of pseudonymised tissue samples, pseudonymised descriptions of DNA and pseudonymised descriptions of state of health if such tissue samples, descriptions of DNA and descriptions of state of health are processed as a set of data and on the condition that the set of data to be processed contains DNA samples, descriptions of DNA or descriptions of state of health of at least five gene donors at a time: see Human Genes Research Act, Article 7(2).
[215] More precisely, research into and treatment of illnesses of gene donors, public health research and statistical purposes: see Human Genes Research Act, Article 16.
[216] Human Genes Research Act, Article 22.

Authority[217] *and the Research Ethics Committee*[218].

The **National Institute for Health Development** further conducts studies using national data bases, using relevant data such as communicable diseases, cancer registry etc. *which have been established on the basis of law and regulated by the specific Minister's statutes*[219].

3.3.5 Finland

The Act on the **Openness of Government Activities** regulates the use of personal data extracted from registers of *public authorities for scientific research purposes*, i.e. the right to review publicly available documentation, the *non-disclosure obligations of employees* of public authorities, secrecy of documents and information as well as other *protection mechanisms* for both public and individual interests.

The Act in Secondary Use of Health and Social Data[220] complements GDPR legislation and concerns the processing of personal data for secondary use[221]. The Act further regulates the "one-stop-shop" central licensing authority for the secondary use of health and social data, **the Social and Health Data Permit Authority Findata**[222], which is directly subordinated to the Ministry of Social Affairs and Health[223].

The Act further lays down extensive criteria and conditions for the secondary use of health and social data. Safeguards include the need for a permit[224], and conditions for the use of the results achieved based on the use of the data[225]. Hence, the conditions for the use of secondary data are (i) authorisation from controllers for further use for other research purposes; and (ii) a *decision* of the Data Permit Authority on the request to access the data from different controllers, national information system services or registers[226]. Secondary use of the data will be allowed for permitted purposes as defined in the law, with a revocable licence issued for a fixed term. A licence may also be required for education, information management and development and innovation activities[227] provided that *the explicit consent of data subjects for secondary use is sought for the latter*, as no category under Article 9(2) GDPR fits.

The Medicines Act regulates medicine trials[228], and requires a permission based on *a research plan* when a clinical trial is to be carried out, as well as a positive opinion of an ethical committee. Researchers and other individuals who come in contact with medical data during the course of the research or in connection to the research procedure, are bound by strict confidentiality. It further refers to **the Act on**

[217] Human Genes Research Act, Article 28.
[218] Human Genes Research Act, Article 29. The Ethics Committee is entrusted with assessing processing procedures for the Gene Bank and ensuring preventive protection of fundamental rights and evaluating compliance with Article 6 of Estonian Personal Data Protection Act.
[219] See Estonia response to the EDPB questionnaire.
[220] See https://stm.fi/en/secondary-use-of-health-and-social-data, viewed 5 July 2021. Finland has adopted some specific legislation concerning medical research, clinical drug trials and the secondary use of social welfare and health information.
[221] Hence for *other* purposes than it has been collected. See Section 2 of the Act. The Act concerns the processing of personal data which are registered in relation to social- and healthcare practices, for research and statistical purposes within the health care sector. The Act regulates combining activities of data related to e.g. health care and population statistics which is in the possession of different national authorities, while ensuring the data protection rights of individuals.
[222] Findata "pools" and "centralises" the data from different controllers and anonymises it for further use. See: Section 4 of the Act.
[223] See Section 17 of the Act. The Data Permit Authority makes decisions on data permits concerning data held by controllers; whether data requests fulfil the requirements set by the law; and is also responsible for the collection, *combination, pre-processing, and disclosure for secondary purposes*, and where necessary anonymisation or pseudonymisation of the data subjected to the permit; and supervises compliance with terms and conditions of the permit; and maintaining a secure hosting service.
[224] Conditions for approval: see Sections 35-42, Section 43.
[225] Section 52.
[226] Section 11.
[227] Section 37.
[228] Medicines Act (*Lääkelaki*), 10.4.1987/395, viewed 5 July 2021, https://www.finlex.fi/en/laki/kaannokset/1987/19870395 (in English but only including the changes made until 2010), Sections 86 – 88a.

Medical Research[229], which sets a detailed framework for medical research involving human beings, clinical medical trials, research concerning foetuses and embryos and the work of the ethical committees[230]. For medical research including humans, focus lays on an assessment of interests, the need to appoint a person in charge of the research, the consent of the person being subject to research and the cancellation of such consent[231]. The Act also defined good clinical practices, and sets requirements for declarations, opinions of the ethical committee, reporting of incidents and serious side-effects[232].

3.3.6 France

In the domain of **statistical research, the Official Statistics Law**[233] states that **for official/public statistics,** communicating and disclosing any data related to the statistical survey, especially personal data, can only be made after the *approval* of the Committee for Statistical Secrecy[234]. In the domain of the **public archives** the personal data, which are already not useful for archival purposes, or purposes of scientific or historic research, should be deleted[235]. Furthermore, data related to the state of health shall be given back to the person entitled to it[236].

Research for *medical and health-related purposes* is robustly regulated by law and requires safeguards[237]. In principle, in addition to the possibilities provided for in Article 9(2) of the GDPR, the processing of health data for research purposes is **lawful** provided that: (i) processing is in the *public interest*; (ii) processing complies with standards issued by the CNIL (**methodologies of reference MR001 to MR006[238] –** see also Annex 2) and the **data controller sends a declaration of compliance to the CNIL [239]**; or (iii) **after the authorisation of the CNIL,** if the processing does not comply with one of the standards

The French Public Health Code (*Code de la Sante Publique*[240]) sets general principles for the implementation of health research. For example, there needs to be an **appointed person responsible**

[229] Act on Medical Research (*Laki lääketieteellisestä tutkimuksesta*), 9.4.1999/488, viewed 5 July 2021,https://www.finlex.fi/en/laki/kaannokset/1999/19990488 (unofficial translation available for the original act from 1999).
[230] There are both regional and national ethical committees. The law also sets criteria for the evaluation of research projects, the compilation of the ethical committees and rules for the members of that committee.
[231] Persons with handicaps, minors, pregnant or breast-feeding women and inmates or patients of forensic psychiatry. There are also special rules regarding certain categories of individuals.
[232] Chapter 2a of the Act.
[233] Act No. 51-711 of 7 June 1951, viewed 7 July 2021, Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. - Légifrance (legifrance.gouv.fr).
[234] Article 6 bis of the Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, viewed 5 July 2021, https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000038314928and Article 17 of the Décret n° 2009-318 du 20 mars 2009 relatif au Conseil national de l'information statistique, au comité du secret statistique et au comité du label de la statistique publique, viewed 5 July 2021, https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000034247251/2021-01-19. Furthermore, any statistical survey of public services must be subject to the prior approval of the Minister responsible for the economy and the Minister to whose jurisdiction the interested parties belong (Article 2 Loi n° 51-711 du 7 juin 1951).
[235] Article L.212-3 of the Code du patrimoine, viewed 5 July 2021, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037825470. Furthermore, data related to the state of health shall be moreover given back to the person entitled to it.
[236] Article L212-4 of the Code du patrimoine.
[237] See Articles 64-77 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[238] CNIL - Méthodologie de référence MR-006, Accessed 7 July 2021, Études nécessitant l'accès aux données du PMSI par les industriels de santé Méthodologie de référence MR-006 | CNIL
[239] As explained by the French SA "MR are sorts of "framework" to comply with in order to reduce formalities. Those formalities (prior authorisation from CNIL) must still be complied with including if the data subject expressed consent when the research does not fall under the scope of a MR".
[240] Article L1121-3 of the Code de la sante publique Chapitre Ier: Principes généraux relatifs aux recherches impliquant la personne humaine (Articles L1121-1 à L1121-17), viewed 5 July 2021, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000006170998/.

for the conduct of a particular research project[241].

3.3.7 Germany

Sectoral legislation in Germany on appropriate safeguards for scientific research is mainly provided in three domains, i.e. social security, biomedical research and artificial intelligence.

Appropriate measures and safeguards **for social security purposes** are contained in the Social Security Code (*Sozialgesetzbuch*, or *SGB*), which defines various areas of scientific research where these safeguards are applicable[242]. In principle, according to Article 75 SGB X, the social administration must obtain the permission of the superordinate authority if it wishes to make social data available for research purposes. For individual areas, there are special regulations for the use of data for research purposes. For the transmission of social data, which have been entrusted to the employee of a public youth welfare agency for the purpose of personal and educational help, can only occur under the legal bases established in Article 65 SGB VIII, while for research purposes by social benefits agencies this is permitted insofar *as it is necessary and the interest of the data subject* and are not impaired or the *public interest* in the research considerably outweighs the interest of the data subject[243]. In the insurance sector, the German Pension Insurance Federation can perform the basic and cross-sectional tasks of the German Pension Insurance for research in the field of old-age insurance and rehabilitation, only if *authorised* by the Federal Representative Assembly of the German Pension Insurance Federation, and for research in long-term care insurance, prior *approval* of the SA and *anonymisation* is required.

Several guidelines have been issued from a legal and ethical standpoint for **biomedical research**. On the one hand, the **German Research Foundation** developed a Memorandum of guidelines for safeguarding good research practices, where higher degrees of responsibility are required from the heads of research institutions and heads of unit as regards professional ethics and legal and ethical standards[244]. For example, the **National Committee of the Federal Ministry of Education and Research** also developed Guidelines on Consent of the Medical Informatics Initiative (MII), applicable to all the university hospitals in Germany. In these guidelines, consent requirements for scientific research are thoroughly addressed[245]. Also, the consent to *secondary use* of patient´s data must be obtained separately

[241] The person responsible for the quality of the research can have access to the personal data, if the data subject, before processing data, had been duly *informed* and had not raised its objection. The access is only provided to **the data that is necessary for quality control**. Persons processing personal data have to comply with the standards of professional ethics.
[242] For instance, for the studying of basic benefits of job seekers by the Federal Ministry of Labour and Social Affairs and the Federal Employment Agency as well as for the research studies on unemployment insurance commissioned to the Institute for Employment Research, subject to, *inter alia*, the following measures: (i) physical, organisational, and personnel separation among the entities; (ii) access control mechanisms; (iii) anonymisation of data as soon as this is possible according to the purpose of the research, and until then, the separate storage of the characteristics relating to a data subject; (iv) in case of insurance data, storage of data without first and last names after the insurance number in a specially protected file system.
[243] Furthermore, in case of transmission of *sensitive data*, the data shall be *anonymised as soon as possible (see* Article 22(2) of the BDSG). In case of further processing, *prior authorisation* by the highest federal or Land authority responsible for the area from which the data originate is required. Lastly, transmission of social data for scientific research purposes on social welfare on behalf of the Federal Ministry of Labour and Social Affaires Government shall be permissible *if necessary and the project cannot be carried out with anonymized or pseudonymized data* and the public interest *substantially outweighs the legitimate interest* of the data subjects. In such cases, the data subject shall be informed in writing about the intended transmission, the purpose of the research project and *their right to object* within one month of being informed.
[244] The guidelines also provide for an independent ombudsperson to whom to turn with questions relating to good research practices and cases of suspected misconduct. Quality assurance is required with regard to methods, calibration, collection, processing, and analysis of research data and the re-use of data is clearly indicated. More concretely, the document advocates for the public access of scientific results, but research data and results should be backed up by adequate means according to the standards of the relevant subject area, and retained for an appropriate period of time. Finally, procedures to handle allegations of research misconduct are required, which define policies and regulations on the basis of a sufficient legal foundation.
[245] Particular emphasis is placed in the various legal bases to process patient´s data. For instance, apart from the consent of the patient, legal bases by virtue of state hospital law are also foreseen for the processing and merger of data. Consent is to be requested as soon as possible and broad consent is preferred. The Guidelines require that patient data will not be used for the development of biological weapons or discriminatory research content, neither research can be aimed at diagnosing patients

by each location processing the data. Further safeguards encompass the evaluation by the *Ethics Committee*; the *conclusion of a DPIA* with the corresponding SA, or a general *"Datenschutzkonzept"* within partner institutions approved by all the corresponding SAs; the set-up of *central trustee services to manage identity data of patients in a secure and separate way*; the establishment of Use and Access Committees at MII partners which decide on the release of data and biomaterials and ensure compliance; the *publication* of the regulations for use and the details of the *funding* and *consortia* involved[246]. *Data transfers* to countries with lower protection levels cannot be made on the basis of consent, and patient data may be *stored* and used for up to 30 years after the patient's most recent consent was given, unless the patient objects in the meantime[247]. Finally, patient data from past treatment cases at the time of consent may be used if they are relevant for the current treatment, *e.g.* data on previous diagnoses, examination findings and therapies.

Additional data protection provisions at a federal and *Bundesland* level may supersede the general provisions relating to safeguards for research depending on the subject matter and the context of the processing, *e.g.*, State Hospital Acts (*Krankenhausgesetze*) of the *Bundesländer* may provide *lex specialis* relating to the appropriate safeguards for the processing of personal data for research purposes in hospitals.

The Hambach Declaration on Artificial Intelligence, which agglutinates the independent federal and state data protection supervisory authorities of Germany, lays down the seven data protection requirements for the **development and implementation of AI solutions**[248].

3.3.8 Greece

Further safeguards are contained for the social research in the law L.4538/2018 on **National and Specific Registers of the National Center for Social Solidarity** (NCSS)[249].

By Ministerial Decision 88453/2019 internal Rules of Procedure for the **National Institute for Social Research (EKKE)** were established**,** requiring inter alia submitting *a Data Management Plan* by the scientific Project Managers at the beginning of each research project. Such a plan should inter alia specify the period of accessibility of the data, the format of the files that will be submitted to the EKKE

or to influencing their specific treatment. As for the consent requirements, the Guidelines provide for transparency and accountability measures such as documentation of the consent and explanatory materials.

[246] Other safeguards include the establishment of distribution lists in which patients can register on newly registered research projects; the offering of the possibility for patients to cancel their participation at any time, verbally or in writing, without providing a reason, and without detriment; the establishment of clear, defined, and appropriate processes for the deletion of data and for additional findings as well as its inclusion in the project application; the rule of the German law for the use of patient data and, if applicable, biomaterial on the basis of the submitted consent documents.

[247] This period is based on the legally determined retention periods for patient data in the care system.

[248] Appropriate measures include: (i) the respect for the principles of Article 5 of the GDPR, in particular the data minimisation principle, and the establishment of technical and organisational measures of Article 25 of the GDPR; (ii) use of AI for constitutionally legitimised purposes, without overriding the requirement of purpose limitation, and the delimitation of purposes by Article 6(4) of the GDPR, although extended processing purposes must be compatible with the original purpose of collection, also for training purposes of AI systems; (iii) transparency, comprehensibility, accessibility, explainability, and accountability of AI systems, according to Articles 5(1)(a), 5(2) and 12 of the GDPR; (iv) risk-assessment to ensure fairness and avoid discrimination and creation of countermeasures to discrimination and risk monitoring; (v) fulfilment by the controller of the data subject rights under Article 12 of the GDPR and following; and (vi) security measures in accordance with Article 32 GDPR and the requirement of a DPIA if personal data is involved; (vii) technical and organisational measures in accordance with Articles 24 and 25 of the GDPR, such as pseudonymisation, as well as the development of knowledge and best practices in conjunction with the SAs.

[249] Here, the law determines that the creation and maintenance of the National Registers is governed by the applicable personal data protection provisions, where anonymisation plays a principal role. The law also regulates the technical and operational requirements of the National and Specific Registers; the conditions and the electronic registration process; the issues of direct information and connection of the National Registers; the disciplinary processes in cases of failure to provide information or incorrect information by those responsible; and the organisational and technical issues of confidentiality and security, such as the right of access and use, data encryption, communications security, confidentiality and use of anonymisation techniques to the Decision of the Minister of Labor, Social Security and Social Solidarity.

Data Repository and the accompanying items, the way of resolving the issues that may arise from the free availability of data, especially regarding the protection of personal data.

Sectoral legislation in Greece has been largely issued in the **health sector**. For these purposes, the law L.4600/2019 on the Establishment of a National Public Health Organization determines some safeguards regarding the processing of health data. As such, the law obliges the individuals processing health data from the National Registers to observe *confidentiality* and the confidentiality provisions contained in the Greek Code of Medical Ethics, the Civil Service Code and the Penal Code apply.[250]

3.3.9 Iceland

The Act on Statistics Iceland (no. 163/2007)[251] regulates the use by **Statistics Iceland** of its large collection of data for scientific research purposes[252]. All the information which has been collected for official statistics are considered *confidential*. Statistics Iceland also reserves the right *to classify data as sensitive, even for categories which are not considered sensitive* under the Icelandic Data Protection Act. According to Article 13 of the Act, Statistics Iceland *can provide access to confidential data* for scientific research and the production of official statistics[253].

Transferring and processing of personal data for the purpose of public archives is regulated in the provisions of the **Public Archives Act**[254].

Approvals of scientific research in the health sector are governed by the **Act on Scientific Research in the Health Sector**[255]. The Act No. 44/2014 on **Scientific Research in the Health Sector** requires that scientific research be founded upon respect for the human dignity of the participants and states that human rights shall *not be sacrificed in favour of the interests of science or society*. Furthermore, scientific research projects in the health sector are to be based upon a *research protocol* which provides information on the study and its principal investigator. In applications submitted to a bioethics committee (of which there are three, the National Bioethics Committee, a committee in Landspítali, the National University Hospital, and a committee in Akureyri Hospital), circumstances which might lead to a *conflict of interest have to be declared*. The Act also states that those who are granted access to identifiable health information materials or other personal data in the implementation or monitoring of a study are subject to *a duty of confidentiality*. Additionally, health information materials which were acquired for a retrospective study, or arise from such research, may be retained **permanently** in *a biobank or health databank*, if this was stipulated in the **research protocol**, which has been **approved by a bioethics committee.** Health data from each scientific study shall be stored separately in a health

[250] It further determines that the specific organisational and technical security measures for the protection of personal data will be issued by a *Ministerial Decision, which will include the use of anonymisation, pseudonymisation and encryption* techniques. Moreover, sensitive data of the National Registers may not be processed for other purposes by third parties, such as employers or insurance companies and banks. Penalties and imprisonment are established in case of interference and exploitation of data from the National Registers.

[251] Act on Statistics Iceland and official statistics (2007 *Lög um Hagstofu Íslands og opinbera hagskýrslugerð*), viewed 5 July 2021 , https://statice.is/about-statistics-iceland/laws-and-regulations/ .

[252] See also Article 11(10) of the Act on Data Protection and the Processing of Personal Data. Processing is to be carried out *based on a law* which provides suitable and *specific measures* to safeguard the fundamental rights and the interests of the data subject.

[253] However, strict security measures are set up for access to the data. A researcher will need to be performing research which is sponsored by certified Icelandic sponsors. Access to the information is restricted, stressing traceability and security. Statistics Iceland will prepare the data based on a request. Access will only be granted after direct or indirect identification has been removed. The research services will also assess the risk of traceability, and if needed e.g. merge categories of data to ensure confidentiality. In order to ensure data protection, access is permitted through secure remote access with login and passwords provided by Statistics Iceland (see https://www.statice.is/services/data-for-scientific-research/, viewed 5 July 2021). Finally, the researcher accessing the data will need to sign a declaration concerning confidentiality and security.

