



HAL
open science

Common Infrastructure for National Cohorts in Europe, Canada, and Africa -CINECA

Éloïse Gennet, Melanie Goisauf, Delphine Pichereau, Emmanuelle Rial-Sebbag

► **To cite this version:**

Éloïse Gennet, Melanie Goisauf, Delphine Pichereau, Emmanuelle Rial-Sebbag. Common Infrastructure for National Cohorts in Europe, Canada, and Africa -CINECA. CINECA Project. 2020. halshs-03836714

HAL Id: halshs-03836714

<https://shs.hal.science/halshs-03836714>

Submitted on 2 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Common Infrastructure for National Cohorts in Europe, Canada, and Africa - CINECA -

Deliverable D7.2

Catalogue of Canadian, European and African ethical and legal gaps

Work Package:	WP7 - Ethical and legal governance framework for transnational data-sharing
Lead Beneficiary:	Inserm
WP Leader(s):	Emmanuelle Rial-Sebbag (INSERM), Melanie Goisauf (BBMRI-ERIC)
Contributing Partner(s):	BBMRI-ERIC; EMBL-EBI
Contractual Delivery Date:	30th November 2020
Actual Delivery Date:	30 Nov 2020
Authors of this Deliverable:	Éloïse Gennet, Melanie Goisauf, Delphine Pichereau, Emmanuelle Rial-Sebbag
Reviewed by:	Leslie Glass, Michaela Th. Mayrhofer
Approved by:	Thomas Keane
Dissemination Level:	Public
Grant agreement:	No. 825775 Horizon 2020 (H2020-SC1-BHC-2018-2020)
Type of action:	RIA
Start Date:	1 Jan 2019
Duration:	48 months



1. Table of contents

1. Table of contents	2
2. Executive summary	5
3. Abbreviations	7
4. Scope	8
4.1 Territorial scope	8
4.1.1 European law	8
4.1.1.1 Direct applicability of GDPR in EU Member States laws	8
4.1.1.2 GDPR compliance of European National laws outside of EU	8
4.1.2 Canadian law	9
4.1.3 African law	10
4.2 Material scope	11
4.2.1 “Personal data” in the scope of GDPR	11
4.2.1.1 Pseudonymised data is personal data protected by GDPR	11
4.2.1.2 Anonymised data falls outside of GDPR	11
4.2.1.4 When anonymised data falls back into GDPR	14
4.2.2 “Health” and “genetic” data in the scope of GDPR	15
4.2.3 Scientific research in contrast with the public interest	16
4.3 Limitations	16
4.3.1 Lack of interoperability given the plurality of normative sources	16
4.3.2 Lack of experience given the recent renewals of most data protection laws	16
4.3.3 Different interpretations of GDPR, yet still compliant	17
5. ELSI questions	17
5.1 How to choose a legal basis for CINECA’s data processing?	18
5.1.1 Is consent the priority legal basis for health data processing in GDPR?	18
5.1.2 Is “explicit consent” to health data processing an attainable standard?	19

D7.2	Catalogue of Canadian, European and African ethical and legal gaps	CINECA
5.1.3	Is “public health” a suitable basis for research activities?	20
5.1.4	Is GDPR pushing towards the scientific (health) research exemption?	20
5.1.5	Is it ethical to use the research exemption?	21
5.1.6	Is it ethical NOT to use the research exemption?	21
5.1.7	Is the research exemption legal in other National laws relevant for CINECA?	22
5.1.7.1	In Switzerland	22
5.1.7.2	In Canada	23
5.1.7.3	In South Africa	23
5.1.7.4	In the United Kingdom	23
5.1.7.5	In the Netherlands	24
5.1.7.6	In Estonia	24
5.1.8	A suggestion for an ethical research exemption instead of consent	25
5.2	How should CINECA apprehend broad consent to further data processing?	26
5.2.1	Once and for all: is broad consent to further health data processing for research purposes acceptable under GDPR?	26
5.2.2	Is broad consent in GDPR accompanied by other safeguards?	27
5.2.3	Is broad consent ethically acceptable for and to patients?	28
5.2.4	Is broad consent legal in other National laws relevant for CINECA?	30
5.2.4.1	United Kingdom	30
5.2.4.2	Switzerland	31
5.2.4.3	Africa	32
5.2.4.4	Canada	33
5.3	Conclusive recommendation	34
6.	Next steps	35
6.1	First findings on benefit sharing & FAIRness	35
6.1.1	Africa	35
6.1.2	Canada: Tri-Council Policy Statement	37
6.1.2.1	Chapter 4 on “Fairness and equity in research participation”	37
6.1.2.2	Chapter 9 on “research involving the first nations, Inuit and Métis peoples of Canada”	37

D7.2	Catalogue of Canadian, European and African ethical and legal gaps	CINECA
6.2	Further cooperation on cross border exchanges	38
7.	Delivery and schedule	39
8.	References	39
8.1	Legal instruments, institutional documents	39
8.1.1	European Union	39
8.1.1.1	EU Member States law	39
8.1.1.2	EU Legal instruments	39
8.1.1.3	EU Case Law	40
8.1.1.4	EU Reports	40
8.1.2	Canada	40
8.1.3	Africa	41
8.1.4	Others	41
8.1.4.1	United Kingdom	41
8.1.4.2	Switzerland	41
8.1.4.3	GA4GH	42
8.1.4.4	BBMRI-ERIC	42
8.2	CINECA	42
8.3.1	Relevant previous deliverables	42
8.3.2	Cohorts' internal policies	42
	CARTaGENE	42
	CHILD	42
	CLSA	42
	EGA	42
	H3 Africa	43
	UK Biobank	43
8.3	Literature	43

2. Executive summary

Background. Remaining liberties that GDPR provides to EU Member States as well as remaining ambiguities on GDPR interpretation keep feeding the debates in the ethical and legal literature. Projects like CINECA, seeking to facilitate health data exchanges between cohorts in Europe, Canada and Africa, offer valuable experience and input on essential ethical and legal gaps between countries and cohorts on questions such as the choice of the ethical lawful basis for international health data sharing and secondary processing for research purposes.

Research questions. The focus of this deliverable will be on answering, both from a legal and an ethical point of view, two priority questions: How to choose a legal basis for CINECA's data processing? And how should CINECA apprehend broad consent to further data processing? The goal will be to study how the CINECA project could be efficiently conducted (especially data sharing) while being legally compliant with relevant laws and regulations and most of all, being compliant with established ethical guidelines and practices across three continents.

Method. The research has consisted in reviewing GDPR provisions and their institutional sources of interpretation; the corresponding legal and ethical literature; the National laws relevant for the cohorts involved in CINECA as well as cohorts' internal governance frameworks and privacy policies when available.

Results. Research has shown that protecting decisional vulnerability in GDPR is so demanding that it seems almost impossible to obtain a specific and freely given consent for lawful further data processing in the context of CINECA. It has also shown that, even though GDPR offers legal exemptions for data processing for scientific research purposes, universities, research organisations and consortia, including in CINECA, are wary to use it for ethical reasons related to the absence of consent, and because of the fear of legal irregularities. Although debated, broad consent is allowed in GDPR for secondary use of data for research purposes in several countries and has also been widely used before in most CINECA cohorts. Researchers are thus drawn to the use of broad consent, but the latter does not fit in the legal basis of "explicit consent" which needs to be specific, and does not (at first glance) fit with the research exemption which is stigmatised for not requiring consent at all, specific nor broad. The practicalities of the use of broad consent for secondary data processing thus still have to be supported by official European guidance.

Recommendation. Use the research exemption as a lawful basis for secondary data processing; Add broad consent as an appropriate safeguard for data subjects' rights; Restrict

the use of the research exemption to research conducted in the “public interest” as defined by National laws.

Limitations. There have been some difficulties gathering information because each CINECA cohort has different sets of guidelines, different approaches to governance, as well as variable levels of governance transparency. Additionally, each country has its own legal and regulatory framework. Frequently, they do not overlap sufficiently for comparison, or when they do, the level of detail is very different for each topic. Another difficulty lies in the fact that many of those data protection laws, national or regional, have been enacted or updated very recently. As a consequence, institutional implementation guidelines are often still missing, as insufficient time has passed for researchers to gather experience, critically analyse, and publish research results or produce documentation for compliance. A last difficulty is related to contradicting interpretations of GDPR, on unclear or debated provisions but most of all, on provisions that are intentionally left for Member States to decide for their own territory. In this regard, National laws can always enact stricter rules regarding the processing of genetic and health related data, while remaining GDPR compliant.

Further work. This deliverable also briefly describes the research that has started on fairness and benefit sharing aspects and on data transfers outside of the European Union.

3. Abbreviations

A29WP	Article 29 Working Party
CHILD	Canadian Healthy Infant Longitudinal Development
CJEU	Court of Justice of the European Union
CLSA	Canadian Longitudinal Study on Aging
CINECA	Common Infrastructure for National Cohorts in Europe, Canada, and Africa
DPA	Data Protection Act
DPO	Data Protection Officer
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EGCUT	Estonian Genome Centre of the University of Tartu
FAIR	Findable, Accessible, Interoperable, Reusable
GA4GH	Global Alliance for Genomics and Health
GDPR	General Data Protection Regulation
H3Africa	Human Heredity and Health in Africa
HRA	Health Research Act
HRO	Health Research Ordinance
OECD	Organisation for Economic Co-operation and Development (OECD)
PIPEDA	Personal Information Protection and Electronic Documents Act
POPIA	Protection of Personal Information Act
TCPS	Tri-Council Policy Statement
UKBB	United Kingdom Biobank

4. Scope

4.1 Territorial scope

4.1.1 European law

4.1.1.1 Direct applicability of GDPR in EU Member States laws

The legal scope of this analysis will include the study of the text of Regulation (EU) 2016/679 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 data¹, more generally known as the **General Data Protection Regulation** (GDPR). The institutional interpretation thereof will also be taken into account, notably from European bodies such as the Court of Justice of the European Union (CJEU), the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS) and the Article 29 Working Party (A29WP).

GDPR is directly applicable in EU Member States, including the **Netherlands** and **Estonia**, where several CINECA cohorts are based: BIOS and LifeLines in the Netherlands, and the Estonian Biobank of the University of Tartu in Estonia. As explained in deliverable 9.9, 7.4² as well as in 9.10 - the ethics report submitted for the first reporting period of the CINECA project, GDPR-compliance of the activities of the three cohorts that are located in an EU Member State (BIOS, LifeLines and Estonian Biobank) remain the responsibility of their own Data Protection Officers. The Netherlands have issued the GDPR Implementation Act³ which has been applicable since 1st January 2020. In Estonia, provisions from GDPR were added thanks to the new Personal Data Protection Act that was adopted in December 2018 and has been applicable since 1st January 2019, together with its Implementation Act adopted in February 2019 which entered into force on 15 March 2019⁴.

4.1.1.2 GDPR compliance of European National laws outside of EU

The **United Kingdom's Data Protection Act**⁵ (DPA) of 2018 was elaborated to enact GDPR provisions⁶ and will be applicable for the cohort UK Biobank. The UK Government has issued the Keeling schedules, showing the differences between GDPR and the UK DPA as amended in 2019 in prevision of Brexit⁷. The free flow of data is still allowed during the transition

¹ 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.

² Kerry G *et al.* CINECA: Data Management Plan v.1 ([Version v.1](#)), 2019.

³ The Netherlands, [Uitvoeringswet Algemene verordening gegevensbescherming](#), 1.1.2020. (and [unofficial translation](#)).

⁴ Estonia, [Personal Data Protection Act](#) (entered into force on 15 January 2019); and its [Implementation Act](#) (entered into force on 15 March 2019).