[254] Article 18 of the Act on Data Protection and the Processing of Personal Data. When personal data is processed for **archiving** purpose, the Icelandic legislation provides for a right to "*provide a statement to be kept with any documentation containing his or her personal data*".

[255] Article 34 of the Act on Data Protection and the Processing of Personal Data.

databank and it is *prohibited to link* together health data on an individual from different studies while they are stored there. Access to and utilisation of the data are subject to the provisions of the **Biobanks and Health Databanks Act**, No 110/2000.

Should health information materials been acquired for use in a specific scientific study on human subjects and should the participants not have granted *consent* for them to be retained for use in subsequent studies, they *shall not be retained for any longer* than is necessary in order to complete the study[256]. After that time the materials are to be destroyed or anonymised, unless their preservation is obligatory under the **National Archives Act** or other legislation. Also, the Publics Archives Act No 77/2014 provides that public access may not be granted to material concerning individuals' financial or private affairs which should reasonably and appropriately be kept confidential, except with the *consent* of the person concerned[257].

Retention of health information materials acquired for clinical trials of medicinal products on human subjects, or arising from such research, is subject to special provisions of the Medicinal Products Act, No. 93/1994, and regulations issued on the basis of that Act.

3.3.10 Italy

Italy has issued sectoral legislation, inter alia, in five main domains of research: epidemiology, electronic health records; scientific publication and teaching; genetic data, and official statistics.

For **epidemiological research purposes**, law regulates the epidemiological surveillance systems and registries of mortality, cancer and other diseases with a view to ensuring active systems of the systematic collection of personal, health and epidemiological data to record and characterise all cases of health risk, a particular disease or a relevant health condition in a defined population[258]. First, they require the establishment of the systems and registries by a decree of the President of the Council of Ministers, upon the proposal of the Minister of Health and after obtaining the opinion of the SA, for the purposes of prevention, diagnosis, treatment and rehabilitation, *planning and assessment of health care, verification of the quality of care, as well as scientific research in the medical, biomedical and epidemiological field*. Furthermore, the required measures include the update of the registers by the *authorities* and *bodies of the National Health Service*, the *pseudonymisation* of health and epidemiological data and the access control systems and mechanisms for the surveillance systems and registers[259].

In the field of electronic health records (EHR), the Decree-Law No 179 of 18.10.12[260] establishes the appropriate measures for the purposes of scientific research in the **medical, biomedical and epidemiological fields**. It provides that the Regions and the Ministry of Health may process health data though the EHR, provided that they *are deprived of the direct identification information of individuals*

[256] A bioethics committee may however decide, after the final findings of the research have been submitted to the committee, that necessary health information materials are to be retained for a specified period, as required in order to evaluate the study.
[257] Article 26 Public Archives Act, No 77/2014.
[258] See the Decree-Law No 179 of 18.10.12 on epidemiological surveillance systems and registries of mortality, cancer and other diseases and Decree of the President of the Council of Ministers on the identification of epidemiological surveillance systems and registries of mortality, cancer, and other diseases adopted on 3.3.2017 are the main corpus of law.
[259] A specific regulation is required for identifying the subjects who may have access to the surveillance systems and registers, the data they may know and the related operations, as well as the measures for the custody and security of the data (see Decree of the President of the Council of Ministers on the identification of epidemiological surveillance systems and registries of mortality, cancer, and other diseases adopted on 3 March 2017 which enlists the surveillance systems and registers of mortality, cancer and other diseases established at national and regional level, viewed on 4 August 2021, https://www.gazzettaufficiale.it/eli/id/2017/05/12/17A03142/sg.
[260] Decreto-Legge convertito con modificazioni dalla L. 17 dicembre 2012, n. 221 (in S.O. n. 208, relativo alla G.U. 18/12/2012, n. 294), viewed 28 April 2021, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012-10-18;179!vig=.

and pseudonymisation techniques are used[261].

The Decision No 146 **issued by the *Garante*** on 5 June 2019 defines **additional safeguards** for the necessary processing of data **for medical, biomedical and epidemiological research purposes**. The *Garante* specifies the duty to controllers *to document*, in the research project, the special or exceptional reasons for which the *consent* and/or the fulfilment of their informational duties *vis-a-vis* the data subject *cannot be achieved*[262]. In the case of **biological data and samples**, it further requires the application of *encryption or identification codes* or other means during the retention period[263].

In the area of **scientific publication and teaching**, the Veneto Region adopted a *Code of conduct* for the use of health data for educational and scientific publication purposes, approved by the Garante on 14 January 2021[264]. The Code specifies that while processing the following categories of data (tax code, sex, age, residence, domicile, profession, civil status, health data, and genetic data), *anonymisation or pseudonymisation* techniques are to be in place, being its processing prohibited if otherwise, *unless the controller asks for consent* of the data subject[265]. *Anonymisation is the rule for the Code*, and only if not possible, the controller has to obtain a specific consent of the data subject, after which the data shall in any event be pseudonymised[266]. Publication of clinical cases is possible as long as the identifiability of the subjects involved is not possible. Information to the data subject is required as well. The *retention period is stipulated as three years*[267]. Finally, the data controller must adopt suitable organisational and technical measures to guarantee a timely and complete telematic response to requests made by interested parties to exercise their rights.

[261] As implementation of these provisions, the Prime Ministerial Decree No 178 of 29.09.2015 was issued and is under revision at this stage. The regulation sets out, among others, the pseudonymisation techniques, the guarantees to ensure the rights of data subjects as well as the security measures with regards to the processing of the personal data concerning health data stored in EHRs. The pseudonymisation requirement is further mirrored in the Ministerial Decree No. 262 of 07.12.16 on the interconnection at national level of the various health information systems of the National Health Service.

[262] As regards the processing methods, the Decision imposes the adoption of *encryption or pseudonymisation techniques* or other solutions where research cannot achieve its aims without the identification, even temporary, of the data subject. In these cases, the codes used *cannot be deduced from the personal identification data* of the data subjects, unless this proves impossible due to the particular characteristics of the processing or requires a manifestly disproportionate use of means. In these cases, as well as for the temporary and essential combination of identifying data, it is also required its *justification in writing*. In general terms, the *Garante prohibits disseminating special categories* of data and allows jointly processing several special categories of data, *for the purposes and areas of scientific research* laid down by the Decision. It also requires the *indication of the retention* period of personal data, following the conclusion of the study, after which the aforementioned data and samples shall be anonymised.

[263] The *Garante* pays further special attention to the placement of suitable arrangements to ensure the *quality* of the data and its correct attribution to the data subjects; appropriate confidentiality (access control), i*ntegrity* (labelling techniques to avoid traceability), and *availability* (partial or complete loss of data) measures in the recording and storage of data, *e.g*. through the partial or complete application of encryption technology to file systems or databases, or through the use of other measures that make the data unintelligible to unauthorised parties; *secure transmission channels*, particularly to centralised databases, or to sponsors or external parties, as well as the nomination of a receiving agent at the sponsor´s premises and the use of different transmission channels for the sharing of the data encryption key in case of optical media transmission (CD-ROM); and with specific reference to the processing of trial data stored in a centralised database, the necessity to adopt *access control* procedures for authentication and authorisation, organisational measures for the periodic verification of the quality and consistency of the access mechanisms, and audit log mechanisms for controlling access and detecting anomalies..

[264] The Code was adopted in order to identify the methods of processing, also by means of anonymisation and pseudonymisation techniques, of personal data on the health of patients, by the data controller and the subjects adhering to the Code for the production of documents for teaching purposes or scientific publication by health professionals.

[265] If compliant with the previous, the processing of data is permitted for the drafting of reports for participation in conferences, seminars and/or drafting of scientific publications, training, in-depth analysis, discussion and scientific debate relating to a clinical case, also in the company context, which is not subject to dissemination. In order to do so, the processing has to be authorised upon the request of a healthcare professional working for the controller, and the data has to be assigned a unique identification code.

[266] The anonymised dataset, produced by adopting the methodologies set out and documented can thus be made available to the professional and may be used by him/her, together with the corporate logo and/or sponsorship, bearing the unique identification code assigned to the dataset.

[267] The requests submitted by the health professional and the datasets shall be kept in an indexed archive with both electronic and analogue methods and subjected to security measures.

The processing of **genetic data for scientific research** is regulated by **Decision No. 146 of the *Garante***. In general, the processing of genetic data and biological samples for scientific research purposes is permitted only if (i) *aimed at protecting the health of the data subject*, third parties or the *community* in the medical, biomedical and epidemiological fields; or (ii) in the context of clinical trials or scientific research aimed *at developing genetic analysis techniques*[268]. When the purposes of the research can be achieved only through the identification, even temporary, of the data subjects, the data controller needs to *separate the identification data from the biological samples and genetic information* already at the time of collection, unless this proves impossible due to the particular characteristics of the processing or requires a manifestly disproportionate use of means. Information shall be provided to the interested parties[269]. In case genetic data and biological samples of people *who cannot provide their consent* and which do not entail a direct benefit for them are to be processed, they may only be processed under strict conditions[270]. In the event that the interested party *withdraws consent* to the processing of data for research purposes, the *biological sample is also destroyed* as long as it has been taken for such purposes, unless, originally or following processing, the sample can no longer be referring to an identified or identifiable person[271]. *Communication and transfer* of genetic data and biological samples collected for scientific research purposes may be done in the context of joint projects and in compliance with Article 26 of the GDPR[272]. *Consent is always required* for scientific research except when provided by law or other specific requirements referred to in Article 9 of the GDPR. The **publication and dissemination** of genetic data should obey specific rules other than those laid down by the GDPR and the PDPC applying to special categories of personal data[273]. In particular, genetic datamust be disclosed by health professionals and health bodies only through a physician designated by the data subject or the data controller or through another health professional authorised by the controller and properly trained with regard to *appropriate procedures and precautions* related to the context in which the data processing is carried out. Also, the processing of genetic data and the use of biological samples for the execution of

[268] The project has to specify (i) the measures to be adopted in the processing of personal data to ensure data protection compliance; (ii) the profiles, measures the custody and security of data and biological samples; (iii) any data processors; (iv) the origin, nature and methods of taking and storing the samples; (v) the measures adopted to ensure the voluntary nature of the provision of the biological material by the data subject.

[269] This needs to highlight (i) the measures adopted to allow the identification of data subjects only for the time necessary for the purposes of collection or subsequent processing; (ii) the ways in which interested parties, who request it, can access the information contained in the research project; (iii) the right for interested parties not to be informed about the results of the research, including any unexpected findings concerning them that are relevant for their health.

[270] These conditions shall occur simultaneously (i) the research is aimed at improving the health of other people belonging to the same age group or suffering from the same pathology or who are in the same conditions and the research programme is subject to a reasoned favourable opinion from the competent ethics committee at territorial level; (ii) a search of similar purpose cannot be carried out through the processing of data referring to persons who can provide their consent; (iii) consent to the processing is acquired by those who legally exercise parental authority, or by a close relative, a family member, a live-in partneror, in their absence, by the manager of the facility where the person is staying; (iv) the research does not involve significant risks for the dignity, rights and fundamental freedoms of the data subjects.

[271] As for the *retention period* and further processing, the Decision No. 146 stipulates that, *in the absence of the consent*, the biological samples and genetic data collected for health protection purposes can be stored and further processed for scientific research if required by European Union law, by law or, in cases not provided by law, by regulation; and if limited to the pursuit of further scientific purposes directly connected with those for which the informed consent of the interested parties was originally acquired. When due to particular reasons it is not possible to inform the data subjects, the storage and further use of biological samples and genetic data *are permitted* if research has a similar purpose; biological samples and genetic data do not allow the identification of the interested parties and it does not appear that the latter have any previously given contrary indications; or the research programme, previously subject to a reasoned favourable opinion from the competent ethics committee at the local level, is subject to *prior consultation with the Guarantor pursuant* to Article 36 of the GDPR.

[272] In the case of autonomous data controllers, it may be done, limited to information without identifying personal data, for scientific purposes directly linked to those for which they were originally collected and clearly determined in writing in the request for data and/or samples. In this case, the requesting subject undertakes not to further process the data and/or use the samples for purposes other than those indicated in the request and not to communicate them or further transfer them to third parties. More concretely, when the processing concerns *research on isolated groups of population* then the research shall be preceded by *information activities vis-à-vis the concerned communities.* This shall illustrate the nature of the research, the aims pursued, the methods of implementation, the sources of funding, the expected risks or benefits for the populations involved, any risks of discrimination or stigmatisation of the communities concerned, as well as those inherent in the knowledge of unexpected relationships of consanguinity and the actions taken to minimise these risks.

[273] In particular, Section 2-f of the PDPC paragraph 8, provides for the prohibition of disseminating of genetic data, biometric data and data relating to health.

presymptomatic and susceptibility tests can be carried out exclusively for research purposes aimed at protecting health.

In the domain of official statistics, the Legislative Decree No 322 of 6.9.1989 lays down the rules on the National Statistical System and on the reorganisation of the National Statistical Institute by highlighting appropriate measures for data minimisation[274]. Furthermore, the Italian SA has issued significant decisions with regard to the principles of data minimisation, storage limitation and data protection by design to reduce the risk of re-identification of data subjects when disseminating statistical results[275].

3.3.11 Norway

The **Norwegian Health Research Act** (H*elseforskningsloven* or *HRA*)[276] stipulates that all proposed health projects must be *approved* in advance by the Regional Committee for Medical and Health Research Ethics (REK)[277]. REK's approval is *often regarded as a supplementary legal ground* for the research, but legal grounds for the processing of health personal data for research purposes are limited to the legal grounds provided under GDPR. In addition to the REK approval, the controller must – together with the DPO (if applicable) – identify a suitable legal ground for the processing of the personal data, as per the GDPR. Furthermore, REK can also decide to exempt the health personnel from his/her duty of client confidentiality[278].

Finally, the **Health Register Act** (*Helseregisterloven*)[279] provides *a legal basis* for establishing *health registries*, from which the data for a lot of scientific research is derived. Section 20 of the Health Register Act states an exemption from the duty of confidentiality for indirectly identifiable health information. Confidentiality does not prevent data controllers from making indirectly identifiable health information available for research purposes. This exemption applies to health information included in statutory health registries, listed in Section 11[280]. These are health registers where names, national identity number and other information based on which persons can be identified, such as the register for causes of death, medical birth register and the Norwegian Patient Register[281]. Also, the health information can only be disclosed if the processing of the information is (i) of significant interest to society; (ii) the consideration of the patient's integrity and confidentiality is safeguarded; and (iii) the processing of the information is unproblematic[282] from an ethical, medical and health perspective[283]. The data controller can also set conditions for the disclosure, to ensure the protection of the fundamental rights and interests of data subjects[284]. Further, it can be mentioned that the Health Register Act is being amended at the time of the writing of this report. Some legislative amendments have been adopted, but have not yet entered into force. An administrative regulation is also subject to public consultation. Among other things, more concrete requirements will be set for deletion of datasets used for research, and due to the new analysis

[274] According to Article 6-bis of said Legislative Decree, personal data should be rendered anonymous after being gathered or when their availability is no more necessary for statistical processing. It further states that separation measures for recorded data should be in place, except if it is proved to be impossible because of particular processing peculiarities or for implying the use of evidently excessive means, and only temporarily matched with personal information if essential for statistical purposes.
[275] See in particular the decision of 23 January 2020, viewed 4 August, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9261093.
[276] *Lov om medisinsk og helsefaglig forskning (helseforskningsloven)*, LOV-2008-06-20-44.
[277] Cf. the Health Research Act Chapter 3. REK undertakes a *standard evaluation* of the research ethics of the project and judges whether the project satisfies the requirements laid down in HRA, and may specify conditions for approval and appropriate safeguards for the research project, e.g. data minimisation (Paragraph 10 HRA).
[278] Confidentiality could in practice be regarded as additional safeguards (Chapter 5 HRA).
[279] *Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)* LOV-2014-06-20-43, viewed 26 May 2021, https://lovdata.no/dokument/NL/lov/2014-06-20-43.
[280] Section 20(1) of *Lov om helseregistre og behandling av helseopplysninger*.
[281] The full list available in Section 11 of the *Lov om helseregistre og behandling av helseopplysninger*.
[282] The Norwegian law uses the wording "*unbetenkelig*".
[283] Section 20 (2) of *Lov om helseregistre og behandling av helseopplysninger*.
[284] Idem.

system, the Health Analysis Platform[285], there will likely be less need for the disclosure of pseudonymised or directly identifiable data. Instead, the analyses are to be conducted in a secure analysis room, and only anonymous analysis results will as a starting point be extracted.

Further, Chapter 5 of the **Health Personnel Act** ("helsepersonelloven")[286], Section 29 in particular, regulates the duty of confidentiality and the right of disclosure. The Health Ministry can determine that information may or shall be provided for use in research, and that in such circumstances, the duty of confidentiality shall not apply[287]. The Ministry can set specific conditions in regulation. Similar provisions, where data can be used for scientific purposes subject to decisions of the responsible ministry, also exist in the Public Administration Act[288] and the National Insurance Act[289].

The **Act relating to treatment biobanks** (Lov om behandlingsbiobanker)[290] regulates the collection, storage, processing and destruction of materials included in biobanks[291]. A register of glistereded biobanks is held by the responsible **Ministry**[292]. The Act stipulates a duty of *confidentiality* for "everyone who creates, stores, uses or otherwise manages or works" with the biobank[293]. In case the specific bank contains information which can be linked to individuals, the Act requires that a data controller exists (which is specified in the Patient Records Act)[294]. The Act relating to treatment biobanks also sets requirements related to the *secure storage* of the material[295] and on *information and consent* of the patients[296]. However, if the collected material will be altered, extended or a new use has been established, *a new voluntary, explicit and informed consent must be obtained*, unless otherwise mentioned in the Act related to medical and health research[297]. Consent can be revoked at any time, and the individual revoking the consent *can require the destruction* of biological material, unless the material is anonymised[298].

Access to materials in a biobank can also be granted to others, *if the donor has consented* thereto and the requesting party has *given information* on the purpose of the use of the material, for how long the material will be processed and if the material will be destroyed, deleted or returned after the intended purpose has been fulfilled[299].

---

[285] Helseanalyseplattformen, Direktoratet for e-helse, 22 July 2021, https://www.ehelse.no/programmer/helsedataprogrammet/helseanalyseplattformen.
[286] *Lov om helsepersonell m.v. (helsepersonelloven)*, LOV-1999-07-02-64.
[287] Section 29 to the Health Personnel Act.
[288] Section 13d, and 13e *Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)*, LOV-1967-02-10, viewed on 6 July 2021, https://lovdata.no/dokument/NLE/lov/1967-02-10.
[289] Section 25(13), National Insurance Act (*Lov om folketrygd - folketrygdloven*), LOV-1997-02-28-19.
[290] Lov om behandlingsbiobanker, viewed 26 May 2021, https://lovdata.no/dokument/NL/lov/2003-02-21-12?q=biobank.
[291] The Act requires that such is carried out in an ethically sound manner and exploited *for the benefit of the individuals and society*. Processing of materials included in the biobanks shall be done in accordance with privacy considerations, principles protecting human dignity, human rights and personal integrity, without discrimination of the data subjects: see Section 1 of the Act related to biobanks.
[292] Section 6 of the Act related to biobanks.
[293] Section 16 of the Act related to biobanks. Section 7 of the Act further requires that each biobank have a person responsible for the biobank, who should have a medical or biological education of higher degree.
[294] Section 7 of the Act related to biobanks. In addition, the Ministry can decide that certain biobanks not only have a person in charge, but also a board of directors and the duties and composition of that board: see Section 7 of the Act related to biobanks.
[295] Section 9 of the Act related to biobanks.
[296] A consent to healthcare is interpreted as comprising also the collection, storage and treatment of biological material: Section 11 of the Act related to biobanks.
[297] Section 13 of the Act related to biobanks.
[298] Section 14 of the Act related to biobanks.
[299] Section 15(1) of the Act related to biobanks. The holder of the material must assess the request, taking the following in to account: whether allowing access to the material will "*make it impossible or significantly complicate*" to safeguard the biobank's legal obligations concerning storage and processing of the material, the interests of the donor and the processing of the material: see Section 15(2) of the Act related to biobanks. A refusal of access can be appealed to the Ministry: see Section 15(5) of the Act related to biobanks.

Both the Norwegian SA and the Norwegian Board of Health Supervision supervise health research, including related to research biobanks (the Health Research Act). The Norwegian SA also supervises the GDPR/Personal Data Act, the Patient Records Act and the Health Register Act. The Health Research Act constitutes the only legislation specifically adopted for the purpose of research. Hence, no legislation corresponding to that applicable to medical and health research has been adopted to other fields of research. For such cases researchers processing confidential information must be granted an exemption from the duty of confidentiality in the form of a decision from the public authority. This decision should serve as a form of safeguard. It can nevertheless be mentioned, that such a decision does not offer the same kind of control over research as in medical and health research.

3.3.12 Poland

The Act on Higher Education and Science[300] states that **Higher Education and Research Institutes** — a special type of legal entity within the Polish legal system[301] - enjoy special exemptions with regard to applying the specific provisions of GDPR, such as Articles 15, 16, 18 and 21[302]. Sensitive data can be processed if the results of the scientific and development process are *published* in a way that the individual, whose data were used, cannot be identified —meaning anonymisation[303]. Moreover, as to the appropriate **technical and organisational security measures**, a *personal data administrator shall be appointed*[304]. The statute also provides that *personal data shall be anonymised as soon as the research objective is achieved*. Until then, the data which may be used to identify the natural person concerned shall be *recorded separately*[305].

Concerning **pharmaceutical and clinical trials**, the Regulation of the Minister of Health of 2 May 2012 on Good Clinical Practice[306], which is *lex specialis* to the Pharmaceutical Law[307], provides the data subject with additional safeguards. It in particular regulates organisational and safety measures with regard to storage of data from clinical trials[308]. Additionally, if the collected data are processed, **the sponsor shall ensure that the processed data can be compared with the original data**[309]. **Medical records** may be established and maintained in order to monitor *the demand for health care services*, monitor the *health status* of service recipients, conduct health prophylaxis or implement health

[300] Act of 20 July 2018 Law on Higher Education and Science.
[301] Articles 6 and 7 Act of 20 July 2018 Law on Higher Education and Science.
[302] The condition for this waiver is the likelihood that these rights will prevent or seriously impede the achievement of the objectives of scientific research and development work. The exemption of these rights needs to be necessary to achieve particular scientific and development objectives.
[303] Art 469b.2 of the Act of 20 July 2018 Law on Higher Education and Science.
[304] Technical and organisational measures include further pseudonymisation and encryption, processing personal data of a minimum number of persons necessary for research and development, in each particular purpose, controlling access to the premises where the documents containing personal data are stored, and developing a procedure to determine how the data are secured: see Art 469b.3 of the Act of 20 July 2018 Law on Higher Education and Science.
[305] They may be combined with particulars of the individual concerned only if the purpose of the research or development so requires.
[306] Regulation of the Minister of Health of 2 May 2012 on Good Clinical Practice.
[307] Pharmaceutical Law.
[308] Paragraphs 4 and 13 of the Regulation of the Minister of Health of 2 May 2012 on Good Clinical Practice, viewed 6 July 2021, http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20120000489/O/D20120489.pdf (Polish version). The sponsor — person responsible for clinical trial - shall prior to the start of processing data including personal data, ensure that there is a **written instruction on the use of the IT data storage system** and **ensure that the IT data storage system is documented to have been implemented after an assessment of its security and functionality**. Moreover, the sponsor shall **provide access to the computerised data storage system and data changes in such a way that data changes can be retrospectively verified**, and it shall **indicate people allowed to process the data obtained in connection with the clinical trial**.
[309] Other researcher's responsibilities include: preparing, storing, updating and making available the list of persons to whom the researcher has entrusted duties related to the conduct of the clinical trial, and acquainting, prior to the start of the trial, all such persons with their duties and with the clinical trial protocol and the investigational medicinal product, to the representatives of the sponsor or the President of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products, hereinafter referred to as the "President of the Office for Registration". Moreover, they should be **keeping records related to the conducted clinical trial** and make them available to entities authorised to inspect them.

programmes or health policy programmes, monitor and evaluate the safety, effectiveness, quality, and cost-efficiency of diagnostic tests or medical procedures of diagnostic tests or medical procedures. They may include personal data — including individual medical data storage[310]. The data contained there may be made available for the purpose of scientific research and for statistical purposes **in a form that does not allow them to be linked to a specific individual**[311].

[310] The minister responsible for health matters is responsible for establishment and maintenance of the medical records: see Article 19(1) of the Act of April 28, 2011 on the Information System in Health Care.
[311] Article 19(7) of the Act of April 28, 2011 on the Information System in Health Care.

4 CONVERGING ELEMENTS AND TRENDS

This section discusses both converging elements (section 4.1) as well as trend (section 4.2) in both EU and national legislation and soft law. The term "converging element" is used if a certain safeguard was present in more than six countries, whereas the term "trends" is used to clarify emerging tendencies in fewer countries.

4.1 CONVERGING ELEMENTS

The most important converging safeguards when implementing Article 89(1) GDPR relate to data minimisation requirements, such as pseudonymisation and anonymisation techniques, technical measures for security management, confidentiality and integrity, including encryption, organisational measures and measures for publication and dissemination, which all tend to protect the rights of the data subjects when their data are used for scientific research. Other important similarities relate to access, disclosure and transfer. In the sectoral legislation, similarities can be mostly found in more established domains as statistical use and registries, while converging elements remain rather modest in the other sectors, e.g. confidentiality obligations. An indication of where the elements were found, are added and detailed as much as possible. Section 4.1.1 discusses converging elements in the general legislation and soft law, while section 4.1.2 analyses converging elements in sectorial legislation and soft law.

4.1.1 General GDPR implementing legislation and soft law

4.1.1.1 Data minimisation: pseudonymization or anonymization

The use of both **pseudonymisation**[312] and **anonymisation** techniques[313] are mentioned and broadly required in 10 to 11 countries to be implemented as safeguards for the rights and freedoms of the data subjects when deploying personal data for conducting scientific research in general[314]. Some countries introduce in their legislation cases also specific normative provisions for anonymisation (e.g. responsible entity) and pseudonymisation (e.g. separation of the codes with corresponding identification data, specify when such a particular data minimisation technique is required, conditions for de-pseudonymisation, responsible persons with regard to keeping the keys and deletion) as well as their order of preference.

Pseudonymisation and anonymisation are crucial safeguards for data subjects, while these safeguards need to be balanced against the interests of the scientific research. They are both *an organizational and technical measure*. Further consultation and guidelines as to the necessity ('when') and procedural aspects ('how') of such safeguards could be considered in order to increase consistency in the EEA States, which would be of benefit for both researchers and data subjects, while facilitating international research in particular.

[312] EE, FI, NO, IS, AT, DE, IT, EL, BG, PL, BE.
[313] FI, NO, IS, AT, DE, IT, EL, FR, PL, BE.
[314] At the same time, few indications are given as to *how* to make the assessment as to *when which technique should be applied*, *how* and *what is needed* for anonymisation as opposed to pseudonymisation, *the responsibility of which remains primarily with the researchers.* Sometimes, national law takes 'sensitive data' as a criterion (e.g., in DE, Article 27(3) *BDSG* imposes anonymisation of special categories of personal data processed "as soon as the research purpose allows"). This is different for research in some specific sectors. Contrary to the general GDPR implementing legislation, some sectors are specific as to what type of and how data minimisation shall be applied for protection of the data subjects' rights: e.g., for statistics, specific law points to anonymisation and/or a specific entity's task is to do so.

4.1.1.2 Technical measures

At least 10 countries require *technical* and organisational measures[315]. At the same time, some countries only refer to the wording as mentioned in Article 89(1) of the GDPR, without specifying what those safeguards entail, while other countries provide detailed guidelines, e.g., the SA on their webpage[316]. Additional similarities with regards to required *technical* measures are the need for **confidentiality, access control**[317] requirements and procedures to prevent intrusions and unauthorised access and activities within the systems and **access logging** in at least 10 of the 12 countries[318]. Similarities can also be identified for technical measures *ensuring integrity and availability*[319]. **Encryption** is imposed as a safeguard in at least 11 of the 12 countries[320]. Similarly, a majority of countries implement input controls, such as record registry of access, input, alteration and deletion[321]. Several countries also require anonymisation once the research is completed or the research purpose can no longer be reached[322].

4.1.1.3 Organisational measures: confidentiality, training and monitoring of measures

The **monitoring** of organisational measures[323] is required in more than eight of the 12 countries. A confidentiality obligation upon all persons authorised to process personal data for scientific research purposes is a safeguard widely spread among the EEA States. While some countries have explicitly recognised the duty to confidentiality in their national law[324], other countries have opted to incorporate a direct reference to the GDPR[325]. At least 11 countries also require that personnel undergo instruction or proper **training** to increase awareness and compliance with the data protection framework for scientific research[326]. A similar authorisation requirement also exists in France, requiring that the data resulting from the processing, and which are kept by the controller or a subcontractor can only be accessed or modified by authorised persons[327]. Poland requires that only the minimum number of people should be granted the right to process the data, based on what is necessary for research and development[328]. Other convergences relate to the establishment of procedures and policies to regularly test, assess, and evaluate the effectiveness of technical and organisational measures for ensuring security. Here, again, while a majority of countries have positivised such duty[329], a minority of them have provided for a direct reference to the GDPR for the implementation of such organisational measures[330].

[315] See e.g., NO: Articles 8 and 9 of the Norwegian Data Protection Act, IS: Article 18(1) of the Act 90.2018, AT, DE: 22 BDSG, IT, EL, BG: Article 25m. of the new, SG No 17 of 2019, FR: Article 78 of the Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, PL: Article 469b of the Law on Higher Education and Science, and FI.
[316] e.g., FI: see the list of safeguards on https://tietosuoja.fi/en/choosing-the-processing-basis-and-ensuring-its-lawfulness.
[317] Additionally, in at least nine of the 12 countries restricted access areas are imposed (closed security areas): FI, NO, IS, AT, IT, BG, FR, PL, BE.
[318] FI, NO, IS, AT, DE, IT, EL, BG, FR, PL, BE.
[319] Technical measures used to address availability are requirements to storage systems and requirements for documented back-up and recovery mechanisms, also implemented in a majority of countries: see FI, NO, IS, AT, DE, IT, BG, FR, BE.
[320] FI, NO, IS, AT, DE, IT, EL, BG, FR, PL, BE.
[321] FI, NO, IS, AT, DE, IT, BG, FR, PL, BE.
[322] See e.g, PL.
[323] EE, FI, NO, IS, AT, DE, IT, EL, BG, PL.
[324] FI, AT, DE, IT, EL, BG, FR, BE.
[325] EE, NO.
[326] EE, FI, FR, PL, NO, IS, AT, DE, IT, EL, BE.
[327] Article 116 of the decree n°2019-536 of May 29, 2019.
[328] Article 469b.3 of the Law on the Higher Education. E., Act of 20 July 2018 The Law on Higher Education and Science, viewed 7 July 2021, act-of-20-july-2018-the-law-on-higher-education-and-science.pdf (konstytucjadlanauki.gov.pl) .
[329] FI, AT, DE, IT, EL, BG, PL.
[330] EE, NO, IS.

4.1.1.4 Safeguards for publication of research and dissemination[331]

At least six countries agree that personal data intended for publication or dissemination should undergo a technical process to prevent or hinder the identification of the data subject, and impose technical measures, in particular pseudonymisation and/or anonymisation ***for dissemination and/****or* ***publication*** of scientific research, to guarantee the respect of the data subjects' rights and freedoms[332].

4.1.1.5 Disclosure and access by third parties and data transfers

In the national legislation of at least six countries[333] specific protection and safeguards are required when personal data are transferred or when the data are disclosed and/or accessed or processed for other purposes[334]. E.g., Estonia additionally requires pseudonymisation or equivalent levels of data protection prior to the transmission of personal data[335]. The Austrian legislator demands the deletion of name data of sensitive data records after the scientific research purposes have been achieved[336]. In Belgium, an agreement needs to be concluded between the two controllers[337].

[331] See also Recital 159 GPDR.

[332] AT, BE, EL, IT, FR, PL. At the same time, the specific measures required may vary. Consent or necessity is generally not required provided the data undergo *pseudonymisation* before being published. Three trends (and groups of countries) can be identified: (i) the countries who impose pseudonymisation and anonymisation techniques (e.g., AT: Austria enables research institutions (Article 2.b.12 of the FOG) to publish and disseminate all personal data for scientific research purposes, in any case, if (a) instead of the name, area-specific personal identifiers or other unique identifiers are used for allocation, or (b) the processing is carried out in pseudonymised form; or (c) if the publications are made in anonymised or pseudonymised form or without names, addresses or photographs); (ii) the countries who adopt pseudonymisation techniques; and (iii) those who opted for the application of anonymisation techniques. The second approach is found in EL and BE. Greece allows the publication if (a) the data subjects have given their consent in writing or (b) the publication is necessary for the presentation of the results of the research. In the latter case, the results must undergo pseudonymisation before being published. Belgium lays down a generic framework on dissemination of personal data for scientific research, which is only applicable in the absence of European Union law, special acts, ordinances or decrees imposing more stringent conditions. Under these conditions, the controller must apply pseudonymisation techniques for the dissemination of personal data. Exception to this rule covers the dissemination of sensitive data, which is not allowed, as well as the dissemination of non-pseudonymous data if some of the following conditions concur: (a) data subject´s consent; (b) data made publicly available by the data subject in person; (c) data closely linked to the public or historical nature of the data subject or facts in which the data subject was involved (Article 205 of the Belgian Data Protection Act).The third group of countries is represented by IT, FR, and PL. Italy allows for the communication and dissemination of personal data by public bodies also to private entities and by electronic networks, except for sensitive data and data relating to criminal convictions and offences (Article 100(1) of the Italian Personal Data Protection Code). For these particular categories of data (in the case of genetic data, biometric data and data relating to health, the specific provisions laid down in Section 2-f , paragraph 8 PDPC prohibit the dissemination of said categories of data, being their dissemination only posible if the information has been adequately aggregated in such a way as to avoid the risk of re-identification of data subjects), the Italian legislator delegates the authority to establish the specific rules for publication and dissemination to the Garante, who shall take account of the principles laid down in the relevant Council of Europe's Recommendations for these purposes (Articles 106(1) and 106(2)(b) of the Italian Personal Data Protection Code).These measures have been addressed in Decision No. 146 issued by the Garante on June 5th 2019 as well as in the Rules of conduct for the processing for statistical or scientific research purposes, published on 14 January 2019. According to these pronouncements, sensitive data and data relating to criminal convictions and offences can only be disseminated for scientific research purposes if anonymised, as a rule. France equally recognises the implementation of anonymisation techniques as a condition for the dissemination of personal data, unless the interest of a third party in the dissemination prevails over the interest or fundamental rights and freedoms of the person concerned (Article 116 of the decree No 2019-536 of May 29, 2019.). In such case, the dissemination of scientific results must be absolutely necessary for its presentation, and the data disseminated must be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Lastly, Poland require anonymisation techniques to be put in place for the publication of scientific results, particularly for sensitive data, if its processing is necessary for conducting scientific research and development work (Article 469b(2) of the Law on the Higher Education.).

[333] BE,EE, FI, AT, DE, IT.

[334] See Article 6(2)(9) of the Finnish Data Protection Act, Article 22(10) of the BDSG, and Article 106(2)(h) of the Italian Personal Data Protection Code.

[335] Article 6(1) of the Estonian Data Protection Act.

[336] Article 2.d.5.m.) of the FOG.

[337] Article 194 of the Act of 30.7.2018.

4.1.1.6 Security management

In 10 out of 12 countries, roles and responsibilities shall be defined while conducting scientific research[338]. E.g., Austrian national law explicitly requires controllers to *"define the distribution of tasks in the processing of data between the organisational units and between employees"*[339].

For the management and evaluation of assets and resources, EEA States seem to have adopted a more lenient approach to the positivation of a systematic governance and management of the resources and assets of the entities in charge of conducting scientific research. In most national legislations, the alignment to this organisational scheme is being done by direct reference to the general provisions of the GDPR, thus *handing over the baton to controllers as to the appropriate measures to be put in place* to maximise the security levels of the processing operations[340].

A special reference to the security management measures within the organisation of the processor is explicitly considered in some countries[341]. Incident response and business continuity plans are not explicitly incorporated into the appropriate organisational measures for scientific research in most of the countries analysed[342][343].

4.1.1.7 Personal data v. 'sensitive' personal data

In most countries[344], there are clear differences in safeguards when personal data are used in research, depending on the type of personal data used ('sensitive' or not) and the domain. Processing of personal data of *special categories tend to be subject to more stringent safeguards*. This is also reflected in sectoral legislation concerning health data in general, clinical trials and biobanks, which obtain more detailed safeguards than for example statistics and social sciences. The difference in approach can be seen as a risk-based approach in the sense that the less sensitive the data, and possible impact upon the data subjects, the lighter requirements are set. Furthermore, such additional national legislation should also be assessed against Article 9(4) GDPR, allowing EEA States to adopt further conditions.

4.1.2 Sectoral legislation and soft law

4.1.2.1 Description of secondary research purposes and related safeguards *in legislation*

In at least six countries, the legislation or *guidelines describe the secondary research purposes*, e.g. of

[338] EE, FI, NO, IS, AT, DE, IT, FR, PL, BE.
[339] Article 2d.5.d.) of the FOG. It is interesting to see the emphasis that the Austrian legislator has placed on security management procedures, as it conspicuously ensures a precise and organised collaboration among the controller´s human resources, while respecting the tasks and purposes of the processing operations.
[340] EE, FI, NO, IS, AT, DE. Nevertheless, countries such as PL have opted to explicitly introduce a vague concept of appropriate organisational measures in their national implementations of the GDPR. In this sense, PL provides for the development of specific *"procedures to determine how the data is secured" (*Article 469b(3) of the Polish Law on Higher Education and Science).
[341] EE, FI, DE, IT, FR. In most cases, such indication pertains to the establishment of internal measures for preventing access to personal data to ensure appropriate security and confidentiality levels among controllers and processors. These requirements become particularly relevant when processing sensitive data for scientific research purposes, as a direct consequence of the risk-based approach of Article 32 of the GDPR. See Article 6.2.4) of the Finnish Data Protection Act and Article 22(5) of the BDSG.
[342] NO, IS, AT, IT, EL, BG. See however Article 66.2.10 of the BPDPA.
[343] Interestingly, countries such as DE and FI have taken a different approach, and have included measures to ensure the rapid restoration of availability and access (in a timely or rapid manner) in the event of a physical or technical incident when processing sensitive data for scientific research purposes: see Articles 22(8) of the BDSG in relation to Article 27(1) of the BDSG and Article 6.2.7 of the FDPA.
[344] See e.g., BG, FR, PL.

the use of biological material stored in biobanks[345]. Requirements regarding the involvement of *relevant authorities[346] and ethics committees*[347] are also frequent. In Iceland, the main rule is that biological samples shall be acquired for clearly defined and lawful purposes[348]. Access can be granted for *further diagnosis of diseases* or the purpose of *quality control* and *method development*, if the data has been anonymised[349].