⁵ United Kingdom, [Data Protection Act \(DPA\)](#) c. 12 of 2018.

⁶ Dove ES & Chen J. "[Should consent for data processing be privileged in health research? A comparative legal analysis](#)". *International Data Privacy Law* 2020, 10(2):117-131 (p. 122).

⁷ UK. Department for Digital, Culture, Media & Sport. [Keeling Schedule for Data Protection Act 2018](#), January 2019.

period before Brexit (until 31 December 2020). UK Government is currently seeking an adequacy decision from the European Commission in order for this free flow to continue after the transition period⁸.

A partnership between UK Biobank and the European Genome-phenome Archive (EGA) has been developed by the European Bioinformatics Institute (EMBL-EBI) together with the Center for Genomic Regulation (CRG). EMBL-EBI, as an international institution, is not subject to EU law. However, it has already ensured that any data processing is compliant with GDPR and has made the analysis results available online⁹.

Lastly, **Switzerland** is also among the non-EU yet European countries involved in CINECA with the cohorts CoLaus and PsyCoLaus. Swiss law is compliant with GDPR as it benefits from an adequacy decision from the European Commission: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland¹⁰. Reference to its **Human Research Act**¹¹ (HRA) and **Human Research Ordinance**¹² (HRO) of 2011, entered into force in 2014, will be included when relevant, as it is sometimes more precise or stricter than GDPR, for instance on genetic data (see below section 5.2.3.2).

4.1.2 Canadian law

The Personal Information Protection and Electronic Documents Act¹³ (**PIPEDA**) is not applicable to CINECA because the Canadian cohorts are publicly funded whereas PIPEDA only applies to the private sector or to organisations that engage in commercial activities.

The other potentially relevant Federal law is the **Privacy Act**¹⁴, which does not specifically apply to health research. In fact, it only applies to “the government’s collection, use, disclosure, retention or disposal of personal information in the course of providing services such as: old age security benefits, employment insurance, border security, federal policing and public safety, tax collection and refunds”.

⁸ Website of the Information Commissioner Office of the UK, <https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/what-does-adequacy-mean/>, last accessed 25 November 2020.

⁹ EMBL Website, “Data protection at EMBL”, [online](#) (last accessed 20 October 22).

¹⁰ [Commission Decision of 26 July 2000](#) pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland.

¹¹ Federal Act on Research involving Human Beings ([Human Research Act, HRA](#)) of 30 September 2011.

¹² Ordinance on Human Research with the Exception of Clinical Trials ([Human Research Ordinance, HRO](#)) of 20 September 2013.

¹³ Government of Canada, Personal Information Protection and Electronic Documents Act ([PIPEDA](#)), S.C. 2000, c. 5.

¹⁴ Government of Canada, [Privacy Act](#), R.S.C., 1985, c. P-21.

The CHILD cohort as well as CLSA are based in the province of Ontario where the **Personal Health Information Protection Act**¹⁵ applies. A practical **Guide**¹⁶ has also been elaborated to help its interpretation.

CARTaGENE is based in Québec, where the 1982 provincial **Act respecting Access to documents held by public bodies and the Protection of personal information**¹⁷ applies.

Funders of public research in Canada are also requesting compliance with **Tri Council Policy guidelines**¹⁸ in order to receive funding. Additionally, the Canadian Institutes of Health Research (CIHR) has issued **Best practices for protecting privacy in health research**¹⁹.

4.1.3 African law

H3Africa is a consortium of more than 500 researchers spread through over 30 African countries, which coordination centre is based at the University of Cape Town (SA). South Africa's long-awaited data protection law, the Protection of Personal Information Act (**POPIA**) n°4 of 2013²⁰, came into effect in July 2020. The South African Ministry of Health issued a standard "Material Transfer Agreement of Human Biological Materials" which parties are compelled to use for any transfer out of, into or within South Africa²¹ and which might have consequences on potential data transfer agreements as well.

Still, each research project has control over its own data and is restricted by its own National law. Significantly, the African Academy of Sciences has established a new Data and Biospecimen governance committee for Africa, with the goal to "create the continent's first cross-disciplinary guidelines for collecting, storing and sharing data and specimens" in a way that would both protect individual data subjects and research participants and benefit African citizens in general²². Although these guidelines would not be legally binding, they would most likely influence research policies as the African Academy of Sciences seems to hold "significant political clout on the continent" and gathers senior government officials, bioethicists, data specialists, legal experts as well as patient organisations and community representatives²³.

¹⁵ Personal Health Information Protection Act (**PHIPA**), 2004, S.O. 2004, c. 3, Sched. A.

¹⁶ Information and Privacy Commissioner for Ontario, [A guide to the Personal Health Information Protection Act](#), December 2004.

¹⁷ Québec, [A-2.1](#). Act respecting Access to documents held by public bodies and the Protection of personal information, 1982.

¹⁸ Government of Canada, Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council. Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – [TCPS 2](#) (2018).

¹⁹ Canadian Institutes of Health Research (CIHR), [Best Practices for Protecting Privacy in Health Research](#), September 2005.

²⁰ South Africa, Protection of Personal Information Act (**POPI Act/POPIA**), assented by Parliament on 19 November 2013, commencement date proclaimed by the President of South Africa for 1 July 2020.

²¹ Thaldar D. "[One material transfer agreement to rule them all? A call for revising South Africa's new standard material transfer agreement](#)", *Humanities and Social Sciences Communications* 2020, 5(105):1-5.

²² Nordling L. "[Africa's science academy leads push for ethical data use](#)", *Nature* 2019, 570:284-285.

²³ *Ibid.*

4.2 Material scope

4.2.1 “Personal data” in the scope of GDPR

4.2.1.1 Pseudonymised data is personal data protected by GDPR

As GDPR does not distinguish between anonymous and anonymised data, identifiable data that is later anonymised will be excluded from the scope of GDPR. Pseudonymised data is personal data if it can re-identify the subject through data linkage – which will be very difficult to coordinate when data exchanges happen between countries, where some of them consider pseudonymised data not to be personal data²⁴. This wide interpretation of personal data in GDPR creates difficulties for instance for biobanks who do not possess the key to their coded data (and are sometimes contractually bound not to search for access to the key). They have to adapt their practice because privacy law regimes are now applicable to their activity as they consequently have to demonstrate a lawful basis to process personal data, all of which constitute obstacles to “routine banking and secondary uses of key-coded personal data”²⁵. According to Art 4.5 GDPR, the key “is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.

Article 4(1) GDPR: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Article 4(5) GDPR: ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

4.2.1.2 Anonymised data falls outside of GDPR

A previous ruling by the Court of Justice of the European Union (CJUE) suggested that it was possible for data to be considered anonymised even if the key to the coded-data would still exist, if there would be enough legal constraints on access to this key. In Breyer²⁶, the Court considered the data to be “identifiable” coded data because the key was accessible by legal means – even if in a very restrictive situation of a cyber-attack. Hence, in theory,

²⁴ Shabani M & Borry P. “[Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation](#)”. *European Journal of Human Genetics* 2018, 26:149-156.

²⁵ Peloquin D, DiMaio M & Barnes M. “[Disruptive and avoidable. GDPR challenges to secondary research uses of data](#)”, *European Journal of Human Genetics* 2020, 28:697-705, p. 700.

²⁶ CJEU, Second Chamber, 19 October 2016, [C-582/14](#), Patrick Breyer v. Bundesrepublik Deutschland, § 44-46; 49.

pseudonymised data can be considered as falling outside of the scope of GDPR, but in practice only in very unlikely situations where the conditions of access to the key would be more restrictive than in the case of a cyber attack.

GDPR is not applicable to personal data rendered anonymous “in such a manner that the data subject is not or no longer identifiable” by “means reasonably likely to be used” taking into account the time, the costs and the technological possibilities (see figure 1 below). As a consequence, it is not applicable to anonymised, anonymous data, nor aggregated data.

However, it needs to be assessed if data can be anonymised and still yield scientifically meaningful results²⁷.

Recital 26 GDPR:

(...) To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

²⁷ Sariyar M & Schlünder I. “[Reconsidering anonymization-related concepts and the term ‘identification’ against the backdrop of the European legal framework](#)”. *Biopreservation and Biobanking* 2016, 14(5):367-374.

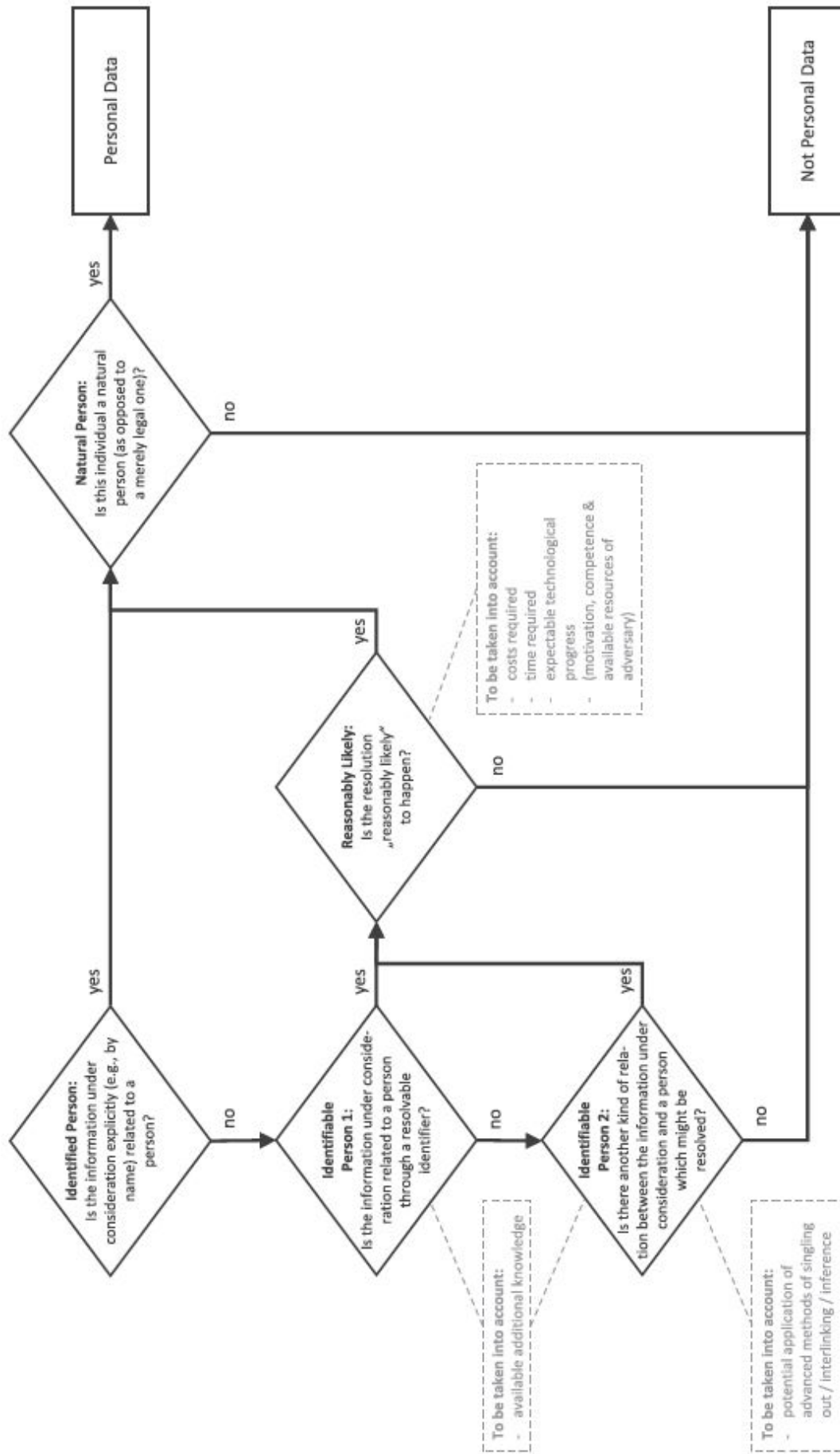


Figure 1 Assessment scheme for person-relatedness of data under the GDPR

28

4.2.1.4 When anonymised data falls back into GDPR

Methods of data linkage enable researchers to bring together several sets of data relating to the same individual or group of individuals and “connect the dots”, enhancing the possibility of discovering new research findings²⁹. Such processes could permit the re-identification of anonymised data, and thus make the data fall back into the scope of GDPR.