4.1.2.2 Description of research methods as transparency measure

In many countries, the legislation or guidelines impose detailed research methods[350].

4.1.2.3 Role for SAs

Eight of the 12 countries give **an important role to the supervisory authorities**[351] for the supervision of research as a safeguard. This role is at the same time also *often substituted and/or completed with a role for the ethical committees* (also in eight of the 12 countries[352]) when personal data are processed for research, especially for sensitive data or research in specific domains, for example when using health-related data, e.g., for secondary research, while this role for ethical committees does not exist in other domains (e.g., research for statistical purposes or social science). One shall also note that the role and the status/nature of the SA is different in the respective domains of research:

- In the (older and more established) domains of the use for statistical purposes, public registers and for archiving in the public interest, the SA is **often a specialised statutory public body**, set up by law[353] authorising disclosure (e.g., to public authorities and researchers) for research and **supervising, assuring or deciding** about the inter alia fulfilment of purposes and other safeguards;
- In other domains, including when health related data is used for research, and in case of likely high risks upon executing the DPIA, the general SA shall in most cases be a priori consulted and authorisation obtained if the safeguards (e.g., consent by the data subject) cannot limit such risks (general SA consultation from the GDPR)[354] .

[345] FI: Section 26-27 of the Biobank Act 688/2012, viewed 5 July 2021,https://www.finlex.fi/en/laki/kaannokset/2012/en20120688; IS: Article 9 of the Act on Biobanks, No. 110/2000, viewed 5 July 2021, https://www.personuvernd.is/information-in-english/greinar/nr/439; NO Section 28 of the Health Research Act, viewed 5 July 2021, https://lovdata.no/dokument/NL/lov/2008-06-20-44#KAPITTEL_6; BG: Article 25m of the Personal Data Protection Act; BE; EE: Human Genes Research Act, Paragraph 1(2), IT: Section 110-bis of the Italian PDPC allowing the further processing of personal data, including the special categories of personal data referred to in Article 9 of the GDPR, by third parties for statistical or scientific research purposes.

[346] IS, FR, NO. Section 28 of the Norvegian Health Research Act sets out that the Regional Committee for Medical and Health Research Ethics decide on the use of human biological material for research purposes without the consent of the patient. This can only be done if the research is of significant interest to society and the welfare and integrity of the participants is considered. Conditions can be set and the patient must be informed that the material can be used in certain cases, and had the opportunity to opt out thereof. An electronic register with overview of patients who have opted out of their biological material being used for research.

[347] FI, FR, BG, PL, IS, NO.

[348] Article 9 of the Act on Biobanks, Paragraphs 1-2.

[349] Article 9 of the Act on Biobanks, Paragraphs 2-3. About Iceland, see also below. One shall however remain critical as to the possibility of 'full' anonymisation for particular personal data.

[350] For instance in Italy.

[351] EE, FI, NO, AT (when the research is aimed at producing personal results and there is no consent and no processing according to the *FOG*), DE, IT, FR, BE. The study found authorisation of use of special categories of personal data by ethics committee (BE, EE, IT, AU) OR Supervisory authority (EE (if there is no ethics committee), FI, NO, EU, DE, IT).

[352] BE, EE, FI, IS, NO IT, AT, FR.

[353] BE, BG, AT, EE, FI, FR, IS, NO.

[354] In some countries, e.g. France, the SA has developed a prior authorisation regime (see also below). In some (Nordic) countries (e.g., Finland) a specific data authority was set up to facilitate and supervising research, as a safeguard.

4.1.2.4 Statistics and population based registries

National legislation relating to **statistics** and regulating e.g., national population-based cancer **registries**[355] imposes very specific safeguards. This legislation *ensures that controllers are informed but also comply with all relevant safeguards*, for reaching the aims, and resulting in flourishing and extensive (international) collaboration in this domain. The collection and use of personal data **from populations for statistical purposes** has a *long(er) tradition*, and is regulated with specific law in at least five countries[356]. *Statutory confidentiality obligations of the statistical authorities* (see also recitals 162-163 GDPR) is a recurring element and the **legislation** further seeks to impose transparent safeguards, such as to guarantee that statistical data *cannot be linked to identified or identifiable* persons where possible and identifying data and intermediate results *separated*, safeguarded and/or duly *deleted*. In some cases, communications to third parties shall be duly governed by *contractual agreements* imposing additional safeguards, such as research *purpose limitation*, transfer restrictions, etc. In some countries, *voluntary participation* by individuals is embedded in the law as well. These legislations and networks provide legal certainty including as to the rights and to the data protection of the data subjects as well.

4.1.2.5 Scientific research in higher education and academic establishments

In at least eight countries[357] **practices and/or rules of conduct** were established for research by national scientific research centers, higher education and academic establishments.

4.1.2.6 Transparency and information to participants in case of use of health

In both international instruments and sectoral legislation of at least six countries, *transparency* about the use of the personal research data towards participants could be considered a safeguard, in particular in the case of the use of health data including biological samples[358]. This is also related to the requirement of informed consent[359]. The more significant data (e.g., genetic data) is used and/or shared for scientific research, **the more detailed the transparency information becomes** e.g., specification of types of research and renewed consent. Norway is a good example, introducing a full chapter on transparency and transparency in research in their Health Research Act[360]. On the other hand, Iceland provides information requirements both in its Act on Scientific Research in the Health Sector, but also to some extent its more specific Biobank Act[361].

[355] These types of registries aim to provide non-personal information and statistics as to the occurrence of particular types of the disease in defined geographical, population, age, etc. domains for epidemiology and public health purposes, as opposed to hospital-based cancer registries, mainly aiming at contributing to patient care by providing information on individuals with cancer, their treatment and the results. See, for a very comprehensive overview, dos Santos Silva, I., 1999, 'The role of cancer registries', in Cancer Epidemiology: Principles and Methods, International Agency for Research on Cancer (IARC), WHO, viewed 5 July 2021, https://publications.iarc.fr/Non-Series-Publications/Other-Non-Series-Publications/Cancer-Epidemiology-Principles-And-Methods-1999.

[356] BE, IT, BG, EE, FR.

[357] BE, EE, FI, FR, DE, EL, IT, NO.

[358] BG, EE, FI, FR, NO, PL.

[359] E.g., Norway adopted specific provisions with direct reference to transparency, but all of them include requirements relating to information to participants.

[360] Chapter 8 of the Health Research Act includes provisions on the right to access for research participants (Section 40), the public's right to access (Section 41), exceptions (Section 42), deadlines for access (Section 43) and public records (Section 44) and finally also deferred disclosure (Section 45).

[361] The Biobanks Act mainly includes information on informed consent, see e.g. Article 7 https://www.personuvernd.is/information-in-english/greinar/nr/439. An obligation to supply information to the general public on provisions of assumed consent, that the rights of individuals as per Article 13 of the Biobank Act. The Act on Scientific Research in the Health Sector provides information requirement related to consent (Articles 18-19).

4.1.2.7 Statutory confidentiality

Processing of personal data of *special categories is* in several countries subject to strict confidentiality *such as for gene research or biological material.* This is likely influenced by international instruments adopted[362].

4.2 TRENDS

This section present safeguards when implementing Article 89(1) GDPR. Trends have been identified as emerging tendencies, which are present in multiple of the 12 countries. The identified tendencies include research or data management plan, the role of the DPO, DPIA, requirements after the completion of the research and medical secrecy. Such trends were found either in general or in sectorial legislation and soft law both at EU and national level.

4.2.1 Research/Data Management Plan

At least four countries (Finland, Germany, Italy, Greece) require the purposes of the research and the management of the data - both during the research (procedures for data minimisation, access, etc.) and thereafter (storage and archiving) - to be clearly defined. In this trend, a research (management) plan is imposed[363], as well as the appointment of responsible persons for the research[364]. Such a research plan also gains importance for research in the medical domain. For clinical trials, such a detailed research plan is common and required for authorisation.

4.2.2 Role for the DPO

Many countries, more specifically, seven out of the 12 countries, require the **appointment of (and/or consultation with) a Data Protection Officer (DPO)**[365], particularly for the processing of special categories of data[366]. It is clear that a DPO can play an important and impartial role in advising the controller about the safeguards, but primarily also in assessing the risks for data subjects and balancing the competing interests[367].

---

[362] See e.g., the Oviedo Convention.

[363] E.g., Finland requires a research plan, when personal data is being processed for scientific of historical research purposes, and when derogating from the rights of data subjects of Articles 15, 16, 18 and 21 of the GDPR. See Section 31(1) of the Finnish Data Protection Act. See also Germany, where the requirement is implemented for special categories of data, when the consent of the data subjects is not obtained (Article 24 HDSIG). Italy does not specifically require a research plan, but "prerequisites and procedures to demonstrate and verify that the data are processed for appropriate statistical purposes or scientific research purposes" (Section 106 of the Italian Data Protection Act). The development of a Data Management (e.g., EL) or a "Data Protection Concept" could also be seen as part of this trend. As to the latter, the German *Bundesland* of Hesse requires a "*Datenschutzkonzept*" or a "Data Protection Concept" prior to the start of the research project, only applicable for the processing of special categories of data without consent for scientific purposes (Article 24 HDSIG). Upon request from the SA, the *Datenschutzkonzept* must be submitted. No mention to the *Datenschutzkonzept* is done at a Federal level in the BDSG.

[364] This is required in some countries. The function of this person, however, varies between the countries. In Finland e.g., derogations from certain rights of the data subject are possible, if a person who is responsible for the research has been designated (Section 31(1) of the Finnish Data Protection Act), The EE legislation requires that a person who is appointed has access to the information which allows for de-pseudonymisation (Section 6(2) of the Estonian Data Protection Act).

[365] FI: Section 6.2.3 of the Finnish Data Protection Act, NO: Section 9 of the Norwegian Data Protection Act, AT: Sections 2(d) and 5(c), DE: Article 22 BDSG, EL: Section 30 of the, BG: Section 69 Bulgarian Data Protection Act, BE: Srt. 190 and Article 204 of the Belgian Data Protection Act.

[366] In some countries, this is only required when processing personal data of special categories: FI: Section 6.2.3 of the Finnish Data Protection Axr, NO: conditional duty to consult, in case a DPIA has not been carried out, Section 9 of the NDPA, AT: DPO must be appointed for processing of special categories of personal data, Section 2.d 5.c. of the, DE: Article 22 BDSG, EL: Section 30 of the Greek Data Protection Act.

[367] The appointment of a DPO is in such cases distinct from the general GDPR requirement relating to the appointment of a DPO. In one country, we found that the appointment of a DPO is explicitly linked with the risk related to the processing of personal data for research. The DPO is in that country also required to issue opinions on the use and the effectiveness of pseudonymization and anonymization techniques: see BE: Art. 190 and 204.

4.2.3 Need for assessment or DPIA

Another trend visible in some of the countries is the need to assess the risks and **the use of a Data Protection Impact Assessment (DPIA)** as a safeguard. Some countries require a DPIA to be carried out for the processing of *special categories* of personal data[368] and/or when *derogating from the rights of data subject*[369]. In this case the researchers are responsible for balancing the competing interests. Other countries have a less direct requirement for a DPIA, but require an assessment[370], or set requirements for DPIAs for certain types of research[371].

4.2.4 Anonymisation or deletion requirement upon completion

Several countries require anonymisation or deletion of data once the research is completed or the research purpose can no longer be reached[372].

4.2.5 Medical secrecy and confidentiality for medical research

Medical secrecy is seen as a safeguard in many countries[373] for medical research.

[368] FI: Section 31(3) of the Finnish Data Protection Act, NO: Section 9 of the NDPA, if the DPO has not been consulted, BE: Section 191, in case codes of conduct have not been approved. See also DE.
[369] Section 31(3) of the Finnish Data Protection Act.
[370] BG: Article 66(2) Bulgarian Data Protection Act.
[371] IT: Section 110 of the for health data without the consent of the data subject, for medical, bio-medical or epidemiological sectors.
[372] See e.g., AT.
[373] See e.g., BE, EE, FI, IS and NO.

5 DIVERGING ELEMENTS AND IMPACT

The analysis of the available sources revealed some important diverging approaches in the countries researched. A strict division between sectorial and general GDPR implementation legislation is difficult to draw, and therefore no longer made. Section 5.1 analyses the most important divergences and variations found whereas section 5.2 discusses the impact of such diverging safeguards. Safeguards both laid out in legislation and soft law are taken into consideration.

5.1 DIVERGENCES AND VARIATIONS

5.1.1 Divergences

5.1.1.1 Constitutional protection of freedom of research

There is constitutional protection of freedom of research in Finland, as well as in some other countries, such as Italy and Germany. This implies that the freedom of research principle is of **equal importance** as the fundamental rights of individuals to data protection, and that the rights shall be balanced. Depending on the domain, this balancing is done and overseen by different bodies.

5.1.1.2 Concept and definition of scientific research

Research is differently understood, sometimes including data use for policy development (Estonia) or not. Further, there is **debate** – notwithstanding the recitals - as to whether the notion of scientific research present in Article 89(1) GDPR should depend on whether the research is only/mainly done **for the public interest/good or not** and how public interest prevails or not[374]. The issue seems to be resolved *differently in the various Member States*[375]. Further, several countries set requirements concerning the need for specific methodology as a condition. For example, Finland refer to the need to respect of general research ethical principles, whereas France does so for sector specific ethical principles. Further, for example Finland[376] and Italy[377], also refer to the need for a well described

[374] It is also debated as to whether research conducted indirectly, or directly for profit, which after all can be almost any kind of activity branded as research, should benefit from possible derogations to data subject's rights when they e.g. publish their research to the broader public, but regardless use it for their profit.

[375] EEA States have also varying definitions. See in this regard also EDPB Study on the secondary use of personal data in the context of scientific research, under Contract No EDPS/2019/02-04, 2020, pp. 45-47, with details to definitions in seven of the 12 countries researched in the present study. Further, note that according to the *Finnish* DPA, not all research can be considered scientific, and the bases for processing and the exceptions designed for scientific research are not applicable to 'non-scientific' research. The DPA points out, that the *planning and survey duties of authorities, or marketing surveys and polls are not scientific research*. Personal data may still be processed for purposes of non-scientific research, but the basis for processing cannot be the one designed for scientific research, and *derogations from the rights of data subjects* are not possible to the same extent. See Finnish DPA, Guidance available via Scientific research and data protection - Data Protection Ombudsman's Office, viewed 5 July 2021, https://tietosuoja.fi/en/scientific-research-and-data-protection. The *Estonian* legislation makes certain hints as to what constitutes scientific research, which is stated to *also include analyses and studies by executive powers for the purpose of policy development*. See Section 6(5) of the Estonian Data Protection Act. Poland implemented Article 89(1) GDPR in *the Law on Higher Education* applicable to research institutes and universities, the main endeavour of which is research that can be understood as an activity for the broadly understood public interest — regardless if it is a public or private institution. One of the criteria is that the institution meets a special number of criteria, *guaranteeing that it is not a purely commercial entity*. The Article 89(1) GDPR exceptions would therefore cover only research institutions recognised as such, which are in principle institutions not conducting research for profit. This means that private companies conducting research and trying to use Article 89(1) GDPR as a legal basis for data processing, and as a waiver for other data processing obligations, *cannot benefit from the exemptions in Poland*. This is because private companies are not subject to Law on Higher Education in Poland regulation, where Article 89(1) GDPR is implemented. See also Iceland and Norway.

[376] See Article 31.1 of the Finnish Data Protection Act, if data subject´s rights are to be derogated.

[377] See Italian Rules of conduct for the processing for statistical or scientific research purposes, published on 14 January 2019, which require, as prerequisites of the processing of personal data, a research project in which several information concerning the processing of personal data should be documented. The project is to be kept, in confidential form, for five

research plan, responsible persons, research goals as described in guidelines, such as 'informed policy' or 'increasing effectiveness'.

5.1.1.3 Specific national legislation dedicated to the processing of personal data for scientific research

Safeguards for research are ***dispersed*** in either the national GDPR implementing legislation or national specific legislation for research (e.g. Austria, France), and/or in specific national guidelines.

5.1.1.4 Safeguards for personal data versus for sensitive personal data

Almost all countries differentiate between the types of data, the main differentiation being between personal data and special categories of personal data[378]. First, it should be noted that as a general rule, the GDPR prohibits the processing of sensitive personal data[379], but it also provides exceptions to that rule: consent constitutes an exception for processing sensitive personal data[380]. Hence, consent should not be considered a safeguard, but a way of making use of the exception provided by the GDPR. This is important to note, as legislation in many countries refers to the need for explicit consent for the use of health or other sensitive data for research For example, some countries require different safeguards based on whether the personal data will be processed with or without the consent of the data subject[381].

In many countries reference to to substantial public interest is prevalent in relation to the processing of sensitive personal data, whether in a specific way or as a general reference to Article 9(2) GDPR. Further, **the requirements for the processing of personal data and personal data of special categories differ considerably**: a few countries provide *general* requirements such as *access rights' restrictions, pseudonymisation, encryption* and *designation of a DPO* and sometimes *anonymisation* for special categories of personal data (e.g., Greece) or very *detailed* requirements in legislation (e.g., Finland) or *guidelines* as to when controllers may rely on Article 9(2)(j) GDPR (e.g., in Finland, where a DPIA has to be carried out and the SA consulted if necessary)[382]. In Norway, the DPO shall be consulted for processing sensitive data, unless a DPIA is drawn up and the SA can grant permission for special categories 'for the sake of important public interests' subject to safeguards. In some countries, references to the necessity of the processing of personal data of special categories is made[383]. What they

years from the scheduled conclusion of the research but it can be consulted at any moment by data subjects (for the purpose of applying the data protection legislation).

[378] EE: Article 6(4) of the Estonian Data Protection Act , FI: Sections 6.1.7 and 6.2 of the Finnish Data Protection Act, NO: Articles 8 and 9 of the Norwegian Data Protection Act, IS: Article 11(10) of the Icelandic Data Protection Act, AT: Article 2d fog DSG, DE: Article 27 BDSG and Article 27 HDISG, IT, EL, FR: Article 44(6) of the French Data Protection Act, PL: Article 469b.2 Law on the Higher Education, and BE.

[379] Article 9(1) of the GDPR.

[380] Article 9(2)(a) of the GDPR.

[381] Such as NO: Articles 8 and 9, EL: Section 30. See also FR, IT: Section 110 of the Italian PDPC allows the processing of health data without the consent of the data subject for scientific purposes in the medical, bio-medical or epidemiological sectors, if certain conditions are met including a DPIA.