For aggregate data, guidance can be found in the European statistics code of practice³⁰, in particular, under principle 5 on statistical confidentiality and data protection. For aggregate data not to be identifiable, some consideration has to be attributed to a threshold for the minimum number of individuals to be represented in a single category of aggregated data. Depending on the type of data and the context in which it is used, the threshold could be set at 3, 5 or 10 individuals, obliging the removal of any category of aggregated data where the number of individuals is less than this threshold. Furthermore, aggregating single categories about the same individuals, even above the threshold, might not necessarily be sufficient to ensure those individuals cannot be indirectly identified again by combining several categories together.

The relevance of setting such a threshold may have to be assessed on a case by case basis by an expert, but it could be relevant when the research studies specific populations, for instance rare disease patients, for whom data aggregation may not hinder reidentification when there are very few people, even at the National level. Canadian TCPS2 (Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans) emphasises this potential need for further privacy and confidentiality in its Article 9.16 for smaller ethnic communities: “Small indigenous communities are characterised by dense networks of relationships. As a result, coding individual data is often not sufficient to mask identities, even when data are aggregated. Some indigenous participants are reluctant to speak to interviewers from their own community because of privacy concerns. Communities themselves have distinguishing characteristics, which in some cases has compromised efforts to disguise the research site, and has led to the stigmatisation of entire communities”³¹.

Even beyond these specific illustrations of rare diseases or indigenous communities, genomic and genetic data have a much higher potential of re-identifiability than health data in general³². It is reasonable to doubt whether genomic data can ever be truly anonymised,

²⁸ Fink M & Pallas F. [“They who must not be identified – distinguishing personal from non-personal data under the GDPR”](#). *International Data Privacy Law* 2020, 10(1):11-36.

²⁹ Baker D, Knoppers BM, Philipps M, van Enckevort D, Kaufmann P, Lochmuller H & Taruscio D. [“Privacy-preserving linkage of genomic and clinical data sets”](#), *IEEE/ACM Trans Comput Biol Bioinform* 2019, 16(4):1342-1348.

³⁰ Eurostat, [European statistics code of practice](#) for the National Statistical Authorities and Eurostat (EU statistical authority), adopted by the European Statistical System Committee, 16th November 2017.

³¹ TCPS2 <https://ethics.gc.ca/eng/documents/tcps2-2018-en-interactive-final.pdf>, p.127.

³² von Thenen N, Ayday E & Cicek AE. [“Re-identification of individuals in genomic data-sharing beacons via allele inference”](#). *Bioinformatics* 2019, 35(3):365-371; Rocher L, Hendrickx JM & de Montjoye Y-A. [“Estimating the success of re-identifications in incomplete datasets using generative models”](#). *Nature Communications* 2019, 10(3069):1-9.

especially as the available technologies will continue to evolve. Technical recommendations have been formulated by a Task Force on Privacy-Preserving Record Linkage launched in 2016 by the Interdisciplinary Committee of the International Rare Diseases Research Consortium (IRDiRC) in collaboration with GA4GH³³.

4.2.2 “Health” and “genetic” data in the scope of GDPR

CINECA aims to facilitate health data sharing between several cohorts for scientific research purposes. Genetic data as well as data concerning health constitute a “special category of personal data” in the sense of Article 9 GDPR. By principle, processing of such sensitive data is prohibited, but derogations are allowed so that processing is possible when based on one of the exceptional lawful bases (see section 5.1).

Data concerning health

Article 4(15) GDPR: ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Recital 35 GDPR: “Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test”.

In GDPR, genetic and health related data benefit from the same protective regime. Swiss law on the contrary attributes two distinctive regimes, the protection of genetic data being stricter. The specificity of genetic data is justified for two related reasons: the difficulties to irreversibly de-identify it³⁴ and the high potential of genomic medicine. As progress in the medical sciences will keep up, and as genetic data has predictive values, Swiss law requires data subjects to be informed before anonymisation of their genetic data. This gives them the opportunity to express their objection to being recontacted while not not impeding potential future clinically relevant findings. Even within the EU, health and genetic data can be subject to stricter national laws impeding data sharing in practice while remaining GDPR compliant (see section 4.3.3).

Genetic data

Article 4(13) GDPR: ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Recital 34 GDPR: “Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained”

³³ Baker D, Knoppers BM, Philipps M, van Enkevort D, Kaufmann P, Lochmuller H & Taruscio D. *op. cit.*

³⁴ Shabani M, Marelli L. “[Re-identifiability of genomic data and the GDPR](#)”. *EMBO Rep* 2019, 20(6):e48316.

4.2.3 Scientific research in contrast with the public interest

The role of scientific research according to GDPR is to provide knowledge that can “improve the quality of life for a number of people and improve the efficiency of social services” (Recital 157 GDPR). As noted by the European Data Protection Supervisor (EDPS), scientific research can be carried out by academic researchers, not-for-profit organisations, governmental institutions as well as commercial companies, within the special data protection regime (referred to later as research exemption) when meeting the following criteria:

“Scientific research is understood to apply where each of the three criteria are met:

- 1) Personal data are processed
- 2) Relevant sectoral standards of methodology and ethics apply, including the notion of informed consent, accountability and oversight
- 3) The research is carried out with the aim of growing society’s collective knowledge and wellbeing, as opposed to serving primarily one or several private interests”³⁵.

All the activities conducted in CINECA’s cohorts fall under this definition of scientific research.

4.3 Limitations

4.3.1 Lack of interoperability given the plurality of normative sources

There have been some difficulties gathering information because each CINECA cohort has different sets of guidelines, different approaches to governance as well as variable levels of governance transparency. Additionally, each country has its own legal and regulatory framework. Most of the time, they do not sufficiently overlap for comparison, or when they do, the level of detail is very different for each topic.

4.3.2 Lack of experience given the recent renewals of most data protection laws

Another difficulty lies in the fact that a lot of those data protection laws, national or regional, have been enacted very recently. As a consequence, institutional implementation guidelines are often still missing, and insufficient time has passed for researchers to gather experience in the application of the laws, to critically analyse them and produce literature (to name a few: GDPR came into effect in 2016 but was implemented in 2018; POPIA was elaborated in

³⁵ European Data Protection Supervisor (EDPS), [A Preliminary Opinion on data protection and scientific research](#), 6 January 2020, p. 11-12.

2013 but applicable from July 2020; the UK DPA dates from 2018; the Swiss DPA is under revision and expected to be passed in 2020).

For instance, helpful guidance is already planned by the European Data Protection Board (EDPB) on the processing of health data for scientific research, as announced in its COVID-19 guideline last April (§43) and as announced by the EDPS when issuing its preliminary opinion on data protection and scientific research, insisting on the fact that constructive criticism would be welcome in order to feed into the future follow up from the EDPB itself³⁶.

4.3.3 Different interpretations of GDPR, yet still compliant

One difficulty in organising international data sharing resides in GDPR itself. As mentioned before, some provisions are still debated and their interpretation is sometimes conflicting. But for many other provisions, GDPR offers an intentional flexibility for Member States to determine their own rules. Contradicting rules about those provisions between Member States would be difficult to solve because they would all still be GDPR compliant.

Among sensitive data listed in Article 9 GDPR, only a few can be subject to stricter National laws according to Article 9.4 GDPR: “Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health”. Thus every difference in Member States’ applications could expectantly constitute a barrier to data sharing while being GDPR compliant.

5. ELSI questions

As also observed by the European Data Protection Supervisor in its January 2020 preliminary opinion³⁷, GDPR interpretation for the scientific community is confusing and as regards to health research often contradictory. In fact, many opposing views can be found on the question of whether the regulation is excessively lenient towards the scientific community³⁸ or on the contrary if “without appreciably improving privacy protections”, unnecessarily complicates its activity notably because of its “ill-considered application to secondary research uses of personal data”³⁹.

For CINECA, the questions won’t be whether GDPR adequately protects data subjects’ rights or promotes scientific research. Rather the goal will be to study how the CINECA project could be efficiently conducted (especially data sharing) while being legally compliant with

³⁶ EDPS, *op. cit.*, p. 6.

³⁷ *Ibid.*, p. 5.

³⁸ Staunton C, Slokenberga S & Mascalzoni D. “[The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks](#)”. *European Journal of Human Genetics* 2019, 27:1159-1167.

³⁹ Peloquin D, DiMaio M & Barnes M. *op. cit.*

relevant laws and regulations and most of all, being compliant with established ethical guidelines and practices across three continents.

The focus of this deliverable will be on answering, both from a legal and an ethical point of view, two priority questions: (5.1) How to choose a legal basis for CINECA's data processing? (5.2) How should CINECA apprehend broad consent to further data processing?; followed by final recommendations (5.3).

5.1 How to choose a legal basis for CINECA's data processing?

5.1.1 Is consent the priority legal basis for health data processing in GDPR?

The processing of personal data in the context of health research can sometimes overlap between several purposes and thus several legal foundations. The European legislator did not specify how to choose the purpose and corresponding legal foundation (nor if combinations are possible)⁴⁰. According to the Directorate-General for Health and Food Safety of the European Commission, the data controller, and thus the sponsor or institution of the investigator, is responsible for choosing and justifying a legal basis for the processing of personal data⁴¹.

As Dove & Chen argue, "a common misperception of modern data protection law, for example, is that data subject consent is a legal obligation for the controller to process the subject's personal data"⁴². This misperception stems "from a normative link that some draw between consent as a research ethics principle and consent as a lawful basis in data protection law"⁴³. Although even the EDPS has recognised that the confusion between the two was understandable, "to view them as a single and indivisible requirement would be simplistic and misleading"⁴⁴, from a legal perspective.

Nonetheless, there are also contradicting interpretations, not on the necessity of obtaining consent *per se*, but on the priority of consent over other lawful bases. Dove & Chen argue that GDPR does not privilege consent as the primary legal basis for processing. On the contrary Hallinan⁴⁵ supports the idea of the existence of an implicit hierarchy in GDPR between the different legal bases: explicit consent (9.2.a GDPR), public interest and public health (9.2.g and i GDPR) and scientific research (9.2.j GDPR). He does so in a moderate way as he also argues for the use of broad consent, as well as for a flexibility in justifying the impossibility to use specific consent and to switch to public interest or scientific research.

⁴⁰ Rage V. "[La base juridique du traitement des données de santé dans le cadre des recherches impliquant la personne humaine](#)". *Panorama de droit pharmaceutique* 2019, 6:163-180.

⁴¹ Directorate-General for health and food safety, (revised) [Questions and answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation](#), 10 April 2019.

⁴² Dove ES & Chen J., *op. cit.*, p. 118.

⁴³ Dove ES & Chen J., *op. cit.*

⁴⁴ EDPS, *op. cit.*, p. 6 & p. 19.

⁴⁵ Hallinan D. "[Broad consent under the GDPR: an optimistic perspective on a bright future](#)". *Life Sciences, Society and Policy* 2020, 16:1 (p. 6).

Interestingly, GA4GH's consent policy explicitly prioritises broad consent over research exemption⁴⁶. However this is only possible because the consent referred to is broad. Such a policy is untenable if the consent had to be specific and thus repeated for each new research project. The question of broad consent will be developed in section 5.2 of this deliverable.

5.1.2 Is “explicit consent” to health data processing an attainable standard?

Some argue that consent for health data processing should be sought simultaneously with research consent, but others argue that research ethics consent should be clearly distinguished from data processing consent. This distinction is particularly important considering the demanding requirements for a valid consent to health data processing in GDPR. According to the Article 29 Working Party (A29WP)⁴⁷, the European Data Protection Board (EDPB)⁴⁸, the European Data Protection Supervisor (EDPS)⁴⁹ as well as the Directorate-General for Health and Food Safety of the European Commission⁵⁰, obtaining a “freely given” consent is very restrictive as it implies that the participants should have a “real choice and control”. A clear situation of imbalance of powers between the participant and the sponsor/investigator will imply that the consent is not freely given in the meaning of the GDPR: this is for instance the case when a participant belongs to an economically or socially disadvantaged group or in any situation of institutional or hierarchical dependency.

This high standard for valid consent will be particularly demanding for all cohorts, for instance when they are focused on vulnerable groups such as the CHILD cohort, CLSA (older adults) or H3Africa (when with economically disadvantaged participants). The H3Africa guidelines for informed consent⁵¹ emphasise the particular challenges informed consent represents as most participants may lack education, wealth, literacy and health care access. Western focus on autonomy and informed consent might not be in line with the more communitarian perspective of most participants. The problem of literacy is especially important as it renders academic debate irrelevant. Thus the guidelines highlight the need of wider community engagement to identify and discuss ethical aspects.

Moreover, European jurisprudence may dissuade the choice of consent as a lawful basis. The Court of Justice of the European Union rule that valid consent cannot be used in the form of pre-ticked boxes but rather, should consist in an “active behaviour with a clear view on the part of the data subject with a view to giving his or her consent”⁵². Similarly, the EDPB recently emphasised the problems triggered by the lawful basis of consent in the context of

⁴⁶ Global Alliance for Genomics and Health. [Consent Policy](#), POL 002 / v 2.0: September 2019, p. 4.

⁴⁷ A29WP, [Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017](#), as last revised and adopted on 10 April 2018, WP259 rev.01.

⁴⁸ EDPB, [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020; EDPB, [Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation \(CTR\) and the General Data Protection Regulation \(GDPR\) \(art. 70.1.b\)\)](#), adopted on 23 January 2019.

⁴⁹ EDPS, *op. cit.*

⁵⁰ Directorate-General for health and food safety, *op. cit.*

⁵¹ H3 Africa, Guideline for informed consent, July 2017, p. 3.

⁵² CJEU, Grand Chamber, 1st October 2019, [C-673/17](#), Planet49.

the Covid-19 pandemic⁵³ as it also means that consent can be withdrawn at any time and the data then has to be deleted (§22). As a consequence, and as the A29WP and EDPB had already noted, consent will not be the appropriate legal basis for most cases.

5.1.3 Is “public health” a suitable basis for research activities?

On the contrary, when using the legal basis of the “public interest in the field of public health” in conformity with Article 9.2.i GDPR, it won’t be necessary to obtain consent from the data subject for the processing of his or her personal data. However, data subject’s rights will still have to be guaranteed and respected, which includes enabling the technical and feasibility measures of respecting the right to access, to rectification, or to limitation of processing.

Although this might seem more suitable for scientific research than the consent basis (for which further rights have to be guaranteed, notably the right to erasure, the right to data portability and the right to object), serious obstacles might still exist. In fact, in contrast with the research exemption (see below section 5.1.4), there will be no presumption of compatibility of purposes for the secondary processing of personal data. Health data sharing within CINECA would thus have to go through a “compatibility test” as foreseen in Article 6.4 GDPR. Yet the latter includes assessment of potentially blocking elements, like the nature of personal data notably if it is sensitive data (Article 6.4.c) and most importantly “the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller” (Article 6.4.b). The risk is thus to face similar restrictions as for the obtention of a “free” consent as the A29WP and the EDPB seem to have a very broad understanding of “situations of imbalance of power”⁵⁴. On the contrary, the research exemption includes a presumption of compatibility of purposes.

5.1.4 Is GDPR pushing towards the scientific (health) research exemption?

GDPR offers other lawful bases that can serve as equal alternatives to consent or public interest, especially the “privileged” position of scientific research.

First of all, according to Article 5.1.b, further processing of personal data for scientific research “shall not be considered to be incompatible with initial purposes”, which means that no “compatibility test” will have to be conducted for secondary use of data.

Second of all, this legal basis releases researchers from having to respect certain obligations. They won’t have to obtain consent and they will also be able to restrict such rights as the right to erasure and to data portability as described in Articles 17.3.d and 20.3 GDPR. Last but not least, Article 89.2 GDPR allows national laws, when they deem it necessary, to restrict other data subject rights for the purpose of scientific research: right of access, right

⁵³ EDPB, [Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak](#), adopted on 21 April 2020, §22.

⁵⁴ EDPB, Guideline 05/2020, *op. cit.*, p. 7.

to rectification, right to restriction of processing, right to object (Articles 15, 16, 18 and 21 GDPR). The Estonian Data Protection Act has implemented those exact restrictions (in Chapter 1, §6(6); whereas Dutch GDPR Implementation act has only chosen to apply restrictions to the first three : right of access, right to rectification, right to restriction of processing, (Articles 15, 16, 18 GDPR; Article 44 Dutch Implementation Act).

Hence, the almost unreachable standards of getting a free and informed consent for health data processing, combined with the attractiveness of relying on the legal basis of scientific research can lead to the conclusion that GDPR pushes the scientific community to use the research exemption. Yet the scientific community seems confused by the “sudden” unnecessary of obtaining (broad) consent and the apparent contradiction with a tradition of ethical values.

5.1.5 Is it ethical to use the research exemption?

The actual controversial question concerns, not the legal, but the ethical acceptability of using the other lawful bases for processing data in health research. There are many critics in this respect against GDPR as it “privileges the interests of those conducting health research to too great an extent (...) as there is concern that researchers will *de facto* resort to an alternative lawful basis even when it is relatively easy to obtain consent”⁵⁵, which is especially dangerous as the scientific research exemption can also be used by private/commercial entities. However, the EDPS reminds the rationale behind and the framework for the research exemption:

“It is a common assumption that scientific research is beneficial to the whole of society and that scientific knowledge is a public good to be encouraged and supported. This translates into a form of ‘social contract’, rooted as such in trust. In this context, where trust plays such a crucial role, performing an activity deemed to be research cannot be a *carte blanche* to take irresponsible risks. From a data protection viewpoint, the principles of necessity and proportionality are essential. For a controller to simply claim to process data for the purposes of scientific research is not sufficient (...) Only scientific research performed within an established ethical framework would therefore qualify as activities falling within the special data protection regime”⁵⁶.

5.1.6 Is it ethical NOT to use the research exemption?

Yet on the opposite, some scholars still have doubts about GDPR really permitting international data sharing for research, emphasising the fact that organisations are too cautious to actually use the research exemption: although the possibility is present, “researchers and research institutions in Europe have been reluctant to use it, likely due to

⁵⁵ Dove ES & Chen J., *op. cit.*, p. 129.

⁵⁶ EDPS, *op. cit.*, p. 11 & 16.

fear of the difficulties that may be caused by their national bodies”⁵⁷, and to the fear of the legal and financial sanctions foreseen in GDPR in case of irregularities⁵⁸. The special regime for scientific research affords a flexibility to Member States, however, at this stage, “the full extent of this special regime is not precisely delineated” in national laws and any limitations to fundamental rights will anyway have to be interpreted restrictively⁵⁹.

This reluctance in practice to use the research exemption is considered by some authors⁶⁰, in the context of the current pandemic, as a threat to “undermine COVID-19 research efforts” and on the contrary deem it an “ethical obligation” to use the research exemption clause for COVID-19 in order to be able to support global efforts and seize the chance to show that solidarity is a European value.

However, one can notice that the international scientific community, when issuing ethical guidelines, tends to prioritise the search for consent by principle, and the use of consent waivers by exception when consent has demonstrated to be too difficult to search for and where ethically justified. This is indeed the case in the GA4GH consent policy, about secondary use of health and genomic data only when broad consent was not implemented at the time of collection⁶¹.

5.1.7 Is the research exemption legal in other National laws relevant for CINECA?

5.1.7.1 In Switzerland

In the Swiss HRA, there is a clear hierarchy between the legal bases of consent and research. In fact, by principle, use and further use of health related data should be based on consent, although unlike GDPR, Swiss HRA is a lot more detailed on how demanding the consent should be (Specific consent, broad consent, default consent...). This will be explained at a later point in this deliverable (see below section 5.2.4.2). But consent is the priority legal basis for further use of biological material and health-related personal data (including genetic data Article 3.f HRA) for research (Articles 32 and 33 HRA).

“In exceptional cases”, further use is possible in the absence of informed consent, as foreseen in Article 34 HRA:

- a. “it is impossible or disproportionately difficult to obtain consent or to provide information on the right to dissent, or this would impose an undue burden on the person concerned;
- b. no documented refusal is available; and

⁵⁷ McLennan S, Celi LA & Buyx A. “[COVID-19: Putting the General Data Protection Regulation to the test](#)”. *JMIR Public Health and Surveillance* 2020, 6(2) :e19279.

⁵⁸ Discussions from the CINECA X-WP ELSI Workshop held on 6 November 2020.

⁵⁹ EDPS, *op. cit.*, p. 18.

⁶⁰ McLennan S, Celi LA & Buyx A., *op. cit.*, p. 2.

⁶¹ Global Alliance for Genomics and Health. [Consent Policy](#), POL 002 / v 2.0: September 2019, p. 4.

- c. the interests of research outweigh the interests of the person concerned in deciding on the further use of his or her biological material and data”.

5.1.7.2 In Canada

In the 2005 best practices for protecting privacy, elaborated by the Canadian Institutes of Health Research (CIHR), consent is clearly given a priority by principle (pp. 37-45). TCPS2 foresees consent waivers (chapter 3) and it will be up to the individual research ethics committee to apply the waiver test.

5.1.7.3 In South Africa

POPIA, by principle, prohibits processing of special information, including “health or sex life or biometric information of a data subject” (Section 26, 1)a). Exceptionally, it can be based on another ground, as described in Section 27, 1): a) consent, b) “establishment, exercise or defence of a right or obligation in law”, c) “an obligation of international public law”, d) “historical, statistical or research purposes”, and e) “information (...) deliberately (...) made public by the data subject”.

The interesting thing is that the lawful basis for processing health data for research is the only one that is subject to further conditions. The research exemption is only valid to the extent that (Section 27, 1)d):

- i. “the purpose serves a public interest and the processing is necessary for the purpose concerned; **or**
- ii. it appears to be impossible or would involve a disproportionate effort to ask for consent”,

In both cases, some guarantees have to be in place to “ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent”.

Hence, the research exemption in POPIA seems to be a last resort to process special information for research purposes. The priority basis would be consent; consent would not be necessary if the research proves to adequately serve the public interest; and if it does not serve the public interest or does not adequately do so, then researchers have to prove that asking for consent is unfeasible.

5.1.7.4 In the United Kingdom

Similarly, the UK DPA, (more specifically its section 19, 1§4) requires consent for processing of sensitive data for research, unless it is both in accordance with article 89(1) GDPR (safeguards) AND it is in the public interest. So the research exemption for sensitive data from GDPR is only applicable in the UK if it is also in the public interest, which is quite restrictive. Unfortunately, there is no further information on what can constitute public

interest, but it does exclude commercial research purposes⁶². It should not be interpreted too strictly as “substantial public interest” is another lawful basis (Section 10(1)(b)).