[382] Overall, Finland includes scientific, historical research and research for statistical purposes for which processing of personal data of special categories is allowed, but lists specific safeguards to be taken. See Sections 6.1 and 6.2 of the Finnish Data Protection Act: "*Such measures include: 1) measures that enable subsequent checking and verification of the identity of the person who has recorded, altered or transferred personal data; 2) measures to improve the competence of the personnel processing personal data; 3) designation of a data protection officer; 4) internal measures by the controller and the processor for preventing access to personal data; 5) pseudonymisation of personal data; 6) encryption of personal data; 7) measures that ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident; 8) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing; 9) specific rules of procedure for ensuring compliance with the Data Protection Regulation and this Act when personal data are transferred or processed for another purpose; 10) a data protection impact assessment in accordance with Article 35 of the Data Protection Regulation; 11) other technical, procedural and organisational measures.*"

[383] E.g. EL, FR and PL.

all have in common though, is the view that personal data and personal data of special categories should be treated differently.

5.1.1.5 Requirements for non-pseudonymized data

In at least four countries (AT, BE, EE, DE (federal level)) ***specific requirements for use of non-pseudonymised data are imposed.***

5.1.1.6 Biological samples and biobanking

Countries are highly diverse and regulation **very fragmented** as to the requirements and safeguards for the use of biological samples for research, research as secondary purposes and gene research[384]. Measures range from explicit consent to balancing of interests by supervisory authorities, **aggregating pseudonimised** data and defining the **type of research** for which data can be used, specific roles to **persons** appointed by the controller, the SA and the Research Ethics Committee. Some countries list *principles applicable for granting access* to samples and information, followed by more *detailed requirements for documentation* to be provided by the person requesting the access[385]. In Iceland, if important interests are at stake and potential benefits outweigh potential inconveniences of the donor or other parties, *the board of a biobank* can *authorise further use* of biological samples, *if approved* by the SA and the National Bioethics Committee[386]. Estonia further *allocates non-transferable ownership of the samples to the tissue databank owner* (*and upon termination of activities to the Republic*) and describes in legislation the specific use rights for specific purposes[387].

5.1.1.7 Detailed safeguarding methodologies and self-certification of compliance

The need for supervision and authorisation by the SA for research in the health sector and for medical research has been simplified in France, whereby the SA is issuing specific guidelines, which researchers need to follow, depending on the sources of the data and the use and re-use, and whereby researchers need to **self-certify that they abide by these requirements**, in order to be **exempted** of any

[384] See also Tzortzatou, O., Slokenberga, S., Reichel, J., da Costa Andrade, A., Barbosa, C., Bekaert, S., van Veen, E.-B., Romeo-Casabona, C., Ó Cathaoir, K., Chassang, G., Debucquoy, A., Derèze, J.-J., Dollé, L., Eaker Fält, S., Halouzka, R., Hartlev, M., Hisbergues, M., Hoppe, N., Huys, I., Kindt, E., Kjersti Befring, A., Kozera, L., Krekora-Zajac, D., Lalova, T., Mayrhofer, M., Negrouk, A., Pawlikowski, J., Penasa, J., Pormeister, K., Rial-Sebbag, E., Siapka, A., Southerington, T., Stenbeck, M., Šutalo, M., Tomasi, M., Valcke, P., and Vella Falzon, R., 'Biobanking Across Europe Post-GDPR: A Deliberately Fragmented Landscape', in Slokenberga, S., Tzortzatou, O., and Reichel, J., (ed.), GDPR and Biobanking. Individual Rights, Public Interest and Research Regulation across Europe, Springer, Law, Governance and Technology Series, 2021, pp. 397-420.

[385] FI: Section 26 of the Biobank Act: (i) the intended use must correspond to the research area defined for the biobank and the criteria and conditions established for the processing of the sample; (ii) terms and restrictions provided by law and determined by the biobank are observed in the research and in the processing of samples and information; (iii) the individual granted access to the samples or information holds the appropriate professional and academic qualifications for processing the samples and information, and the granting of access to the sample or information is in connection with the duties of the recipient. Requirements also exist concerning the coding used; Section 27 requires a research plan, a statement by the competent ethics committee (as referred in the Medical Research Act), or a statement necessary to assess the fulfilment of the conditions. Restrictions of access is only allowed only if justified and fulfilling requirements in Section 27. Further, a written agreement is required.

[386] Article 9(4) of the Icelandic Act on Biobanks. The access is subject to permissions by the SA and a research protocol approved by the National Bioethics Committee (or relevant ethics committee).

[387] See EE: Human Genes Research Act, 8.1.2001, https://www.riigiteataja.ee/en/eli/508042019001/consolide. Article 15 on the right of ownership of tissue samples and right to use descriptions of state of health genealogies and personal data connected therewith means that: (i) the controller's right of ownership of a tissue sample is created from the moment the tissue sample is taken. The controller's right to use the description of state of health, genealogy and written consent of a gene donor and the right to process the personal data contained therein is created at the moment of preparation thereof; (ii) tissue samples in the ownership of the **controller are not transferable**. Upon termination of activity of the controller, the right of ownership of tissue samples, descriptions of state of health, genealogy and written consents of gene donors in the possession of the controller and the right to process the personal data connected therewith shall transfer to the Republic of Estonia.

authorisation requirement (see also Annex 2).

5.1.1.8 Increasing rights of data subjects for transparency, information and deletion

In many countries, information and transparency to data subjects are emphasised. Also, the withdrawal of the consent is explicitly mentioned and repeated. In some countries, data subjects are entitled to request deletion of information provided, including e.g., biological samples. These rights could be considered as safeguarding the interests and rights of data subjects as well, and could be envisaged to further strengthen. On the other hand, some countries also link reduced rights to increased other safeguards.

5.1.2 Variations

5.1.2.1 General or detailed approach

One important variation, is the way the studied countries approach the safeguards foreseen in Article 89(1) GDPR[388]. The GDPR specifically mentions technical and organisational measures, and in particular those ensuring respect for the principle of data minimisation, pseudonymisation and anonymisation. Whereas some of the countries have adopted an approach in their national legislation by simply referring to Article 89(1) GDPR[389], others have adopted specific law for research[390] or issued extensive general data protection schemes, with or without specifically mentioning safeguards for scientific research[391]. Others have adopted a number of safeguards with a high degree of granularity[392].

5.1.2.2 Risk assessment and balancing: by the legislator, supervising /ethics authority and/or researchers

In general, and in sectors alike, risk assessments of the use of personal data for research are done in varying ways. In the more 'traditional' research sectors, such as statistics but also in archives, an initial risk assessment has already been done by the national legislator[393]. In other sectors and countries, the requirement for researchers to carry out a DPIA is imposed as a safeguard implying a proper assessment and balance, also as to involving the SA or not. Lastly, especially in the health research, clinical trial and biobank sector, many countries have adopted legislation requiring the assessment and/or approval

[388] Article 89(1) of the GDPR mentions "*appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject*", technical and organisational measures "*in particular in order to ensure respect for the principle of data minimisation*" and "*those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner*."

[389] Such as NO: Section 9(1) of the Norwegian Data Protection Act and IS: Article 18(1) of the Icelandic Data Protection Act.

[390] E.g. AT.

[391] Such as EE.

[392] Such as the safeguards by Belgium for the disclosure of personal data. Belgium provides for the most stringent safeguards for the disclosure of data in scientific research contexts. As such, it imposes a greater onerousness on the controller who discloses data to a third party, as it requires it to prevent the reproducibility of the disclosed data by the third party in cases where (i) it concerns sensitive data or data relating to criminal convictions and offences; or (ii) the agreement between controllers forbids it; or (iii) any such reproduction may compromise the safety of the data subject. According to Article 208 of the BDPA, this obligation of the initial controller does not apply when the data subject has given his consent; the data were made public by the data subject; the data are closely linked to the public or historical nature of the data subject; or the data are closely linked to the public or historical nature of facts in which the data subject was involved.

[393] For e.g., statistics, by imposing confidentiality, anonymisation of the data, etc. in legislation. In a few countries, such safeguards are extended in as far that a national authority collects, anonymises and is responsible for holding the databases and in some cases also facilitates further processing, such as the authority of Findata in Finland, and similar arrangements in NO and IS.

by SAs/competent authorities[394] and/or an ethics committee[395].

5.1.2.3 Varying importance attached to public interest depending on the countries and the sectors

Some countries stress the importance of the public interest in research, which may outweigh the interests of individuals[396].

5.1.2.4 Important but varying roles for central research authorities

An interesting approach, adopted in a few (mainly Nordic) countries is the **prominent role of a central authority**, sometimes also a "one-stop-shop" for overseeing the use of (e.g., social and health) data for scientific research purposes. In Finland, the authority Findata is a licensing authority, promoting the secondary use of health and social data, facilitating data permit processes and working to improve the data protection for individuals[397]. In Norway, the Norwegian Centre for Research Data facilitates sharing and reuse of data, gives advice on data management and data protection in research[398]. A similar centre is established in Iceland (see above). For specific *sectors*, like biobanks, such (public) authorities also have a crucial role while their competences vary. In other countries[399], public authorities are also often involved depending on the sector, while their role is more limited.

5.1.2.5 Public dissemination requirement

Only a few countries **require the publication of the research as a requirement**[400]. This could include making the result of the research publicly available on the internet, including information on the legal basis used.

5.1.2.6 Technical and organizational measures for destruction/deletion

Only a few countries adopt detailed measures related to the **deletion or destruction of the personal data after the withdrawal of (the consent by) a data subject** (e.g., for biological samples/biobanks) or after **expiration** of the research purpose[401].

5.1.2.7 Sector specific identifiers for research

Austria is one of the few countries which explicitly chooses for and mandates to use independent *area-**specific identifiers***, which may be attached to research material in machine-readable form for protecting personal data[402]. Such identifiers shall differ from any other general identifier, e.g., identifiers used for civil identification purposes.

---

[394] Mainly in biobanking and clinical trials legislation.
[395] In several countries (e.g., BE, EE, FI, FR, DE) **ethics committees** are given an important role for approving research, especially if sensitive data are processed. In Norway, the Ethics Committees have also provided guidelines for privacy. IT: Section 110 of the Italian PDPC allows the processing of health data without the consent of the data subject for scientific purposes in the medical, bio-medical or epidemiological sectors, if certain conditions are met, including a DPIA and the positive and reasoned assessment of the research project by the competent ethics committee.
[396] E.g., NO.
[397] See https://findata.fi/en/, viewed 3 June 2021.
[398] See https://www.nsd.no/en/about-nsd-norwegian-centre-for-research-data/, viewed 5 July 2021.
[399] E.g., FR, DE.
[400] E.g., AT.
[401] FI: not directly included in the text of the Finnish Data Protection Act, but referred to in the guidance of the SA, viewed 3 June 2021, https://tietosuoja.fi/en/destruction-anonymisation-or-archiving-of-data. AT directly implement such requirements in Article 7 DSG and DE. NO and IS solely refer to the measures foreseen in Article 89(1) GDPR. https://tietosuoja.fi/en/destruction-anonymisation-or-archiving-of-data.
[402] Section 9 E GovG.

5.1.2.8 Varying references to ethical principles and roles of ethical committees for scientific research

While scientific research should be governed by an ethical framework[403], a lack of pronouncement by the EEA States as to the intersection of the data protection framework and the corresponding ethical standards governing scientific research was identified. Few mention the need for respect for ethical standards in the national law as a requirement for processing data for scientific research purposes. France has positivised a duty for personnel accessing and modifying data resulting from scientific research to respect the rules of ethics applicable to the sectors of activity in which the scientific research is being conducted as an additional measure to ensure confidentiality[404]. In various countries, ethical committees are involved at the same time[405].

5.1.2.9 Transmission, disclosure and/or transfer of the research data

The GDPR requires controllers and processors to evaluate the risks inherent to the processing of personal data. In assessing those risks, consideration should be given, among others, to the unauthorised disclosure of personal data. From the countries analysed, Italy recognises the necessity of establishing said safeguards for the data exchanges for scientific research purposes that *"are carried out with entities and agencies abroad"*[406]. Disclosures of data for scientific research are recognised in several jurisdictions requiring, however, **different specific technical and organisational measures**[407].

Divergence further exists as to specific rules for personal data ***not to be revealed*** *to outsiders* (e.g., Finland), countries with specific rules (whether in legislation or guidelines) ***for archiving*** research results/data (e.g., France, has detailed guidelines) or ***pooling*** data and knowledge (e.g., with a specific public authority, e.g., Norway) or ***when contracts*** need to be concluded (e.g., Belgium, France).

5.1.2.10 Biobanks: Governance, agreements, consent, transparency and involvement of governmental bodies

The sectoral legislation contains a wide area of approaches with regard to safeguards for biobanking and genetic research[408].

5.2 IMPACT

While the objective of the GDPR is to harmonise the level of personal data protection all over the EU, the many domains of national competences as to how to regulate detailed issues render *the legal*

[403] European Data Protection Supervisor, 6 January 2020, A Preliminary Opinion on data protection and scientific research, viewed 5 July 2021, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
[404] Article 116 of the Decree No 2019-536 of May 29, 2019.
[405] E.g., BE, EE, FR, IT.
[406] Article 106(2)(h) of the Italian Personal Data Protection Code.
[407] For instance, EE, FI and BE expressly recognise the legitimate disclosure of data for said purposes if certain safeguards are met, *i.e.* FI allows the disclosure of data as long as it is not "revealed to outsiders" (see Article 31(3) Finnish Data Protection Act). See also EE and BE, if data is being pseudonymised or rendered in a format which provides equivalent levels of protection (Article 6(1) of the Estonian Data Protection Act and Article 207 of the Belgian Data Protection Act).
[408] E.g., AT stresses encryption, deletion of identifiers after conversion, separate storage of additional data, anonymisation of data accessed by third parties, access control mechanisms, data availability, documentation on access to data (logs) and security management procedures (Articles 15a.6, 7 and 10 of the Austrian Data Protection Act) while the Belgian HBM Act imposes a written agreement on the topic of the research, traceability, organisation and technical measures when transmitting personal data, a coded copy of donor's consent and the advisory role of FAMHP (Belgian HBM Act). In EE, legislation creates gene banks, stressing the composition of data, the rights and duties of genes' donors, restrictions on the use of data, conditions for generic research, restriction of use of the bank, pseudonymisation by a third party, the SA's role and the REC's role , while IS states that no public access is possible without the data subject's consent. In NO, there is for treatment biobanks a national registry, one person responsible by biobank (or a board of directors) with medical or biological education of higher degree and in case access to the biobank is rejected, appeal possible by the Ministry.

landscape fragmented. Safeguards applicable to personal data used for scientific research are a good example[409]. While Article 89(1) GDPR is to be generally applied all over the EU, there remain numerous divergences as mentioned in this study, which *may negatively impact the ability to conduct cross-border research, and research in general.*

This is especially apparent where the requirements for the processing of *sensitive personal data* diverge across the EU, but also may *differ depending on the sector and goal of the research*. This type of data is of particular relevance in important health-related research, aiming at improving health care, developing medicines, researching diseases, a pandemic, etc. not only of benefit to individuals but also the population at large. It further means *inter alia* that *cross-border research projects need to fulfill potentially numerous different requirements for each Member State* if data are used by various controllers in different EEA States for the same project.

Moreover, the notion of research itself is understood differently across the EU, while different legal basis may be required depending on whether the research meets certain methodology and publication requirements. The divergences also impact the rights of data subjects in different ways[410]. Another issue is that the different understandings of *the notion of public interest* which is often evoked as a justification for the re-use of personal data for the purpose of research. In the case of cross-border research, these varying views are problematic as well. It also remains uncertain how *SAs, administrative authorities and courts* in each EEA State decide and adjudicate on whether (substantial) public interest justification could be evoked, which is especially problematic in case of cross-border research and which would require distinct assessments which are difficult in case of limited (explicit) guidelines for a proper understanding, assessment and for balancing the conflicting rights. Therefore, some guidance towards finding a common understanding would be important.

Most impact of the variations in safeguards appear in particular domains governed by *sectoral regulation*. Biological samples and gene research are a primary example of the fragmented legal landscape[411], while being an emerging and very important research domain, also for public health and policy purposes[412]. SA and ethical committees are also involved to different degrees, all rendering such research and *especially (international) cooperation* increasingly burdensome. All those divergences mean that the *compliance burden for conducting cross-border research is multiplied by the number of the EEA States of which citizen's personal data are gathered* and *used*. Varying safeguards therefore risks becoming a disincentive to use personal data for the purpose of research *in cooperation* with institutions from other EEA States. Finally, a lot will also depend on the (level of) guidance and activity of national SAs as to whether a comprehensive understanding and compliance is possible.

[409] See also Pormeister, K., 2018, 'Genetic research and applicable law: the intra-EU conflict of laws as a regulatory challenge to cross-border genetic research', Journal of Law and the Biosciences, vol. 5, no. 3, pp. 706–723, viewed 5 July 2021, https://doi-org.kuleuven.ezproxy.kuleuven.be/10.1093/jlb/lsy023.

[410] For example, if a university in Poland or Finland would like to do research with a company from France or Belgium, the collection and the use of personal data of data subjects from Poland and Finland for research purposes by these companies may be subject to varying derogations and safeguards as required by Article 89(1).

[411] Pormeister, K., 2018, 'Genetic research and applicable law: the intra-EU conflict of laws as a regulatory challenge to cross-border genetic research', Journal of Law and the Biosciences, vol. 5, no. 3, pp. 706–723, viewed 5 July 2021, https://doi-org.kuleuven.ezproxy.kuleuven.be/10.1093/jlb/lsy023.

[412] The divergences range i.e., from whether EEA States apply broader, informed consent as a safeguard or to situations where consent is not needed, to situations for which particular rights derogations are provided in implementing laws in each Member State.

6 AVENUES AND POLICY RECOMMENDATIONS

6.1 GENERAL RECOMMENDATIONS

In general, and due to the high divergence of safeguards required on many aspects of research as presented in this study, **EEA States should reassess the appropriate safeguards** imposed by their national legislation in order to comply with the GDPR data protection requirements (Article 89(1) GDPR) in the field of scientific research in light of the results from this study. EEA States shall take into account that **the more risks research poses** (e.g., in the health domain), the **more strict safeguards in a detailed legal framework** (e.g. specific legal provisions) are required, while in less risky situations (e.g., when used for statistical purposes), more general requirements may be sufficient.

In addition:

- There is no uniformity in EEA States' approaches as to what **shall be understood by 'scientific research'**. Overall, it remains important to have a common understanding of 'scientific research'[413]. As scientific research is no longer isolated in one country, but increasingly cross border and international, such a **common understanding** should be reached, for example by defining common methodologies, aims and purposes.
- **Increased dialogue** between EEA States' SAs, European Institutions and competent bodies, key stakeholders and the larger public (citizens) is recommended on all relevant issues including the concept of scientific research, the assessment of the risks and the balances between the public interest in research and the rights of the data subjects .
- EEA States should reassess the sectoral appropriate safeguards imposed by their national legislation in order to comply with data protection rules in the field of scientific research regarding specific processing of personal data such as **genetic data, biobanks, personal data related to health**, etc. which especially demonstrate many variations as demonstrated in this study. SAs could discuss and agree upon common guidelines for each of these specific domains, types of research (primary vs secondary) and depending on the phase of the cycle of the research (collection, use, dissemination, etc.) based upon typical approaches and examples of some EEA States.
- As a preliminary measure, a dialogue should be started with the relevant stakeholders in each domain, i.e., society, research entities and governments alike, **for mapping the needs and goals** of each domain in a coherent way, and seems inevitable.

6.2 SPECIFIC RECOMMENDATIONS

Furthermore, specific recommendations can be made. The next two tables provide suggestions for reaching more consistency in terms of safeguards needed for personal data use for scientific research which could be developed in future EDPB guidelines or documents. These recommendations are based on the findings of this study, and indicate whether they are based upon convergences or trends. In just a few cases, the recommendations are based on an important need for clarification. They are also broadly divided in recommendations for research in general and for specific sectors.

[413] For different concepts and definitions, see above, as well as EDPB Study on the secondary use of personal data in the context of scientific research, under Contract No EDPS/2019/02-04, 2020.

Table 1: Recommendation for safeguards for personal data use for scientific research in general

No	Summary	Convergence / trend or important need	Findings	Recommendations
1.	**Pseudonymisation** and **Anonymisation**	Convergence / trend	Pseudonymisation and anonymisation measures are broadly required in 10 to 11 countries.	Legislation shall impose **pseudonymisation** and **anonymisation requirements, and** specify **when** there is a need for pseudonymous data and anonymous data (e.g., also upon the end of the research project, for disclosure to third parties, transfer, publication), and whether or not there is a **specific order to follow** (e.g., 'waterfall system'), both in general and for specific sectors (e.g., anonymous data for statistics). Legislation complemented with appropriate guidelines shall also impose **how to reach this** as such (e.g., need of designated person, trusted third party or not, advice of DPO, access to pseudonymisation keys, etc).
2.	**Sensitive and non-sensitive data**	Important need	Sensitive and non-sensitive data should be treated differently as they pose different risks and receive different safeguards in many countries.	Legislation should clearly distinguish and provide detailed requirements for safeguards for sensitive data in general and in specific domains.
3.	**Technical and organisational measures**	Convergence	Converging required *technical* measures include confidentiality, access control procedures and access logging in at least 10 of the 12 countries, and restricted areas, as well as encryption. The monitoring of *organisational* measures is required in more than 8 of the 12 countries, while a confidentiality obligation is imposed upon personnel. At least 11 countries also require that personnel undergo proper training.	General (i) technical and (ii) organisational measures shall be imposed, including (i) **confidentiality, access control procedures** and **access logging**, and **restricted areas**, as well as **encryption** and (ii) a **confidentiality obligation imposed upon personnel, training** and the **monitoring** of such measures.
4.	**Research and data management plan**	Trend	In at least four countries, a detailed research / data management plan is required, either by law or national guidelines.	Submission of a detailed **research and personal data management plan** as a safeguard could be required for scientific research's use, including before re-use or access to the data.
5.	**Guidelines for scientific research in higher education,**	Convergence	In at least eight countries practices and/or rules of conduct were established for (funded) research by	Need for the establishment of **guidelines, practices and/or rules of conduct** for scientific research by national scientific

No	Summary	Convergence / trend or important need	Findings	Recommendations
	national research centers and other academic establishments		national scientific research centres, higher education and academic establishments.	research centres, higher education and academic establishments.
6.	**Guidelines for publication and dissemination**	Convergence	At least eight countries agree that personal data intended for publication or dissemination should undergo a technical process to prevent or hinder the identification of the data subject, and impose technical measures, in particular pseudonymisation and/or anonymisation.	Personal data for **publication and/or dissemination should prevent the identification** of the data subject, in particular by proper pseudonymisation and/or anonymisation.
7.	**Security for protecting the data**	Convergence	In 10 out of 12 countries, roles and responsibilities for security purposes are to be defined while conducting scientific research.	Specification and adoption of security management measures fit for guaranteeing the least intrusion when using the data for research.

Table 2: Recommendations for safeguards for personal data use for scientific research in specific *sectors*

No	Summary	Convergence / trend or need	Findings	Recommendations
	IN GENERAL			
1.	**Role of SA and ethical committees**	Convergence	Eight of the 12 countries give **an important role to the SAs**[414] for the supervision of research as a safeguard. This role is at the same time also *often completed with a role for the ethical committees* (five of the 12 countries).	Clarification of the distinct **role to the SAs and** the **ethical committees** for reviewing and/or authorising research as a safeguard for the assessment of the risks in specific situations[415] or if data are obtained from government databases or when 'sensitive' data is processed or if data are processed without consent.
2.	**Involvement of a DPO**	Trend	In at least five countries, **appointing (and/or consulting) a DPO** is required for sensitive data and assessing the risks.	**The need for the appointing (and/or consulting) of a DPO**.
3.	**Need for DPIA or assessment**	Trend	In at least four countries, use of **a DPIA or assessment** is imposed for	**The need for a DPIA or other type of assessment.**

[414] EE, FI, NO, AT, DE, IT, FR, BE.
[415] E.g. when research is conducted for policy development by government (see e.g. EE).

No	Summary	Convergence / trend or need	Findings	Recommendations
			sensitive data and assessing the risks.	
	SECTOR SPECIFIC			
4.	**Statistics and population based registries: specific laws with ample safeguards**	Convergence	In several countries, law imposes the safeguards when processed for registries or for statistical purposes such as statutory confidentiality, separate storage and preference or obligation for anonymous data, often supervised by special institutes with specific competences for mitigating risks.	The adoption of a **law** regulating the safeguards for the use for statistical purposes, including (the procedures and responsibilities) for anonymisation.
5.	**Medical domain**	Convergence	In at least six countries, **transparency** towards participants is considered a safeguard. The more significant the data (e.g., genetic data, biological material) used and/or shared for scientific research, **the more detailed the transparency information becomes** (e.g., with specification of types of research and renewed consent and even a right to delete).	Guidelines detailing the **transparency and information requirements** for specific (sensitive) data and their scientific research use in the (bio)medical domain.
6.	**Medical domain**	Divergence	Ethical committees have a varying role in countries. Their involvement in research, especially concerning medical data, should be further specified.	Guidelines for the specification of **the role of ethical committees** in scientific research.
7.	**Biobanks: Specification of research, legal basis, safeguards and role of SA and ethics committees in law**	Emerging trend	In at least three countries, law regulates the legal basis, separate storage and specific (secondary) research, outlining safeguards, and the role of the SA and the Research Ethics Committee.	Guidelines for the adoption of **law** regulating the safeguards, including the legal basis, specific (secondary) research and separate storage while outlining the separate role of a SA and the Ethics Committees.

7 CONCLUSION

The countries which were subject of this study all include specific requirements for scientific research as safeguards for the data subject as part of their data protection framework. While some simply evoke Article 89(1) GDPR as a sole description of applicable safeguards, without providing further details, others regulate them – sometimes in specific laws dedicated to research and data protection - in significant detail.

Taken as a whole, *the overall types of safeguards are similar*, such as required data anonymisation, pseudonymisation as data minimisation measures, technical and organisational measures, including access control and the appointment of responsible persons for the research, as well as security management, and distinct requirements for special categories of personal data, which are all important converging safeguards used in the various EEA States. For specific domains, SAs and ethics committees have an important role in the majority of the countries, higher education institutions receive detailed guidance, and transparency increases depending on the nature of the data and the level of risks to the data subjects, just to name a few. At the same time, *numerous differences exist in the more detailed requirements* which could impact the level of protection, such as varying or strict interpretations of the concept of scientific research, the importance attached to public interest, and consent requirements. One could hence conclude that while EEA-wide the States studied globally have similar approaches, the complication is in *the details of the safeguards, which vary extensively both in detail as in granularity and protection*. The question which arises is hence whether the harmonisation efforts should focus on streamlining the overall types of safeguards, which may seem to be within reach, or rather on the detailed requirements, which could be seen as where harmonisation is most lacking and would be welcomed. This is a policy decision. Such further harmonisation and consistency endeavours, however, are much needed given that the differing levels and modes of protection create additional burdens for research in general, including (increasingly important) cross-border research.

We maintain further that – while there might be some debate in some EEA States - EEA States *shall adopt national law* - as understood in the fundamental rights context - specifying the safeguards when personal data is used for scientific research for rendering the freedoms and the rights of data subjects more secure.

Furthermore, one shall note that Article 89(1) GDPR covers a wide variety of scientific research domains, while the sources and types of the (re)use of personal data are very different and the purposes and aims of the research are ***very diverse.*** We found, based upon our analysis, that the safeguards are sometimes therefore very specific and contend that the safeguards should be adapted to each domain and each specific type of scientific research. Because of the diverse aims of the distinct 'scientific research' categories, the *safeguards to be effective should hence always be developed and be seen against the needs and characteristics of each of the scientific research purposes processing operations.* A dialogue with stakeholders for each domain, i.e., society, research entities and governments alike, for mapping these needs in a coherent way, seems inevitable. This should also include the source of the data (e.g., from data kept by the government) or whether research is done with the data as a primary or secondary purpose.

A last open question when designing the guidelines is whether the common denominator should be the most stringent and demanding requirements and safeguards for personal data, or those demanding less. The first option will surely leverage the level playing field to a higher level of protection while risking a chilling effect on research with personal data. The less demanding option creates risks for privacy, data protection rights and freedoms while incentivising research. At the same time sensitivities and traditions of states should also be respected. Especially where there already exists a mature level and consensus about the protection of personal data in the context of research. Nevertheless, creating unified rules should be an objective in itself. This in order to foster cross-border, but also more privacy and data protection-friendly research, will contribute to building a better Single Market and society.

ANNEX 1 - ACRONYMS AND ABBREVIATIONS

Country abbreviations:

Abbreviation	Member State
AT	Austria
BE	Belgium
BG	Bulgaria
DE	Germany
EE	Estonia
EL	Greece
FI	Finland
FR	France
IS	Iceland
IT	Italy
NO	Norway
PL	Poland

Other:

Acronym or abbreviation	Explanation
BBMRI	BioMolecular Research Infrasttructure
BCR	Belgian Cancer Registry
BDSG	German Federal Data Protection Act
BVefG	German Federal Constitutional Court
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale De l'Informatique et des Libertés (French SA)
CNRS	Centre National de la Recherche Scientifique
CT	Clinical Trial(s)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSG	Austrian Data Protection Act
EAG	European Archives Group
EC	Ethical Committee
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ENCR	European Network for Cancer
EU	European Union
FAMHP	(Belgian) Federal Agency for Medicine and Health Products
FOG	Austrian Research Organisation Act
GDPR	General Data Protection Regulation
GOGG	Austrian Health GmBH
GTelG	Austrian Health Telematics Act
HBM	Human Body Material
HER	Electronic Health Records
HOSIG	Hessian Data Protection Act
HRA	Norwegian Health Research Act
MII	Medical Informatics Initiative
NCPHA	National Centre of Public Health and Analysis
NCSS	National Center for Social Solidarity
NSD	Norwegian Centre for Research Data
OSA	Official Statistics Act

Acronym or abbreviation	Explanation
PDSP	Personal Data Protection Code
RE	Research Ethics
SA(s)	Supervisory Authority(-ies) as mentioned in the GDPR
SGB	Social Security Code

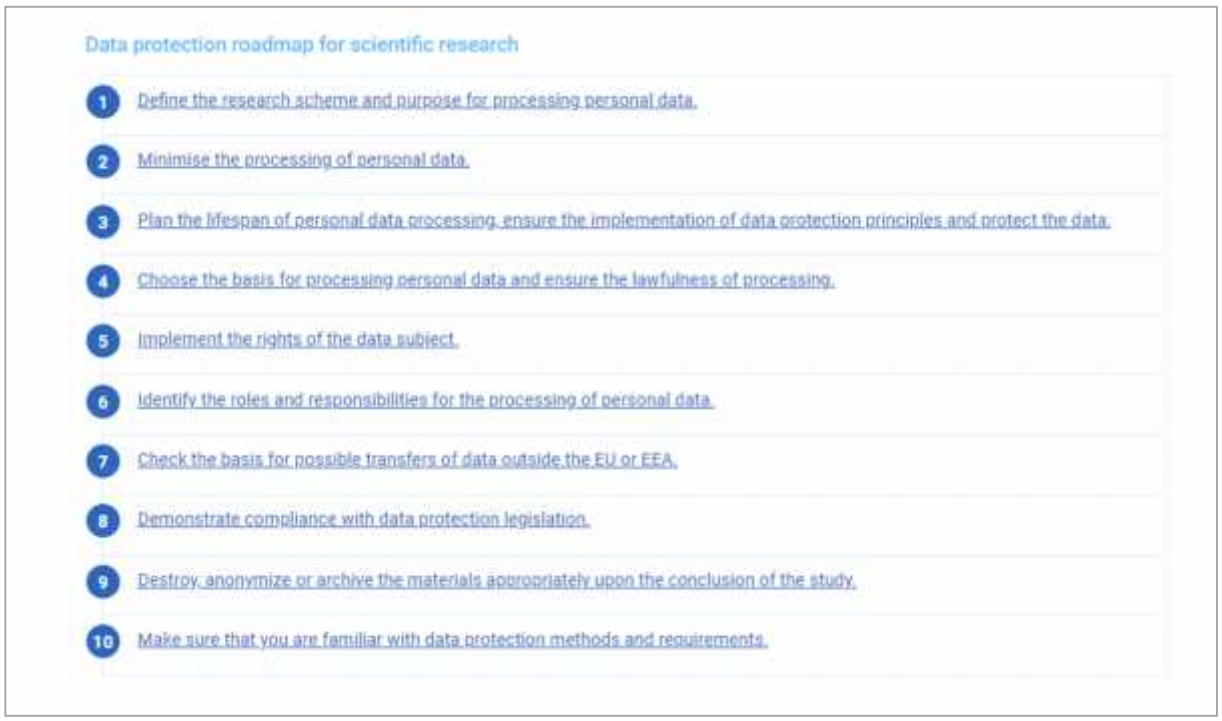
ANNEX 2 – EXAMPLES OF DETAILED GUIDELINES - FINLAND AND FRANCE

This Annex contains examples of detailed guidelines and requirements for research, issued in Finland and France for scientific research. Whereas the guidelines in Finland are for *research in general*, the 'methodology' set out in France by the SA is *for health and medical research*.

Finland

The Data Protection Ombudsman draws up a data protection roadmap for the scientific research, with the purpose of guiding controllers when considering the data protection aspects of the research phases and lifespan of data. Please see Figure 1 below.

Figure 1: Data protection roadmap for scientific research



Source: Finnish Data Protection Ombudsman

Under each of the topics of the roadmap, more detailed guidelines are provided.

Purpose limitation

Starting with the requirements of *purpose limitation*, the Data Protection Ombudsman notes that the purpose of the scientific research is normally specified in the research plan.

Consent and the quality thereof are closely connected to the principle of purpose limitation. When it comes to the use of consent as the basis for the processing of personal data, the Data Protection Ombudsman observes that some flexibility might be needed for the sake of the research. The Data Protection Ombudsman provides three ways of specifying consent. First, if the purpose of the study cannot be fully specified at the start of the study, it is possible to benefit from a *more general consent* for the purpose of the research. As the study develops, *consent for later phases* of the research can be obtained. Second, transparent communication is key. In order to obtain any specific consent during the phases of the study, the controller should update the data subject regularly on the developments of the

research. Third, drafting a comprehensive research plan[416] which is available to the data subject can also help in a situation where it is not possible to identify the detailed purposes.

The Data Protection Ombudsman provides some specification on the content of the research plan. The research plan should *specify the research scheme*, the intended research *questions, material, methods and which data* are needed for the research and why the data are needed for answering the research questions. Also, the research plan should specify whether the research concerns a cross-sectional study or a follow-up study, which could render the processing of the data necessary for a longer time. The research plan will also need to be available to the data subject before consent is given.

Data minimisation

As for *safeguards*, the Data Protection Ombudsman highlights the need for **data minimisation**[417]. The necessary data to be processed for the research should be assessed at the earliest possible stage, taking into account both the amount and the nature of the personal data processed and aiming for processing as little data as possible. Therefore, the processing of personal data should always be avoided when possible. In practice, such an approach needs to be based on clearly defined research questions, from which the need for (the minimum amount of) processing personal data can be derived[418]. The need of minimisation does also apply to the storage time of personal data.

Anonymisation and pseudonymisation

In this context, **anonymisation** is important. The Data Protection Ombudsman stresses, that the un-identifiability must be permanent, and it cannot be possible for the controller or a third party to convert the data into information that can be used for identifying the data subject. Further, **pseudonymisation** is pointed out as often used for scientific research, and carried out immediately after the collection of the data. Encoding of personal data and false names are mentioned as examples of pseudonymisation techniques. Additionally, the Data Protection Ombudsman identifies the elimination of directly identifying information (names, personal identity codes) from the material for the purpose of data minimisation.

Risk assessment and safeguards

Further, the Data Protection Ombudsman also refers to the data protection principles of the GDPR[419]. The guidelines of the Data Protection Ombudsman are based on a **risk assessment** approach. Accordingly,

> "*Technical and organisational safeguards are particularly important for protecting personal data in the context of scientific research. The controller must always asses the risk posed by the processing of personal data to the data subjects and implement safeguards in proportion to the risk. Identifying the necessary safeguards requires defining the environment in which the research material will be processed in practice (e.g. the technical platform, premises, data transfers) and the personnel processing it (controller, joint controllers, processors, researchers and other staff).*"[420]

[416] "*or other clear and detailed description of the study available to the data subjects*", as per the wording of the Data Protection Ombudsman, viewed 23 March 2021, https://tietosuoja.fi/en/defining-the-research-scheme-and-purpose-for-processing-personal-data.
[417] Webpage of the Data Protection Ombudsman, viewed 23 March 2021, https://tietosuoja.fi/en/minimisation-of-personal-data.
[418] Webpage of the Data Protection Ombudsman, viewed 23 March 2021, https://tietosuoja.fi/en/lifespan-of-personal-data-processing-data-protection-principles-and-the-protection-of-data.
[419] Idem.
[420] Idem.

Additionally, the Data Protection Ombudsman also sets out the particular points which the risk assessment shall address. These are the following:

- the nature of processing (e.g. special categories of personal data, personal identity codes and data subject to non-disclosure for personal safety reasons);
- the scope (e.g. number of data subjects and storage time);
- the context (e.g. the vulnerable position of the data subject and confidentiality); and
- the purposes of the processing (e.g. will the data be used in decision-making or will the processing have other judicial effects).

Based on this, the risks involved should be identified and as a next step, the severity and likelihood of each risk and potential resulting damage should be evaluated. Based on the level of risk, the data controller should assign the safeguards to mitigate the risks. The risks identified by the Finnish SA are the following (but not limited thereto):

- minor (e.g. waste of time or momentary annoyance);
- limited (e.g. a feeling of invaded privacy with no permanent damage);
- significant (e.g. a feeling that one's fundamental rights have been violated, such as feeling discriminated, or serious psychological damage such as depression or phobias); or
- high (e.g. long-term or permanent physical or psychological damage or rupture of family ties).