Hence, UK DPA 2018 is even stricter than POPIA as, if researchers cannot prove the public interest of the research, consent has to be the legal basis, without any flexibility if consent is too demanding or impossible to obtain.

5.1.7.5 In the Netherlands

A similar rule has been enacted in the Netherlands, with the supplementary condition of the public interest and a demonstrated impossibility to obtain consent:

“Article 24. Exceptions for Scientific or Historical Research or Statistical Purposes

In view of Article 9(2)(j) of the Regulation, the prohibition on processing special categories of personal data does not apply if:

- a. the processing is necessary for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1) of the Regulation;
- b. the research referred to in point (a) serves a public interest;
- c. requesting explicit consent proves to be impossible or requires disproportionate effort;
- and
- d. adequate safeguards are provided to prevent disproportionate infringement of the data subject's privacy”.

Besides, the Netherlands have stricter rules for genetic data, but Article 28 still allows processing of genetic data for research purposes if it serves a public interest, if adequate safeguards are provided and if it is proven that collecting consent is impossible or requires disproportionate effort.

5.1.7.6 In Estonia

The Estonian Data Protection Act (Chapter 1, §6) also allows processing of sensitive data for scientific research under specific conditions which may be even more restrictive than all previous ones, notably because of the need to comply with three cumulative criteria: impossibility to meet research purposes without the identifying information, overriding public interest and no excessive damage of the data subject’s rights.

Summary of Chapter 1, §6 on the processing of sensitive data for research purposes:

- 1) Only pseudonymised data can be processed for research purposes without the consent of the individual

⁶² Dove ES & Chen J, *op. cit.*, p. 123.

2) De-pseudonymisation is also allowed for scientific research purposes, but the processors have to designate a specific person to be permitted access to the information allowing pseudonymisation.

3) Processing of personal data without consent for scientific research interests is allowed under cumulative conditions:

- purpose cannot reasonably be met if it is de-identified
- overriding public interest
- the scope of obligations of the data subject does not change and his/her rights are not excessively damaged

4) Need for an approval either by an ethics committee, or in the absence thereof, by the Estonian Data Protection Inspectorate.

5.1.8 A suggestion for an ethical research exemption instead of consent

Dove & Chen got inspiration from the South African POPIA and from the British DPA, to propose a compromise: they encourage the search for consent without using the latter as a lawful basis for data processing. This suggestion is quite close to South Africa's POPIA approach: "one does not mandate consent as the lawful basis for processing personal data for health research – but does strongly encourage it – and, in the absence of consent as the lawful basis, requires a public interest justification or justification of impracticability of obtaining consent if one is to avail themselves of advantageous research exemptions"⁶³ :

A 'South Africa+' model would combine the choice it currently provides (public interest justification for forgoing consent or impracticability to obtain consent) with enhanced procedural and substantive safeguards, similar to those stipulated in the GDPR. These safeguards would include technical and organisational measures, such as strongly encouraging anonymisation and pseudonymisation where possible; having a data protection officer in circumstances where the core activities of the controller or the processor consist of processing genomic or health-related data on a large scale; and having a data protection impact assessment undertaken in circumstances where the processing involves new technologies, or, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals. It should also include transparency in the decision-making process such that the controller makes clearly explicit the reasons for which data processing consent is deemed impracticable to obtain or the research purpose serves a public interest, thereby overriding the consent obligation⁶⁴ . The authors deem this approach as achieving the best balance between data subject rights and the promotion of socially valuable health research.

⁶³ Dove ES & Chen J, *op. cit.*, p. 119.

⁶⁴ *Ibid.*, p. 130.

Such a suggestion, requiring the research to promote public interest, had also been formulated by BBMRI-ERIC in 2015 in order to avoid potential abuse or misuse by commercial actors using the research exemption⁶⁵. Similarly, the GA4GH consent policy clearly seems to imply the existence of a hierarchy in the legal basis of consent, putting the necessity to search for consent first, and as a last resort, if appropriate, share anonymised data or even share personal data after authorisation from a competent authority giving consent waiver (§III)⁶⁶. However, a notable difference is that it also includes the use of broad consent whereas acceptability of broad consent in GDPR is debated in the case of sensitive data.

5.2 How should CINECA apprehend broad consent to further data processing?

5.2.1 Once and for all: is broad consent to further health data processing for research purposes acceptable under GDPR?

Although it was not at the beginning of the legislative process, GDPR does, in its final version, contain provisions which seem “tailor made to support broad consent”.

Recital 33 GDPR: “It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose”.

According to A29WP in its guideline on consent, as confirmed later by the EDPB, Recital 33 GDPR has to be interpreted in a stricter way and with a higher degree of scrutiny when it concerns processing of special categories of data from Article 9 GDPR, as is the case in CINECA. A29WP seems to require that consent must be sought as soon as the new research project design is final and “before that next stage begins”⁶⁷.

This opinion from the A29WP has been criticised as it “downplays Recital 33 to the point of becoming nearly non-existent and hence showing an anti-democratic tendency as the legislator inserted that clause in the final text with a purpose”⁶⁸. This was also stated by the European Parliamentary Research Service⁶⁹, who confirms that this opinion from the A29WP

⁶⁵ BBMRI-ERIC. [Position Paper on the General Data Protection Regulation](#). October 2015.

⁶⁶ Global Alliance for Genomics and Health. [Consent Policy](#), POL 002 / v 2.0: September 2019.

⁶⁷ A29WP, *op. cit.*, p. 28.

⁶⁸ Van Veen E-B. “[Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate](#)”. *European Journal of Cancer* 2018, 104:70-80; See also Peloquin D, DiMaio M & Barnes M, *op. cit.*, p. 700.

⁶⁹ European Parliament, Panel for the Future of Science and Technology (STOA), [How the General Data Protection Regulation changes the rules for scientific research](#), PE 634.447, July 2019.

significantly narrows down the possibility of broad consent for research. Refusing broad consent may discourage researchers to rely on consent and just choose another legal basis, otherwise they would need the time and administrative resources to recontact research subjects for each new project. On the contrary the use of broad consent allows researchers to engage in research for which data subjects have been given the opportunity to exercise their autonomy and give consent, without slowing down the progress of health research.

Hallinan argues that the guidelines from the A29WP should not be considered as narrowing down the newly introduced possibility of using broad consent in the GDPR, and that the use of broad consent might be legitimate even under Articles 9.2(a) and 4(11) GDPR requiring specific and explicit consent⁷⁰.

First, he argues that this narrow interpretation from the A29WP is actually meant to protect the data subject, who is clearly disadvantaged by the power imbalance with the data processor, notably when the latter's interests are not aligned with those of the data subject, and especially in the case of commercial organisations or bureaucratic institutions. According to the author, this cautiousness is understandable in such cases, but is not applicable to the scientific community because of the social benefits that might emerge from the permissibility of broad consent: those social benefits may be larger for genomic research than in health research in general, which would justify the more acceptable use of broad consent⁷¹.

Second, he argues that even though EDPB (and before it, A29WP), has the power, according to Article 70 GDPR, to interpret the latter regulation in areas left open by the legislator, it does not mean that its interpretation can go against the initial intention of the legislator. Thus the existence of Recital 33 is the written witness of the intention of the legislator to introduce granularity of consent, witness that, given the controversial debates during the legislative process, cannot be seen as having been introduced without due knowledge of its meaning and consequences on the acceptability of broad consent for scientific research⁷².

5.2.2 Is broad consent in GDPR accompanied by other safeguards?

The EDPS recently confirmed that Recital 33 cannot take precedence over the conditions set for obtaining consent to data processing as described in Articles 4(11), 6(1)a, 7 and 9(2)a GDPR: "when research purposes cannot be fully specified, a controller would be expected to do more to ensure the essence of the data subject rights to valid consent are served, including through as much transparency as possible and other safeguards"⁷³. Interestingly, the EDPS suggests the following solution:

⁷⁰ Hallinan D, *op. cit.*, p. 11.

⁷¹ Hallinan D, *op. cit.*, p. 13.

⁷² Hallinan D, *op. cit.*, p. 13.

⁷³ EDPS, *op. cit.*, p. 18.

“Even where consent is not appropriate as a legal basis under GDPR, informed consent as a human research participant could still serve as an ‘appropriate safeguard’ of the rights of the data subject. Under what conditions such informed consent might be deemed an appropriate safeguard is still unclear. Certainly, innovative forms of consent in research activities, like tiered and dynamic consent, are promising practices that should be further encouraged and developed”⁷⁴.

Besides, even if specific consent would be more precise, broad consent might still be ethically acceptable because GDPR guarantees, in any case, the right to information of the data subject (Articles 13 and 14 GDPR) and the principle of fairness and transparency (Article 5(1)a GDPR). As the EDPS emphasises, “the principles of fairness and transparency echo to a large extent the foundational principles of informed consent in research ethics”⁷⁵, and the right to information as set out in articles 13 and 14 GDPR apply to further processing, even if the purpose is compatible (Article 13(3) and 14(4) GDPR).

5.2.3 Is broad consent ethically acceptable for and to patients?

The practice of research based on deposited biomaterials and related data, in particular the use and sharing of prospectively collected samples and data stored in biobanks, has led to the establishment of broad consent as the preferred model. A major critique was raised on the fact that participants are asked to consent to the use of their donations in yet unknown future research projects, questioning whether this type of consent could be understood as based on *informed* decision-making. While the physical risks for participants are limited, risks related to the future use and sharing of health data in multiple ways and across countries have raised concerns about potential harms related to the protection of privacy. The potentials of research with genomic data, particularly improvements in genetic analysis, has led to a change in the risk profile, especially in regard to re-identifiability and stigmatisation⁷⁶.⁷⁷ In meeting both needs, to enable large-scale research and to protect participants in the long term, it can be argued that “the broad consent model is best, provided it is also deep”⁷⁸, ensuring “a strong and continuous ethical review process, with the specific mandates for proposed research resting on evaluations of whether that research falls within the scope of the broad consent, and continuous provision of information to participants”⁷⁹. Such an approach could be seen as being in line with the information and transparency requirements mentioned before, as it emphasises that ethics, information is not *done* by signing the consent sheet, but that information needs to be understood as a process. Findings from a survey among biobank professionals have shown that informing participants about data

⁷⁴ EDPS, *op. cit.*, p. 20

⁷⁵ EDPS, *op. cit.*, p. 20.

⁷⁶ Kasperbauer T, Gjerris M, Waldemar G & Sandøe P “[Communicating Identifiability risks to Biobank donors](#)”, *Cambridge Quarterly of Healthcare Ethics* 2018, 27:123-136.

⁷⁷ Helgesson G. “[In Defense of Broad Consent](#)”. *Cambridge Quarterly of Healthcare Ethics* 2012, 21(1):40-50.

⁷⁸ Mikkelsen RB, Gjerris M, Waldemar G & Sandøe P. “[Broad consent for biobanks is best – provided it is also deep](#)”. *BMC Medical Ethics* 2019, 20(1):71, p. 2.

⁷⁹ *Ibid.*, p. 9.

sharing and multiple uses of data in the informed consent needs to be improved, together with participant engagement⁸⁰.

Based on these specific conditions of biobank-related research, the use of broad consent has become common practice; however, although the possibility not to use consent at all is offered in GDPR, “giving up consent altogether is likely to be controversial”⁸¹. Some researchers have conducted an empirical study in Germany with more than 500 patients, 75.7% of whom strongly approving the idea of abolishing altogether patient consent for secondary use of data⁸². The authors of the study moderately related these results to the context of the research setting where broad consent is already widely accepted. Still, people who are reluctant to use data without consent should not be disregarded, the authors propose to introduce an opt-out mechanism before sample collection as well as increased transparency and data protection and governance.