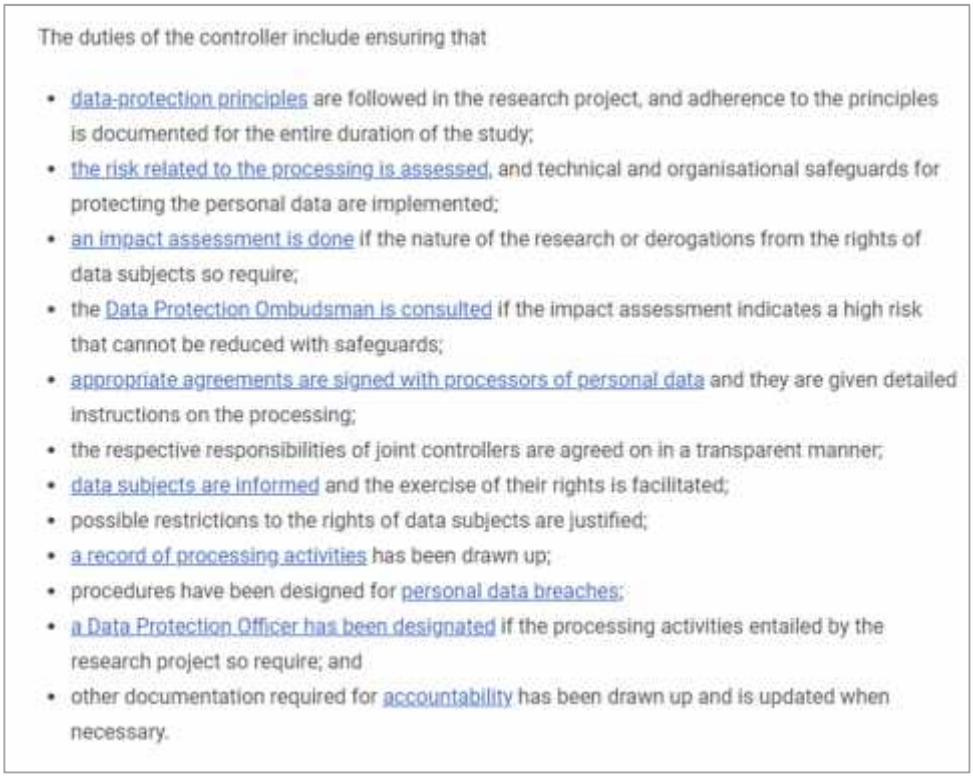
Designing the safeguards, it should be noted that the higher the risk, the more comprehensive the safeguards should be. In this assessment, the safeguards should address both internal threats (identified as threats caused by their own personnel, processors, processing devices or environments) and external threats (such as unauthorised access to research materials). The format of the research materials also influences which safeguards are considered appropriate, such as paper questionnaires or physical tissue samples. Examples of safeguards are divided into technical and organisational safeguards[421].

Technical	Organisational
Firewalls	Restricting access to material limited by duty (both data controllers and processors)
Anti-virus software	Data protection instructions for personnel
Encrypted connections for data transfer	Data protection training for personnel
Collection and monitoring of log data	Designation of a data protection officer
Retrospectively collect log data to investigate suspected violations	NDAs
Anonymisation (as defined by WP29)	Regular testing and evaluation of the efficiency of technical and organisational measures
Pseudonymisation	Special procedural regulations designed to ensure compliance with data protection regulations when transferring personal data or changing the purpose of processing
Encryption of personal data	Performing a data protection impact assessment provided for in Article 35 of the GDPR
Measures guaranteeing the constant reliability, integrity, availability and fault tolerance (including the ability to restore data availability and access to them in the event of a physical or technical fault) of the processing systems and services related to the processing	Ensuring lawfulness in other respects (e.g. taking into considerations specific legislation applying to data processing in certain fields, such as medical research)

[421] The listed safeguards have been compiled from the following webpages: https://tietosuoja.fi/en/choosing-the-processing-basis-and-ensuring-its-lawfulness, https://tietosuoja.fi/en/lifespan-of-personal-data-processing-data-protection-principles-and-the-protection-of-data and divided into technical and organisational by the researcher. Both sites viewed on 23 March 2021.

Finally, it can also be mentioned that the Finnish Data Protection Ombudsman has also listed the duties especially of the controller, while highlighting the need *to define the responsibilities of different data processing partners* (data controller and processors, sub-processors)[422].

Figure 2: Extensive list of the duties of controllers for scientific research


The duties of the controller include ensuring that

- data-protection principles are followed in the research project, and adherence to the principles is documented for the entire duration of the study;
- the risk related to the processing is assessed, and technical and organisational safeguards for protecting the personal data are implemented;
- an impact assessment is done if the nature of the research or derogations from the rights of data subjects so require;
- the Data Protection Ombudsman is consulted if the impact assessment indicates a high risk that cannot be reduced with safeguards;
- appropriate agreements are signed with processors of personal data and they are given detailed instructions on the processing;
- the respective responsibilities of joint controllers are agreed on in a transparent manner;
- data subjects are informed and the exercise of their rights is facilitated;
- possible restrictions to the rights of data subjects are justified;
- a record of processing activities has been drawn up;
- procedures have been designed for personal data breaches;
- a Data Protection Officer has been designated if the processing activities entailed by the research project so require; and
- other documentation required for accountability has been drawn up and is updated when necessary.

Source: Webpage of Data Protection Ombudsman

Impact assessment in scientific research[423]

The Data Protection Ombudsman also highlights that it is mandatory to carry out an Impact Assessment when the risk to the rights and freedoms of individuals are seen as high. It is required when at least two of the following apply:

- The processing involves special categories of personal data or other data of a highly personal nature.
- Personal data is processed on a large scale.
- The processing involves aggregation of data.
- The processing involves individuals in a vulnerable position, such as patients, children or the aged.
- The processing involves the use of new technological and organisational solutions or innovations.
- The processing involves biometric data.
- The processing involves genetic data.
- The processing involves location data.

[422] Listed on the webpage of the Data Protection Officer, viewed 23 March 2021, https://tietosuoja.fi/en/roles-and-responsibilities-for-processing-personal-data.
[423] As described on the webpage of the Data Protection Officer, viewed 23 March 2021, https://tietosuoja.fi/en/lifespan-of-personal-data-processing-data-protection-principles-and-the-protection-of-data.

- The controller wishes to derogate from the obligation to inform the data subjects by virtue of Article 14(5)(b) of the GDPR.
- The controller wishes to derogate from other rights of the data subject.

If the impact assessment leads to the conclusion that the processing will result in a high risk to the data subjects' rights, and the controller is not able to reduce that risk, the Data Protection Ombudsman needs to be consulted. This can be done easily by filling in an online form available at the Data Protection Ombudsman's webpage.

Appropriate destruction, anonymisation or archiving of data when concluding the research

With references to the GDPR, the Finnish Data Protection Ombudsman highlights the need to end the lifespan of the personal data appropriately at the end of the research[424]. The focus lays foremost on destruction, anonymisation and archiving.

Concerning the destruction of data, the SA notes that the most effective way depends on the storage medium. Shredding or burning are effective for physical paper material, whereas data on a USB stick can be destroyed by destroying the USB-stick. Electronic data can also be overwritten, but the SA notes that simply deleting or transferring files to the recycle bin of the computer does not entail permanent destruction.

Anonymisation has already been touched upon above. The Finnish SA refers to the WP29 opinion on anonymisation techniques[425]. It also mentions, that should the data controller not be familiar with anonymisation techniques themselves, they should ask for appropriate assistance.

As for archiving, it is noted that the responsibility for archived material still lies with the data controller, in accordance with the GDPR. The SA also provides guidance on the archiving principles, as per the GDPR[426].

France

CNIL methodologies for health and medical research

Methodologies of reference with regard to research in the medical and health domain, issued by CNIL, state the conditions and safeguards for the processing of personal data in this domain. If the party processing personal data for medical and health research purposes complies with them, the *authorisation of processing by CNIL is not needed*[427]. The researcher, however, needs to notify CNIL about compliance with each of methodologies issued, if they are applicable.

These methodologies contain different conditions for specific research. MR-001 provides guidelines for medical and health-related research, where consent of the data subject had been obtained, whereas MR-003 provides the guidelines when no consent was obtained, and MR-004 when personal data is re-used. It is important to underly that it is not a consent, which has its source in GDPR. It is a consent requested in and based on the French Public Health Code.

[424] Webpage of the Data Protection Ombudsman, viewed 23 March 2021, https://tietosuoja.fi/en/destruction-anonymisation-or-archiving-of-data.
[425] Article 29 Working Party's opinion 5/2014 on anonymisation techniques, https://ec.europa.eu/newsroom/article29/news-overview.cfm.
[426] Webpage of the Data Protection Ombudsman, viewed 23 March 2021, https://tietosuoja.fi/en/destruction-anonymisation-or-archiving-of-data.
[427] CNIL, Recherches dans le domaine de la santé: la CNIL adopte de nouvelles mesures de simplification, viewed 5 July 2021, https://www.cnil.fr/fr/recherches-dans-le-domaine-de-la-sante-la-cnil-adopte-de-nouvelles-mesures-de-simplification.

In general, all methodologies issued by CNIL include e.g. **obligations to appoint a Data Protection Officer, notify and give a data subject access to his or her data, and obligation to use anonymous data whenever possible, or pseudonymise it**. The results of the research should only show anonymised data. Some of these methodologies are further described hereunder.

Methodology MR-001[428] sets up the rules for conducting the research when the *consent of the data subject is obtained*. The methodology relates primarily to research on humans, where the data subject is directly engaged. **A person responsible for the project shall be appointed and it appoints the person responsible for personal data protection**. The party responsible for **processing should not collect data, except for that which is needed, adequate and limited to what is necessary for the research purposes**. The necessity of **collecting particular data shall be justified in a scientific way in the research protocol**. Particular categories and kinds of **data shall be enlisted in the corresponding research methodology document**. The personal data of patients shall only be kept for the period necessary to conduct research or only for two years after the last publication of results, or if the results are not published until signing the final report about the research project. The methodology of research shall stipulate the kinds of data through which data subjects can be directly identifiable and also those through which they are indirectly identifiable. People accessing personal data shall preserve professional secrecy. **General information and notice to the data subject shall be issued, informing about the character and purposes of the research. Explicit, clear, freely given and written consent** shall be given by the data subject if its data is about to be processed, especially if research requires examination of genetic characteristics. The person responsible for the research should conduct **an impact assessment**, describing risks to the data subject's fundamental rights. It should introduce a sufficient level of protection, **through technical and organisational measures**, that will secure data subjects against these potential risks. The person responsible for the research should monitor and control the application of all the above-mentioned safeguards.

Methodology MR-003[429] relates to research in the domain of health, but *without obtaining the consent of the data subject* (consent-based on French Publich Health Code), where the data subject has been informed about the research but did not opposed it. This means that the person concerned did not oppose the research before it had been informed about it. The methodology relates particularly to the research, where engagement of human subject is not directly needed, and the research is conducted on the clusters of people. In this case, all the rules from MR-001 are applicable except that consent is not required. The main difference is that the use of data based on which a data subject *can be directly identified shall be excluded* from reference methodology.

Methodology MR-004 applies to the research when personal data is mainly re-used and there is *no initial collecting of personal data*. All projects under the definition in this methodology should be additionally registered. All requirements from the above-mentioned methodologies are applicable, except that, as in MR-004, explicit consent to participate in the research is not required and *data directly relating to an identifiable individual shall be excluded* from reference methodology.

The CNIL framework of reference concerning data *retention* in the field of health research[430] is a supplementary document, which defines in detail the period for which data applied in health research can be and ought to be retained. Each period depends on the type of health research conducted and on which methodology issued by CNIL was applied.

[428] CNIL, Méthodologie de référence MR-001, Recherches dans le domaine de la santé avec recueil du consentement, viewed 5 July 2021, https://www.cnil.fr/fr/declaration/mr-001-recherches-dans-le-domaine-de-la-sante-avec-recueil-du-consentement.
[429] CNIL, Méthodologie de référence MR-003, Recherches dans le domaine de la santé sans recueil du consentement, viewed 5 July 2021, https://www.cnil.fr/fr/declaration/mr-003-recherches-dans-le-domaine-de-la-sante-sans-recueil-du-consente.
[430] CNIL, Référentiel les durées de conservation: Recherches dans le domaine de la santé, viewed 5 July 2021, https://www.cnil.fr/sites/default/files/atoms/files/referentiel_-_recherches_dans_le_domaine_de_la_sante.pdf.

ANNEX 3 – SOURCES OF INFORMATION

Legislation

Austrian Parliament. (1999). *Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657).* Vienna: Austrian Official Gazette.

Austrian Parliament. (1981). *Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation (Forschungsorganisationsgesetz – FOG) StF: BGBl. Nr. 341/1981 idF BGBl. Nr. 448/1981 (DFB).* Vienna: Austrian Official Gazette.

Belgian Federal Parliament. (1990). *Act of 15 January 1990 setting up the Crossroad Database for Social Security, as modified by Act of 5.9.2019 regarding ISCs (Article 11).* Brussels: Belgian Official Gazette.Belgian Federal Parliament. (2006). Health Act of 13 December 2006, adding Article 45quinquies to the Royal Decree No 78 of 10.11.1967. Brussels: Belgian Official Gazette.

Belgian Federal Parliament. (2018) — *Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Belgian Data Protection Act.* Brussels: Belgian Official Gazette.

Kingdom of Belgium. (2018). *Royal Decree of 9 January 2018 on biobanks.* Brussels: Belgian Official Gazette. Bulgarian Parliament. (2002). *Personal Data Protection Act.* Commission for Personal Data Protection. Sofia: Bulgarian Official Gazette.

Council of Europe. (1997). *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine.* Oviedo: European Treaty Series No. 164.

Estonian Parliament (Riigikogu). (2018). *Estonian Personal Data Protection Act.* Tallinn: Estonian Official Gazette.

Estonian Parliament (Riigikogu). (2000). *Human Genes Research Act.* Tallinn: Estonian Official Gazette.

Estonian Parliament (Riigikogu). (2005). *Medicinal Products Act, passed 16.12.2004, RT I 2005, 2, 4, entry into force 01.03.2005.* Tallinn: Estonian Official Gazette.

Estonian Parliament (Riigikogu). (2010). *Official Statistics Act, passed 10.06.2010, RT I 2010, 41, 241, entry into force 01.08.2010, .* Tallinn: Estonian Official Gazette .

European Parliament and the Council. (2001). *Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the EEA States relating to the implementation of good clinical practice.* Brussels: Official Journal of the European Union

European Parliament and the Council. (2004). *Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells.* Brussels: Official Journal of the European Union

European Parliament and the Council. (2008). *Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation 1101/2008.* Brussels: Official Journal of the European Union

European Parliament and the Council. (2014). *Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.* Brussels: Official Journal of the European Union

European Parliament and the Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* Brussels: Official Journal of the European Union

European Parliament and the Council. (2020). *Proposal for a Regulation Of The European Parliament And Of The Council on European data governance (Data Governance Act), COM/2020/767.* Brussels: Official Journal of the European Union

Finnish Parliament. (2015). *Act on the Openness of Government Activities, 621/1999, as amended by 907/2015,* . Helsinki: Finnish Official Gazette.

Finnish Parliament. (1987). *Medicines Act 395/1987* . Helsinki: Finnish Official Gazette.

Finnish Parliament. (2018). *Data Protection Act 1050/2018.* Helsinki: Finnish Official Gazette.

Finnish Ministry of Justice,. (2018). Proposal of the Finnish Government for *Personal Data Protection Act, Hallituksen esitys HE 9/2018* . Helsinki : Finnish Official Gazette.

French Parliament. (1951). *Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques.* Paris: French Official Gazette.

French Parliament. (1978). *Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties.* Paris: French Official Gazette.

French Parliament. (2004). *Act of 20 February 2004 Code du patrimoine.* Paris: French Official Gazzette.

French Presidency. (2019). *Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - Légifrance (legifrance.gouv.fr),* Paris: French Official Gazette.

German Federal Parliament (1999). *Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG).* (1999). Berlin: StF: BGBl. I Nr. 165/1999, German Official Gazette.

German Federal Parliament. (2014). *Bundesdatenschutzgesetz (BDSG).* Berlin: German Official Gazette.

German Parliament of Hesse. (20018). *Hessischen Gesetzes zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit vom 3. Mai 2018 (GVBl. S. 82),* Hesse: Hessian Official Gazette.

Greek Parliament. (2019). *Law 4624/2019 Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.* Athens: Government Gazzette of the Hellenic Republic.

Icelandic Parliament. (1944). *Constitution of the Republic of Iceland.* Reykjavik: National Legislative Bodies.

Icelandic Parliament. (2007). *Act on Statistics Iceland and official statistics (2007 Lög um Hagstofu Íslands og opinbera hagskýrslugerð).* Reykjavik: Icelandic Official Gazette.

Icelandic Parliament. (2018). *Act No. 90/2018 on Data Protection and the Processing of Personal Data (2018 Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga)* . Reykjavic : Icelandic Official Gazzete.

Italian Parliament. (2019). *Personal Data Protection Code containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal.* Rome: Italian Official Gazette.

Italian Presidency. (2012). *Decree-Law No 179 of 18.10.12 on epidemiological surveillance systems and registries of mortality, cancer and other diseases* . Rome: Italian Official Gazette.

Italian Presidency. (2012). *Decreto-Legge convertito con modificazioni dalla L. 17 dicembre 2012, n. 221 (in S.O. n. 208, relativo alla G.U. 18/12/2012, n. 294),* Rome: Italian Official Gazette.

Italian President of the Council of Ministries. (2017). *Decreto del Presidente del Consiglio dei Ministri sull'identificazione dei sistemi di sorveglianza epidemiologica e dei registri di mortalità, cancro e altre malattie adottato il 3.3.2017* . Rome: Italian Official Gazette.

Italian Ministry of Health. (2016). *DECRETO 7 dicembre 2016, n. 262 Regolamento recante procedure per l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, anche quando gestiti da diverse amministrazioni dello Stato. (17G00016)* . Rome: Italian Official Gazette.

Italian President of the Council of Ministers. (2015). *DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 29 settembre 2015, n. 178 Regolamento in materia di fascicolo sanitario elettronico. (15G00192).* Rome : Italian Official Gazette.

Norwegian Parliament. Department of Health and Social Care. (2008). *Act on Medical and Health Research (Health Research Act).* Oslo: Norwegian Official Gazette.

Norwegian Parliament. Department of Health and Social Care. (2014). *Lov om helseregistre og behandling av helseopplysninger (helseregisterloven).* Oslo : Norwegian Official Gazette.

Norwegian Parliament. Department of Health and Social Care. (2018). *Act on Therapeutic Biobanks (Therapeutic Biobank Act).* Oslo: Norwegian Official Gazette.

Norwegian Parliament. Department of Justice and Emergency Preparedness. (2021). *Act on the procedure in administrative matters (Administrative Procedure Act).* Oslo: Norwegian Official Gazette.

Norwegian Parliament. Department of Labour and Social Affairs. (2021). *National Insurance Act.* Oslo: Norwegian Official Gazette.

Norwegian Parliament. (2018). *Data Protection Act (Personopplysningsloven), LOV-2018-06-15-38.* Oslo: Norwegian Official Gazzete.

Norwegian Parliament. (2021): Department of Health and Care Services. (2021). Health Personnel Act (*Lov om helsepersonell m.v. helsepersonelloven*), *LOV-1999-07-02-64.* Oslo: Norwegian Official Gazette.

Polish Ministry of Health. (2012). *Regulation of the Minister of Health of 2 May 2012 on Good Clinical Practice.* Warsaw: Polish Official Gazette.

Polish Parliament. (2018). *Act of 20 July 2018 The Law on Higher Education and Science.* Warsaw.

United Nations Educational, Scientific and Cultural Organization (UNESCO), . (2005). *Universal Declaration on Bioethics and Human Rights.* Paris: UNESCO.