Several studies in Canada show a relative trust from patients towards public research, hospitals, university researchers and data institutes. A 2007 study had shown⁸³ that from more than a thousand responders, 32% were in favour of specific consent (for each research use), 29% in favour of broad consent, 24% for a simple notification (and opt out) and 11% felt no consent nor a notification was needed. A 2016 study also showed that, while 41% of their participants were willing to share their health information for specific research projects only, 61% of them felt comfortable with their de-identified health data being shared without consent⁸⁴.

Moreover, there is a risk that repeated requests for consent will lead either to “consent fatigue”, or to routinisation of consenting without reading. This in return, would defy the intention of consent as “freely given”, “specific”, “informed” and “unambiguous”, challenging consent both as the appropriate legal basis for data processing as well as ethical requirement⁸⁵.

Most recently, findings from the large-scale “Your DNA, Your Say” project⁸⁶ provide insights into public (including research participants) attitudes towards sharing of genomic data and health information, and draws on the responses from 36,268 individuals across 22 countries. Results show that the willingness to donate such data as well as trust in data processing

⁸⁰ Goisauf M *et al.* “[Data in Question: A Survey of European Biobank Professionals on Ethical, Legal and Societal Challenges of Biobank Research](#)”. *PLOS ONE* 2019, 14(9):e0221496.

⁸¹ For instance: Gelinis L, Wertheimer A & Miller FG. “[When and why is research without consent permissible?](#)”. *Hastings Cent Report* 2016, 46:9.

⁸² Richter G, Borzikowsky C, Lieb W, Schreiber S, Krawczak M & Buyx A. “[Patient views on research use of clinical data without consent: Legal, but also acceptable?](#)”. *European Journal of Human Genetics* 2019, 27:841-847.

⁸³ Willison DJ. “[Alternatives to Project-specific Consent for Access to Personal Information for Health Research: What Is the Opinion of the Canadian Public?](#)”. *Journal of the American Medical Informatics Association* 2007, 14(6): 706-712.

⁸⁴ Page SA, Manhas KP, and Muruve DA. “[A survey of patient perspectives on the research use of health information and biospecimens](#)”. *BMC Medical Ethics* 2016, 17:48.

⁸⁵ Mikkelsen RB, Gjerris M, Waldemar G & Sandøe P. *op. cit.*; Cambon-Thomsen A. “[The social and ethical issues of post-genomic human biobanks](#)”. *Nature Reviews Genetics* 2004, 5:866-873.

⁸⁶ Middleton A *et al.* “[Global Public Perceptions of Genomic Data Sharing: What Shapes the Willingness to Donate DNA and Health Data?](#)”. *The American Journal of Human Genetics* 2020, 107(4):743-752.

including multiple actors are relatively low. In view of CINECA's aim to share genomic data internationally, the study highlights the importance of developing international policy and practice.

In addition to this finding, previous studies have come to the conclusion that most research participants want to have a say in how their samples and data are used^{87,88}. Re-consent is preferred when the circumstances under which research with their samples and data is performed change^{89,90}. Interviews with breast cancer patients in three European countries showed that half of the interviewees wanted to be asked for re-consent for future research⁹¹. Interactive research settings provide insights into how opinions are built. It has been observed in a study⁹² that assessments of consent models are shaped by concerns about the "appropriateness" of research practice and developments, especially regarding research with genomic data. Whereas complete absence of consent was rejected, the preference for broad consent is constituted as a compromise between the aim to support health research while coping with uncertainty toward samples and data uses, a lack of knowledge about biobanking practices and risks (especially the risk of re-identification), and an unclear future connected to unknown purposes of sample and data use.

Recent discussions about the ethical acceptability of broad consent were related to its use in low and middle income countries, notably in Africa: even if widely used and accepted, some authors argue that it should only be permissible with supplementary safeguards elaborated after "genuine" engagement with the community⁹³ and after explicit discussions, notably potential re-identification of genomic data, benefit sharing and commercial use of research results⁹⁴.

5.2.4 Is broad consent legal in other National laws relevant for CINECA?

5.2.4.1 United Kingdom

In some Member States who did not pass any laws introducing broad consent, it was nevertheless an accepted practice for years, as the author notes, "for example (...) in the

⁸⁷ Mester JL et al. "[Communicating with Biobank Participants: Preferences for Receiving and Providing Updates to Researchers](#)". *Cancer Epidemiology Biomarkers & Prevention* 2015, 24(4):708-712.

⁸⁸ Hemminki E et al. "[Finnish people's attitudes towards biomedical research and its sponsorship](#)". *Genomics, Society and Policy* 2009, 5(2):67-79.

⁸⁹ Kaye J, Whitley EA, Lund D, Morrison M, Teare H & Melham K. "[Dynamic consent: a patient interface for twenty-first century research networks](#)", *European Journal of Human Genetics* 2015, 23:141-146.

⁹⁰ Budin-Ljøsne I et al. "[Feedback of Individual Genetic Results to Research Participants: Is It Feasible in Europe?](#)", *Biopreservation and Biobanking* 2016, 14(3):241-248.

⁹¹ Petersen I, Desmedt C, Harris A, Buffa F & Kollek R, "[Informed consent, biobank research, and locality: perceptions of breast cancer patients in three European countries](#)", *Journal of Empirical Research on Human Research Ethics* 2014, 9(3):48-55.

⁹² Goisau M & Durnová A. "[From Engaging Publics to Engaging Knowledges: Enacting "Appropriateness" in the Austrian Biobank Infrastructure](#)". *Public Understanding of Science* 2018, 28(3):275-289.

⁹³ Tindana P & De Vries. "[Broad Consent for Genomic Research and Biobanking: Perspectives from Low- and Middle-Income Countries](#)". *Annual Review of Genomics and Human Genetics* 2016, 17:2.1-2.19.

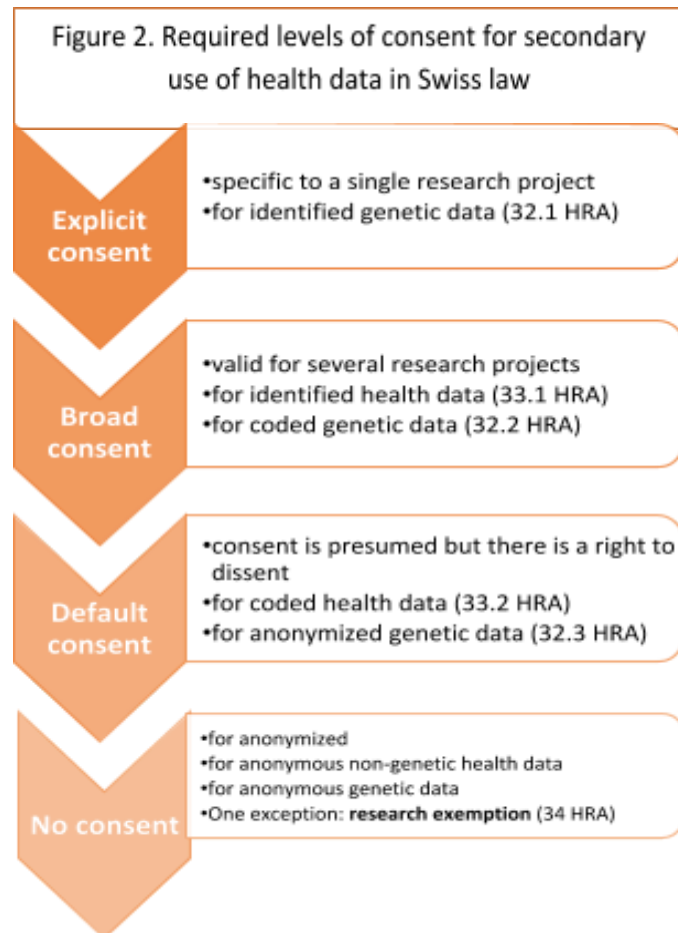
⁹⁴ Moodley K & Kleinsmidt A. "[Allegations of misuse of African DNA in the UK: Will data protection legislation in South Africa be sufficient to prevent a recurrence?](#)". *Developing World Bioethics*, First published 7 August 2020.

high-profile genomic research infrastructure project UK Biobank⁹⁵. It was later backed as well in law thanks to the Human Tissue Authority's 2017 guideline on consent (for the Human Tissue Act of 2004, p. 11).

5.2.4.2 Switzerland

Martani et al. criticised the exceptionally strict regime that Swiss law grants to genetic data⁹⁶, as summarised in Figure 2. By principle, broad consent in Swiss law can only allow for secondary use of genetic data when it is at least coded or pseudonymised. The HRA provides for an exception for research, which yet seems restrictive as the following criteria have to be met:

“a. it is impossible or disproportionately difficult to obtain consent or to provide information on the right to dissent, or this would impose an undue burden on the person concerned; b. no documented refusal is available; and c. the interests of research outweigh the interests of the person concerned in deciding on the further use of his or her biological material and data” (Article 34 HRA).



The Swiss lawmaker granted this stricter regime to genetic data because of the high re-identifiability potential of genetic data. Martani et al. however argue against these “unequal normative standards” for data reuse saying that although genetic data is highly sensitive, other health related but non-genetic data can be at least as sensitive because new technologies allow to easily re-identify non-genetic data. “Therefore, from the “perspective of data subjects’ privacy, it would seem more appropriate that a distinction (if any) in regulatory requirements for secondary use were based on the degree of sensitiveness of personal data, or simply on the degree of de-identification, rather than on the genetic or non-genetic nature of the data themselves”. The sensitivity of the data should also be appreciated depending on “whether the data are shared and reused cross border; 2) whether the data were initially collected under a strong assumption of confidentiality (e.g.

⁹⁵ Hallinan D, *op. cit.*, p. 14.

⁹⁶ Martani A et al., “Regulating the secondary use of data for research: arguments against genetic exceptionalism”, *Frontiers in Genetics* 2019, 10:1254.

medical history or notes taken during a psychotherapy); 3) what conditions there are for allowing reuse by third parties, especially industry”⁹⁷.

5.2.4.3 Africa

According to the **H3Africa guidelines for consent**, “**broad consent**” is the default form of consent for the consortium (p. 7), while denying the critics of broad consent being a “blanket consent”. On the contrary, it has to be demonstrated that broad consent is accompanied by an agreement so that data sharing is always made in compliance with consent, for instance having a data access committee or research ethics committee to assess and validate data access (p. 10). In this context, the broad consent model seems to be the preferred and recommended model in African research studies.

A more specific version of broad consent is the model of “**tiered consent**” where the patient is invited to choose between several options (no further sharing, sharing for research on the same medical condition or sharing for any medical research).

H3 Africa guidelines for consent, p. 11:

An example of a tiered or layered consent option is the following:

“Tick the option you choose:

I do not want my sample to be shared with other scientists.

OR

My sample can be shared with other scientists for research in a field related to [describe the field of your study, e.g. cardiovascular research].

OR

My sample can be shared with other scientists for health research in any field.”

And in fact, research has shown that most research projects conducted in the H3Africa consortium tend to use broad consent: out of nineteen H3Africa projects, seven use broad consent, five used tiered consent whereas only one used specific consent⁹⁸.