World Medical Association. (2002). *Declaration Of Taipei On Ethical Considerations Regarding Health Databases And Biobanks* . Washington DC: 53 WMA General Assembly.

Case Law

I. v Finland, no. 20511/03 (ECtHR July 17 , 2008,).

KHO:2013:181, 365 (Finish Supreme Administrative Court November 22, 2013).

M.S. v Sweden, no. 20837/92 (ECtHR August 27, 1997).

P.T. v La République de Moldavie, no. 1122/12 (ECtHR May 26, 2020).

also Tzortzatou, O. S.-B.-C.-J. (2021). Biobanking across Europe Post-GDPR. In S. Slokenberga, O. Tzortzatou, & J. and Reichel, *GDPR and Biobanking* (pp. 397-420). Springer Law, Governance and Technology Series.

Article 29 Data Protection Working Party. (2014). *Opinion 05/2014 on Anonymisation Techniques.* Brussels: Article 29 Data Protection Working Party.

Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation (Forschungsorganisationsgesetz – FOG) StF: BGBl. Nr. 341/1981 idF BGBl. Nr. 448/1981 (DFB), . (n.d.).

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG). (1999). Berlin: StF: BGBl. I Nr. 165/1999.

Bundesland of Hesse. (20018). *Hessischen Gesetzes zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit vom 3. Mai 2018 (GVBl. S. 82),* . Hesse.

Bushan Mishra, S. A. (2011,). *Handbook of research methodology.* Educreation Publishing.

Chassang, G. and Rial-Sebbag, E.,. (2018). Research Biobanks and Health Databases: the WMA Declaration of Taipei, Added Value to the European Legislation (Soft and Hard Law). *European Journal of Health Law*, 501-516.

CNIL. (2018). *Authentification par mot de passe: les mesures de sécurité élémentaires.* Paris: CNIL.

CNIL. (2018). *Guide sécurité des données personnelles.* Paris: CNIL.

CNIL. (2018). *Méthodologie de référence MR-003, Recherches dans le domaine de la santé sans recueil du consentement.* Paris: CNIL.

CNIL. (2021). *CNIL - Méthodologie de référence MR-006. Études nécessitant l'accès aux données du PMSI par les industriels de santé Méthodologie de référence MR-006 | .* Paris: CNIL.

CNIL. (2021). *Méthodologie de référence MR-001, Recherches dans le domaine de la santé avec recueil du consentement.* Paris: CNIL.

CNIL. (2021, July 5). *Recherches dans le domaine de la santé : la CNIL adopte de nouvelles mesures de simplification*. Retrieved from https://www.cnil.fr/fr/recherches-dans-le-domaine-de-la-sante-la-cnil-adopte-de-nouvelles-mesures-de-simplification

CNIL. (2021). *Référentiel les durées de conservation: Recherches dans le domaine de la santé.* Paris: CNIL.

CNRS. (2019). *Les sciences humaines et sociales et la protection des données à caractère personnel dans le contexte de la science ouverte, Guide Pour la Recherche,* . Paris: CNRS.

CoE. (1997). *Explanatory Memorandum to Recommendation Rec(1997)18 on the protection of personal data collected and processed for statistical purposes.* Strasbourg: CoE.

Council of Europe. (1997). *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine.* Oviedo: European Treaty Series No. 164.

Council of Europe. (2006). *Recommendation CM/Rec (2016)6 of the Committee of Ministers to member States on research on biological materials of human origin, which is a successor of Council of Europe, Recommendation Rec(2006)4 on research on biological materials* . Strasbourg: CoE.

Council of Europe, . (2019). *Recommendation CM/Rec 2019 of the Committee of Ministers to member States on the protection of health-related data.* Strasbourg: CoE.

De Bot, D. (2020). , 'De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit',. *Mechelen, Wolters Kluwer*, 351-353.

Decision, BvR 424/71 und 325/72 (BVerfG May 29, 1973).

Decision, BvR 333/75 (BVerfG March 1, 1978).

Department of Health and Social Care. (2008). *Act on Medical and Health Research (Health Research Act).* Oslo: Norwegian Offcial Gazette.
Deutsche Forschungsgemeinschaft. (2019). *Guidelines for Safeguarding Good Research Practice Code of Conduct.* Deutsche Forschungsgemeinschaft.
DSK. (2019). *Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO* . DSK.
ECtHR - M.K. v. France , no. 76100/13 (ECtHR September 24, 2015).
Engelfriet, A. e. (2018). De Algemene Verordening Gegevensbescherming – Artikelsgewijze commentaar'. *Ius Mentis,*, 289.
European Archives Group. (2018). *Guidance on Data Protection for Archive Services, EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector.* Brussels : EAG.
European Commission. (2018). *The European Cancer Information System (ECIS) web application, Computing and disseminating European statistics on cancer burden.* Brussels: JRC Technical Reports.
European Data Protection Board . (2021). *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research.* Brussels: EDPB.
European Data Protection Board. (2019). *Opinion 3/2019 concerning Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR).* Brusssels: EDPB.
European Data Protection Board. (2020). *Study on the secondary use of personal data in the context of scientific research, under Contract No EDPS/2019/02-04, 2020.* Brussels: EDPB.
European Data Protection Supervisor. (2020). *A Preliminary Opinion on data protection and scientific research.* Brussels: EDPS.
European Parliament. (2019). *European Parliament, How the General Data Protection Regulation changes the rules for scientific research.* Brussels: Panel for the Future of Science and Technology.
European Parliament and the Council. (2001). *Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the EEA States relating to the implementation of good clinical practice.* Brussels: OJEU.
European Parliament and the Council. (2004). *Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells.* Brussels: OJEU.
European Parliament and the Council. (2008). *Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation 1101/2008.* Brussels: OJEU.
European Parliament and the Council. (2014). *Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.* Brussels: OJEU.
European Parliament and the Council. (2020). *Proposal for a Regulation Of The European Parliament And Of The Council on European data governance (Data Governance Act), COM/2020/767.* Brussels : OFEU.
Findata. (2021, July 5). *Social and Health Data Permit Authority Findata promotes secondary use of health and social data, facilitates data permit processing and improves data protection for individuals.* Retrieved from https://findata.fi/en/

Finish Ministry of Justice. (2015). *Act on the Openness of Government Activities, 621/1999, as amended by 907/2015, .* Helsinki.
Finish Ministry of Social Affaires and Health . (2021, July 5). *Secondary use of health and social data*. Retrieved from https://stm.fi/en/secondary-use-of-health-and-social-data
Finish Parliament. (1987). *MEDICINES ACT 395/1987* . Helsinki: Finish Official Gazette.
Finish Parliament. (2018). *Data Protection Act* . Helsinki.
Finish Parliament. (2018). *Personal Data Protection Act, Hallituksen esitys HE 9/2018* . Helsinki.
French Parliament. (1951). *Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques.* Paris: French Official Gazette.
French Parliament. (2004). *Act of 20 February 2004 Code du patrimoine.* Paris: French Gazzette.
Garante della Privacy. (2018). *Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510]* . Rome: Garante della Privacy.
Garante per la protezione dei dati personali. (2018). *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018* . Rome: Garante per la protezione dei dati personali.
Greek Parliament. (2019). *Law 4624/2019 Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.* Athens: Government Gazzette of the Hellenic Republic.
Health Care Knowledge Centre (Federaal Kenniscentrum voor de Gezondheidszorg or KCE). (2015). *Ten years of multidisciplinary teams.* Brussels: KCE report 239.
Heinz Huber v Bundesrepublik Deutschland, Case C-524/06 (Judgment of the Court (Grand Chamber) December 16, 2008).
Icelandic Parliament. (2007). *Act on Statistics Iceland and official statistics (2007 Lög um Hagstofu Íslands og opinbera hagskýrslugerð).* reykjavik: Icelandic Official Gazette.
Icelandic Parliament. (2018). *Act No. 90/2018 on Data Protection and the Processing of Personal Data (2018 Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga)* . Reikjavic : Icelandic gazzete.
Irish Council for Bioethics. (2005). *Human Biological Material: Recommendations for Collection, Use and Storage in Research* . Dublin: Irish Council for Bioethics.
Italian Parliament. (2019). *Personal Data Protection Code containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal.* Rome.
Italian Presidency. (2012). *Decree-Law No 179 of 18.10.12 on epidemiological surveillance systems and registries of mortality, cancer and other diseases* . Rome: Italian Official Gazette.
Italian Presidency. (2012). *Decreto-Legge convertito con modificazioni dalla L. 17 dicembre 2012, n. 221 (in S.O. n. 208, relativo alla G.U. 18/12/2012, n. 294), .* Rome: Italian Official Gazette.
Italian President of the Council of Ministries. (2017). *Decreto del Presidente del Consiglio dei Ministri sull'identificazione dei sistemi di sorveglianza epidemiologica e dei registri di mortalità, cancro e altre malattie adottato il 3.3.2017* . Rome : Italian Official Gazette.

Lalova, T. N.-J. (2021). 'An overview of Belgian Legislation Applicable to Biobank Research and its Interplay with Data Protection Rules',. In S. T. Slokenberga, *GDPR and Biobanking. Individual Rights, Public Interest and Research Regulation across Europe* (p. 187 et seq.). Springer Law, Governance and Technology Series.

Ministry of Education and Research . (2021, July 5). *Norwegian Centre for Research Data*. Retrieved from https://www.regjeringen.no/en/dep/kd/organisation/kunnskapsdepartementets-etater-og-virksomheter/Subordinate-agencies/norwegian-social-science-data-services-/id440384/

Ministry of Health. (2012). *Regulation of the Minister of Health of 2 May 2012 on Good Clinical Practice.* Warsaw: Polish Official Gazette.

Ministry of Health. (2016). *DECRETO 7 dicembre 2016, n. 262 Regolamento recante procedure per l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, anche quando gestiti da diverse amministrazioni dello Stato. (17G00016)* . Rome: Italian Official Gazette.

Mondschein, C. F. (2019). 'The EU's General Data Protection Regulation (GDPR) in a Research Context. *Kubben, P., Dumontier, M., Dekker, A. (eds.). Fundamentals of Clinical Data Science, Springer*, 55-74.

National Center for Social Research. (2019). *Adoption of the Code of Ethics and Conduct Research Ethics and the Rules for the Application of Principles and Operation of the Committee on Ethics and Research Ethics Committee of the National Centre for Humanities an.* Athens: Greek Gazzette.

Norwegian Centre for Research Data. (2021, July 5). *NSD Strategy 2021–2024*. Retrieved from https://www.nsd.no/en/about-nsd-norwegian-centre-for-research-data/nsd-strategy-20212024/

Norwegian Department of Health and Social Care. (2014). *Lov om helseregistre og behandling av helseopplysninger (helseregisterloven).* Oslo : Norwegian Official Gazette.

Norwegian Department of Health and Social Care. (2018). *Act on Therapeutic Biobanks (Therapeutic Biobank Act).* Oslo: Norwegian Official Gazette.

Norwegian Department of Justice and Emergency Preparedness. (2021). *Act on the procedure in administrative matters (Administrative Procedure Act).* Oslo: Norwegian Official Gazette.

Norwegian Department of Labour and Social Affairs. (2021). *National Insurance Act.* Oslo: Norwegian Official Gazette.

Norwegian National Committee for Research Ethics in Science and Technology. (2015). *Guidelines for Research Ethics in Science and Technology.* Oslo: Norwegian National Committee for Research Ethics in Science and Technology.

Norwegian Parliament . (2018). *Data Protection Act (Personopplysningsloven), LOV-2018-06-15-38.* Oslo: Norwegian Gazzete.

Office of Data Protection Ombudsman . (2021, March 23). *Roles and responsibilities for processing personal data in scientific research.* Retrieved from https://tietosuoja.fi/en/roles-and-responsibilities-for-processing-personal-data

Office of Data Protection Ombudsman. (2021, March 23). *Destruction, anonymisation or archiving of data at the conclusion of research.* Retrieved from https://tietosuoja.fi/en/destruction-anonymisation-or-archiving-of-data

Office of teh Data Protection Ombudsman. (2021, March 23). *Lifespan of personal data processing, data protection principles and the protection of data in scientific research.* Retrieved from https://tietosuoja.fi/en/lifespan-of-personal-data-processing-data-protection-principles-and-the-protection-of-data

Office of the Data Protection Ombudsman. (2021, July 5). *Minimisation of personal data in scientific research.* Retrieved from https://tietosuoja.fi/en/minimisation-of-personal-data

Office of the Data Protection Ombudsman. (2021, July 5). *Scientific research and data protection*. Retrieved from https://tietosuoja.fi/en/scientific-research-and-data-protection

Ombudsman, T. O. (2021, July 5). Retrieved from Defining the research scheme and purpose for processing personal data: https://tietosuoja.fi/en/defining-the-research-scheme-and-purpose-for-processing-personal-data

P.N. v Germany, no. 74440/17 (ECtHR June 11, 2020).

Peruzzo and Martens v. Germany, 7841/08 et 57900/12 (ECtHR April 4, 2013).

Polish Parliament . (2018). *Act of 20 July 2018 The Law on Higher Education and Science.* Warsaw.

Pormeister, K. (2018). Genetic research and applicable law: the intra-EU conflict of laws as a regulatory challenge to cross-border genetic research. *Journal of Law and the Biosciences*, 706–723.

Portmeister, K. (2017). Genetic data and the research exemption: is the GDPR going too far? *International Data Privacy Law*, 139.

President of the Council of Ministers. (2015). *DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 29 settembre 2015, n. 178 Regolamento in materia di fascicolo sanitario elettronico. (15G00192).* Rome : Italian Official Gazette.

Ragnhildur Guðmundsdóttir against the Icelandic State, no. 151/2003 (Supreme Court of iceland November 27, 2003).

Recht, G. (2014). *Bundesdatenschutzgesetz (BDSG).* Berlin: G. Recht.

Republic of Bulgaria. (2002). *Personal Data Protection Act.* Sofia: Commission for Personal Data Protection.

Republic of France. (2019). *Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - Légifrance (legifrance.gouv.fr),* . Paris.

Republic of Iceland. (1944). *Constitution of the Republic of Iceland.* reykjavik: National Legislative Bodies .

Republique of France. (1978). *Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties.* Paris.

Riigikogu. (2000). *Human Genes Research Act.* Tallin: Estonian Official Gazette.

Riigikogu. (2005). *Medicinal Products Act, passed 16.12.2004, RT I 2005, 2, 4, entry into force 01.03.2005.* Tallin: Estonian Official Gazette.

Riigikogu. (2010). *Official Statistics Act, passed 10.06.2010, RT I 2010, 41, 241, entry into force 01.08.2010,* . Tallin: Estonian Official Gazette .

S. And Marper v. The United Kingdom, 30562/04 and 30566/04 (ECtHR December 4, 2008).

Science Europe. (2021). *Practical Guide to the International Alignment of Research Data Management – extended Edition.* Brussels: Science Europe.

The European Parliament and the Council of the European Union. (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* . Official Journal of the European Union.

The Norwegian Centre for Research Data. (2021, August 08). *Norwegian Centre for Research Data*. Retrieved from https://www.nsd.no/en/about-nsd-norwegian-centre-for-research-data/

The Norwegian National Research Ethics Committee. (2021, July 5). *The Personal Data Act*. Retrieved from https://www.forskningsetikk.no/en/resources/the-research-ethics-library/legal-statutes-and-guidelines/the-personal-data-act/

The Norwegian National Research Ethics Committees. (2019). *Guidelines for Research Ethics in the Social Sciences, Humanities, Law, and Theology.* Oslo: The Norwegian National Research Ethics Committees.

The Research Council of Norway. (2019). *Ethical Standards in Research.* Oslo: The Research Council of Norway.

United Nations Educational, Scientific and Cultural Organization (UNESCO), . (2005). *Universal Declaration on Bioethics and Human Rights.* Paris: UNESCO.

Université Paris Nanterre. (2019). *Règlement général pour la protection des données.* Paris: Université Paris Nanterre.

University of Macedonia. (2019). *Code of Ethics and Conduct of Scientific Research.* Thessaloniki: University of Macedonia.

University of Tartu. (2017). *Estonian Code of Conduct for Research Integrity.* Tartu: Centre for Ethics, University of Tartu.

World Medical Association. (2002). *Declaration Of Taipei On Ethical Considerations Regarding Health Databases And Biobanks* . Washington DC: 53 WMA General Assembly.

Z v Finland, no. 22009/93 (ECtHR February 25 , 1997).

ANNEX 4 - QUESTIONNAIRE TO SAs– NATIONAL SOURCES OF INFORMATION

Country

Please, provide the name of your Country/Supervisory Authority:

I. **Are the requirements for appropriate safeguards with regard to data processing for the purpose of scientific research of Article 89(1) GDPR implemented in your country by specific provisions in:**

a) National GDPR legislation (national laws, regulations, directives, acts and decrees)

No [ ]

Yes [ ]

If so, please provide hereunder details and links, including to an English translation.

Reference to the national legislation (Name, Article, Hyperlink)	Short Description

b) National sectoral legislation (e.g. health, security, banking, telecoms, energy, IT/ICT, smart cities' research, autonomous vehicles, social sciences, defense, archives)

No [ ]

Yes [ ]

If so, please provide hereunder details and links, including to an English translation.

Reference to the national legislation (Name, Article, Hyperlink)	Short Description

c) Non-binding governmental documents (guidelines, notices and communications)

No [ ]

Yes [ ]

If so, please provide hereunder details and links, including to an English translation.

Reference to the document (Name, Article, Hyperlink)	Short Description

d) Guidelines, opinions and decisions of Supervisory Authorities (SAs)

No [ ]

Yes [ ]

If so, please provide hereunder details and links, including to an English translation.

Reference to the document (Name, Article, Hyperlink)	Short Description

e) Non-governmental regulations or documentation such as industry codes; standards; rules of professional associations or research associations (e.g. in the health, security, banking, telecoms, energy, IT/ICT, smart cities' research, autonomous vehicles, social sciences, defense, archives sector)

No [ ]

Yes [ ]

If so, please provide hereunder details and links, including to an English translation.

Reference to the document (Name, Article, Hyperlink)	Short Description

f) <u>(Framework) contracts and processing agreements between research institutions and individual researchers/research groups</u>

No [ ]

Yes [ ]

If so, please provide hereunder details and links, including to an English translation.

Reference to research institution (Name, Hyperlink)	Short Description

II. Are there in your country any <u>other</u> requirements, specifications or guidelines relating to the need for appropriate safeguards for processing of personal data for scientific research purposes (in force or planned) based on:

a) <u>Any other type of legislation, soft regulation or industry rules?</u>

An example of such type of legislation is Archiefwet 1995 in the Netherlands that has requirements that may affect the rights of data subjects. Are there similar laws for archiving or records keeping/records management/documentation/registries in other countries (e.g. record-keeping requirements for dual-use/export controls regulations for strategic sectors)?

An example of an industry rule is Dutch Research Council (NWO) that has a data management protocol to be followed by researchers in the wide range of scientific domains, and requires them to submit data management plan which should comply with certain criteria or provide certain information (e.g. storage).

b) <u>National or international jurisprudence (e.g. national courts, ethical committees, jurisprudence of the Court of Justice of the EU (CJEU))?</u>

No [ ]

Yes [ ]

If yes, please, provide specify:

Reference to the requirements	Short Description

Thank you very much for your participation!!