Yet the question of the legal acceptability of broad consent in recently applicable **POPIA** is not that clearly positive⁹⁹. According to section 13(1) of **POPIA**, “Personal information must be collected for a specific, explicitly defined and lawful purpose”. Further processing or secondary use is possible but it has to be compatible with the initial purpose (Section 15(1)), compatibility being assumed in two relevant cases for CINECA and only when the data subject has consented to further processing (Section 15(3)a):

- For research purposes when results are not published in an identifiable form (Section 15(3)e), which might be problematic notably for genomic information, which is inherently identifiable¹⁰⁰
- For research purposes, even when published in an identifiable form if the public interest, the data subject’s benefits or a third party’s benefits “outweighs, to a

⁹⁷ Martani A *et al.*, *op. cit.*

⁹⁸ Munung NS *et al.* “[Obtaining informed consent for genomics research in Africa: analysis of H3 Africa consent documents](#)”. *Journal of Medical Ethics* 2016, 42:132-137.

⁹⁹ Nordling L. “[South African law may impede human health research](#)”. *Science* 2019, 363(6429):802.

¹⁰⁰ Staunton C *et al.* “[Safeguarding the future of genomic research in South Africa: Broad consent and the Protection of Personal Information Act No. 4 of 2013](#)”. *S Afr Med J* 2019, 109(7):468-470.

substantial degree”, the interference with privacy (Section 15(3)f combined with Section 37(1&2)), which might also be difficult to demonstrate.

As a consequence, broad consent can definitely be deemed as legally acceptable for further processing of health data in South African law, but it is subject to stricter safeguards when the health data is genomic data because of its high identifiability.

5.2.4.4 Canada

The CHILD governance framework definitely foresees the use of broad consent as it specifies that consent forms should include clauses allowing, among others, “international data sharing; (...); Access to patient-level coded data, including genomic/omic and phenotypic data, and biological samples, under a controlled-access mechanism; Use of data and/or biological samples for future health research into the early-life origins of many conditions which affect children, adolescents and adults, subject to the controlled access process and ethical requirements; potential use of data and/or biological samples for commercial purposes (...)” (p. 17). Specific consent is also foreseen, notably the conditions under which a participant can be re-contacted for a new specific project (p. 20).

By principle, in the Ontario PHIPA, if the purpose of health data sharing is not related to treatment, consent from the data subject has to be expressed. However, consent is not always necessary, and notably for the purpose of research and as long as certain requirements are met (previous approval from a research ethics board for instance)¹⁰¹.

According to the Article 5.5.A of **TCPS2**, informed consent is not the only option to justify further processing. Unless the research “relies exclusively on the secondary use of non-identifiable information” (Article 5.5.B TCPS2), researchers have to demonstrate (all requirements have to be satisfied) to the ethics committee that:

- a. “identifiable information is essential to the research;
- b. the use of identifiable information without the participants’ consent is unlikely to adversely affect the welfare of individuals to whom the information relates;
- c. the researchers will take appropriate measures to protect the privacy of individuals and to safeguard the identifiable information;
- d. the researchers will comply with any known preferences previously expressed by individuals about any use of their information;
- e. it is impossible or impracticable (see Glossary¹⁰²) to seek consent from individuals to whom the information relates; and

¹⁰¹ Information and Privacy Commissioner for Ontario, [A guide to the Personal Health Information Protection Act](#), December 2004., p. 11, p. 20 & p. 28.

¹⁰² “ ‘impracticable’ refers to undue hardship or onerousness that jeopardizes the conduct of the research; it does not mean mere inconvenience”.

- f. the researchers have obtained any other necessary permission for secondary use of information for research purposes”.

5.3 Conclusive recommendation

In most cases, relying on the research exemption might be the more realistic and appropriate lawful basis to choose for CINECA¹⁰³, while still developing broad/tiered consent as a more ethical approach and as an “appropriate safeguard” to data subjects’ rights, together with increased efforts to comply with the principles of “fairness and transparency” e.g. by increasing efforts to inform data subjects or by limiting research activities to those promoting public interest, as summarised in the table below.

Table 1: Summary comparison of the legal bases available under GDPR for data sharing and secondary use, the protection regime each one provides to the data subjects, and the recommendation for CINECA.

Lawful basis in GDPR	Explicit consent	Public interest in the field of public health	Scientific research
Consent	<p>Consent has to be specific to each research project (i.e. broad consent is not possible)</p> <p>Consent has to be “freely” given (strict interpretation of EDPB regarding the relation between data subject and data controller)</p>	No consent is necessary	<p>No consent is necessary</p> <p>Broad consent is possible</p>
Compatibility of purposes for further data processing	Automatic compatibility of research purposes	No presumption of compatibility of purposes. Compatibility test to demonstrate (including the relation between data subject and data controller as interpreted strictly by EDPB)	Presumption of compatibility of purposes
Data subjects’ rights	<p>Transparency</p> <p>Right to information</p> <p>Right to access</p> <p>Right to rectification</p> <p>Right to erasure</p> <p>Right to restriction of processing</p> <p>Right to portability</p> <p>Right to object</p>	<p>Transparency</p> <p>Right to information</p> <p>Right to access</p> <p>Right to rectification</p> <p>Right to erasure</p> <p>Right to restriction of processing</p> <p>Right to portability</p> <p>Right to object</p>	<p>Transparency</p> <p>Right to information</p> <p>Right to access</p> <p>Right to rectification</p> <p>Right to erasure</p> <p>Right to restriction of processing</p> <p>Right to portability</p> <p>Right to object</p>

¹⁰³ Discussions from the CINECA X-WP ELSI workshop held on 6 November 2020 online.

Other			Additional safeguards : - Ethics committee opinion - Restrict to research in the public interest - Pseudonymization - Broad consent
Conclusion			Recommended for CINECA

6. Next steps

6.1 First findings on benefit sharing & FAIRness

Deliverable 7.1 entitled “Catalogue of ELSI issues”¹⁰⁴ as well as discussions during the virtual AGM in March 2020 allowed us to identify benefit sharing and FAIR principles as topics that would be relevant for WP7 to study. More time will be needed to produce an output and provide recommendations to the CINECA community (for instance thanks to the planned webinar in Spring 2021). Yet, first elements are available and already show that African and Canadian legal/regulatory frameworks will constitute valuable sources of input.

6.1.1 Africa

Recently applicable **POPIA** contains a section authorising data processing about the subject’s race or origin only if the latter complies “with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination” (Section 29.1.b).

On a more general level, the **H3Africa guidelines for consent** note the importance of a “robust governance framework that should seek to promote global health and research equity and take into account five key elements: respect, authentic community engagement and trust building, the preservation of privacy and confidentiality, feedback of results, and capacity strengthening” (p. 10).

Finally, the question of benefit sharing, fairness and equity is also being explored by other researchers. An open network has been created in July 2019: “**GO FAIR Implementation Network Africa**” (**GO FAIR IN Africa**) 2019-2020¹⁰⁵. It has been created in order to “help solve the problem of the current extraction of data from the continent without returning benefits” ; to point “to the possibility of a governance of data that will benefit the African continent”; “to root digital data within a philosophy that data are owned by the data

¹⁰⁴ Gennet É & Goisau M. CINECA: Catalogue of ELSI issues [D7.1](#), 2019.

¹⁰⁵ GO FAIR IN Africa, [Manifesto of the FAIR Implementation Network – Africa](#), to establish the Africa connection of the Internet of Data and Services, 2019-2020, 22 July 2019.

subjects” and explore “the contribution that African philosophy can make to the global internet of data and services due to its epistemology of united and collective existence expressed within local realities”.

The African Academy of Sciences has established a new **Data and Biospecimen governance committee for Africa**, with the goal to “create the continent’s first cross-disciplinary guidelines for collecting, storing and sharing data and specimens” in a way that would both protect individual data subjects and research participants and benefit African citizens in general¹⁰⁶. “Even when data-sharing policies are negotiated as part of international partnerships, African scientists might feel unable to push back against the wishes of powerful donors or research partners. African scientists may not question unfair policies for fear of harming their funding chances — and instead simply accept the grants and their inequitable conditions”¹⁰⁷. Discussions on fairness and benefit sharing regarding African data are of utmost importance and currency. As some authors have recently highlighted, there is a long history of allegations of unethical use of African data and material¹⁰⁸, as well as potential repeated misuse and commercialisation of African genetic material¹⁰⁹. The debate actually goes beyond only health data and concerns also more generally the use and sharing of human biological material in Africa¹¹⁰. For instance, the South African Ministry of Health compels researchers to use a Standard Material Transfer Agreement¹¹¹, but literature has been criticising the fact that the latter was “flawed in theory and likely to be inadequate in practice” and thus not suitable to actually promote benefit sharing¹¹².

Moodley & Kleinsmidt, 2020

“Concerns have been raised around the alleged commercialisation of South African genetic material by various research institutes nationally and abroad. We consider whether the Protection of Personal Information Act in South Africa will conflict with or complement existing protections in health law and research ethics. The Act is not applicable to de-identified samples that cannot be re-identified but we question whether genetic samples can ever be truly de-identified. **The research participants in this matter provided consent for use of their samples for research but did not consent to commercialisation by global research institutions, and neither did the researchers. We suggest that consent models incorporating broad consent as an option should include explicit discussions around benefit sharing and commercialisation.** Mistrust between researchers and participants impedes scientific research and can harm relationships built up over the years between South African researchers and local communities.”

¹⁰⁶ Nordling L. “[Africa’s science academy leads push for ethical data use](#)”, *Nature* 2019, 570:284-285.

¹⁰⁷ Nordling L. “[Africa’s science academy leads push for ethical data use](#)”, *Nature* 2019, 570:284-285.

¹⁰⁸ Nienaber A. “[Consent to and authorisation of the export and use of human biological specimens for future research - perspectives from three African countries](#)”. *The Comparative and International Law Journal of Southern Africa* 2011, 44(2):225-254.

¹⁰⁹ Moodley K & Kleinsmidt A. *op. cit.*

¹¹⁰ Stokstad E. “[Major UK genetics lab accused of misusing African DNA](#)”. *Science* 2019.

¹¹¹ South Africa, Government [Notice 719](#), Government Gazette 41781 of 20 July 2018.

¹¹² Thaldar D. “[One material transfer agreement to rule them all? A call for revising South Africa’s new standard material transfer agreement](#)”, *Humanities and Social Sciences Communications* 2020, 5(105):1-5.

6.1.2 Canada: Tri-Council Policy Statement

6.1.2.1 Chapter 4 on “Fairness and equity in research participation”

Chapter 4 of the TCPS2 is exclusively relevant to “**fairness and equity in research participation**”. Its goal is to highlight the (often) inappropriate exclusion of groups of participants, who are excluded from the burdens of participating in research, but who are thus also excluded from all its benefits. “The principle of Justice holds that particular individuals, groups or communities should neither bear an unfair share of the direct burdens of participating in research, nor should they be unfairly excluded from the potential benefits of research participation. Inclusiveness in research and fair distribution of benefits and burdens should be important considerations for researchers, research ethics boards (REBs), research institutions and sponsors” (p. 49). As a consequence, the chapter provides guidance on how to include some groups who have historically often been “inappropriately excluded on the basis of attributes such as culture, language, religion, race, disability, sexual orientation, ethnicity, linguistic proficiency, gender or age”. Article 4.1 prohibits exclusion on those attributes and gives further guidance for several particular groups: women, women in reproductive capacity, pregnant or breastfeeding, children, elderly, people lacking decision making capacity and vulnerable people (vulnerability being assessed from the context, e.g. dependent, poor or institutionalised people).

The equitable distribution of research benefits may be direct for those groups (individual health benefit, training for the local community) or indirect (knowledge about the group to which participants belong) (p. 54).

6.1.2.2 Chapter 9 on “research involving the first nations, Inuit and Métis peoples of Canada”

First nations, Inuit and Metis people’s cultures include “core values such as reciprocity (...) which they advance as the necessary basis for relationships that can benefit both Indigenous and research communities”. In fact, history shows that most research has been carried out by non-indigenous researchers and have not reflected Indigenous world views. The goal now is to “encourage collaboration and engagement between researchers and participants”, considering the “premise that engagement with community is an integral part of ethical research involving Indigenous peoples” (p. 107).

This chapter could easily be extended to other communities than the Inuit and Métis people, as a “community” is defined as a “group of people with a shared identity or interest that has the capacity to act or express itself as a collective. In this Policy, a community may include members from multiple cultural groups. A community may be territorial, organisational, or a community of interest” (p. 109).

The original and interesting perspective of this chapter relies on its collective perspective which contrasts with the traditional principle of “respect for persons” that is usually expressed from an individual participant point of view. On the contrary, emphasis is put on collective rights and welfare (p. 110), and where the welfare of a community is likely to be affected by the research, article 9.1 suggests for researchers to seek engagement and input from the community (Article 9.8-9.12), and for the research to benefit the community, notably through capacity building (Article 9.13-9.14).

6.2 Further cooperation on cross border exchanges

CINECA’s goal is to facilitate transfers of personal health data to/from third countries (i.e. non-EU countries) or international organisations and will thus have to comply with Chapter V GDPR. The ideal option for compliant transfers is when the latter are based on an adequacy decision (Article 45(3) GDPR). As presented in deliverable 9.9, none of the Canadian or African cohorts in CINECA are based in a country benefiting from an adequacy decision; only Switzerland does. CINECA thus has to subject most its transfers to “appropriate safeguards” pursuant to Article 46 GDPR.

Article 46(2) GDPR: appropriate safeguards in the absence of an adequacy decision

- a) legally binding and enforceable instrument
- b) binding corporate rule
- c) standard data protection clauses adopted by the Commission
- d) standard data protection clauses adopted by a supervisory authority and approved by the Commission
- e) approved code of conduct
- f) certification mechanism

In the case where none of the safeguards of Article 46 would be appropriate, there remains the option to, exceptionally, base data transfers outside the EU on derogations foreseen in Article 49 GDPR, including consent and an important reason of public interest. However, this does not seem suited to CINECA activities. The EDPB recently confirmed that derogations for specific situations can only take place as an exception – like in the case of COVID-19 research – and have to be interpreted restrictively, for COVID-19 for instance either on the basis of public interest or on explicit consent¹¹³. Such derogations have nonetheless to be temporary regarding the global emergency, “repetitive transfers of data to third countries part of a long lasting research project in this regard would need to be framed with appropriate safeguards in accordance with Article 46 GDPR”¹¹⁴.

As noted in deliverables 9.9, 7.1¹¹⁵ and 7.4¹¹⁶ (Data Management Plan), CINECA does not grant any automatic data access nor any shortcut. All data access will be governed by a Data Access Agreement between the cohort owner, the principal investigator and the principal investigator’s institute. Yet CINECA will actively participate in promoting knowledge and

¹¹³ EDPB, Guidelines 03/2020, *op. cit.*, §§62-63.

¹¹⁴ *Ibid.*, §§66-67.

¹¹⁵ Gennet É & Goisauf M, *op cit.*

¹¹⁶ Kerry G, *op cit.*

expertise on the matter, both at an internal and an external level, *e.g.* as has been done with the [CINECA Webinar](#) on the code of conduct from BBMRI on 1st October 2020.

Benefit sharing and FAIR/fair aspects will be discussed in 2021 among CINECA partners, and will be the topic of a webinar or workshop from the ELSI point of view in Spring 2021.

CINECA will not propose anything that would be unique to its project but rather offers additional support to existing initiatives. Its input nonetheless offers an original and rare tri-dimensional perspective gathering European, Canadian as well as African partners to other initiatives. The ELSI WP of CINECA are actively participating in the EUCAN collaborative working group on ELSI issues in international health and genomic data sharing.

7. Delivery and schedule

Delivery is on time.

8. References

8.1 Legal instruments, institutional documents

8.1.1 European Union

8.1.1.1 EU Member States law

Estonia, Personal Data Protection Act (entered into force on 15 January 2019); and its Implementation Act (entered into force on 15 March 2019).

The Netherlands, Uitvoeringswet Algemene verordening gegevensbescherming, 1.1.2020. (and unofficial translation).

8.1.1.2 EU Legal instruments

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 (General Data Protection Regulation)

Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304).

8.1.1.3 EU Case Law

CJEU, Second Chamber, 19 October 2016, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland

CJEU, Grand Chamber, 1st October 2019, C-673/17, Planet49.

8.1.1.4 EU Reports

A29WP, Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017, as last revised and adopted on 10 April 2018, WP259 rev.01.

Directorate-General for health and food safety, (revised) Questions and answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, 10 April 2019.

EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020.

EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted on 21 April 2020.

EDPB, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (art. 70.1.b)), adopted on 23 January 2019.

EDPS, A Preliminary Opinion on data protection and scientific research, 6 January 2020.

European Parliament, Panel for the Future of Science and Technology (STOA), How the General Data Protection Regulation changes the rules for scientific research, PE 634.447, July 2019.

Eurostat, European statistics code of practice for the National Statistical Authorities and Eurostat (EU statistical authority), adopted by the European Statistical System Committee, 16th November 2017.

8.1.2 Canada

Government of Canada, Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5.

Government of Canada, Privacy Act, R.S.C., 1985, c. P-21.

Government of Canada, Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council.

Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2018).

Canadian Institutes of Health Research (CIHR), Best Practices for Protecting Privacy in Health Research, September 2005.

Québec, A-2.1. Act respecting Access to documents held by public bodies and the Protection of personal information, 1982.

Ontario:

- Personal Health Information Protection Act (PHIPA), 2004, S.O. 2004, c. 3, Sched. A.
- Information and Privacy Commissioner for Ontario, A guide to the Personal Health Information Protection Act, December 2004.

8.1.3 Africa

South Africa, Protection of Personal Information Act (POPI Act/POPIA), assented by Parliament on 19 November 2013, commencement date proclaimed by the President of South Africa for 1 July 2020.

South Africa, Material Transfer Agreement of Human Biological Materials, Government Notice 719, Government Gazette 41781 of 20 July 2018.

GO FAIR IN Africa, Manifesto of the FAIR Implementation Network – Africa, to establish the Africa connection of the Internet of Data and Services, 2019-2020, 22 July 2019.

8.1.4 Others

8.1.4.1 United Kingdom

Data Protection Act (DPA) c. 12 of 2018.

UK. Department for Digital, Culture, Media & Sport. Keeling Schedule for Data Protection Act 2018, January 2019.

Human Tissue Authority, Code of Practice A, Guiding Principles and the Fundamental Principle of Consent.

8.1.4.2 Switzerland

Federal Act on Research involving Human Beings (Human Research Act, HRA) of 30 September 2011.

Ordinance on Human Research with the Exception of Clinical Trials (Human Research Ordinance, HRO) of 20 September 2013.

Swiss Academy of Medical Sciences (SAMS). Research with human subjects (2015).

8.1.4.3 GA4GH

Global Alliance for Genomics and Health. Consent Policy, POL 002 / v 2.0: September 2019.

8.1.4.4 BBMRI-ERIC

BBMRI ERIC. Position Paper on the General Data Protection Regulation. October 2015.

8.2 CINECA

8.3.1 Relevant previous deliverables

Gennet É & Goisau M. CINECA: Catalogue of ELSI issues D7.1, 2019.

Kerry G *et al.* CINECA: Data Management Plan v.1 (Version v.1), 2019.

8.3.2 Cohorts' internal policies

CARTaGENE

Access and use policy for data and biosamples, March 2018.

Information Brochure for participants. Phase A & Phase B.

Information Brochure for participants. Follow-up. March 2014.

Information Brochure for participants. Environment and nutrition component.

CHILD

Governance Framework. Version 1. November 2019.

CLSA

Data and Biospecimen Access Policy and Guiding Principles, March 2018.

Study Information Package and Summary.

Privacy Policy, November 2012.

EGA

Lappalainen I *et al.* "The European Genome-phenome Archive of human data consented for biomedical research" *Nature Genetics* 2015, 47:692-695.

H3 Africa

Data Sharing, Access and Release Policy, August 2014.

Data and Biospecimen Access Committee Guidelines, July 2017.

Guideline for informed consent, July 2017.

UK Biobank

Access procedures: Application and review procedures for access to the UK Biobank Resource, November 2011.

Ethics and governance framework, October 2007.

8.3 Literature

Baker D, Knoppers BM, Philipps M, van Enckevort D, Kaufmann P, Lochmuller H & Taruscio D. "Privacy-preserving linkage of genomic and clinical data sets", *IEEE/ACM Trans Comput Biol Bioinform* 2019, 16(4):1342-1348.

Budin-Ljøsne I *et al.* "Feedback of Individual Genetic Results to Research Participants: Is It Feasible in Europe?", *Biopreservation and Biobanking* 2016, 14(3):241-248.

Cambon-Thomsen A. "The social and ethical issues of post-genomic human biobanks". *Nature Reviews Genetics* 2004, 5:866-873.

Clayton EW *et al.* "The law of genetic privacy: applications, implications, and limitations". *Journal of Law and the Biosciences* 2019, 6(1):1-36

Dove ES & Chen J. "Should consent for data processing be privileged in health research? A comparative legal analysis". *International Data Privacy Law* 2020, 10(2):117-131 (p. 122).

Fink M & Pallas F. "They who must not be identified – distinguishing personal from non-personal data under the GDPR". *International Data Privacy Law* 2020, 10(1):11-36.

Gelinas L, Wertheimer A & Miller FG. “When and why is research without consent permissible?”. *Hastings Cent Report* 2016, 46:9.

Goisaufl M *et al.* “Data in Question: A Survey of European Biobank Professionals on Ethical, Legal and Societal Challenges of Biobank Research”. *PLOS ONE* 2019, 14(9):e0221496.

Goisaufl M & Durnová A. “From Engaging Publics to Engaging Knowledges: Enacting “Appropriateness” in the Austrian Biobank Infrastructure”. *Public Understanding of Science* 2018, 28(3):275-289.

Hallinan D. “Broad consent under the GDPR: an optimistic perspective on a bright future”. *Life Sciences, Society and Policy* 2020, 16:1.

Helgesson G. “In Defense of Broad Consent”. *Cambridge Quarterly of Healthcare Ethics* 2012, 21(1):40-50.

Hemminki E *et al.* “Finnish people's attitudes towards biomedical research and its sponsorship”. *Genomics, Society and Policy* 2009, 5(2):67-79.

Kasperbauer T, Gjerris M, Waldemar G & Sandøe P “Communicating Identifiability risks to Biobank donors”, *Cambridge Quarterly of Healthcare Ethics* 2018, 27:123-136.

Kaye J, Whitley EA, Lund D, Morrison M, Teare H & Melham K. “Dynamic consent: a patient interface for twenty-first century research networks”, *European Journal of Human Genetics* 2015, 23:141–146.

Martani A *et al.*, “Regulating the secondary use of data for research: arguments against genetic exceptionalism”, *Frontiers in Genetics* 2019, 10:1254.

McLennan S, Celi LA & Buyx A. “COVID-19 : Putting the General Data Protection Regulation to the test”. *JMIR Public Health and Surveillance* 2020, 6(2) :e19279.

McLennan S, Maritz R, Shaw D & Elger BS. “The inconsistent ethical oversight of healthcare quality data in Switzerland”. *Swiss Med Wkly* 2018, 148:w14637.

Mester JL *et al.* “Communicating with Biobank Participants: Preferences for Receiving and Providing Updates to Researchers”. *Cancer Epidemiology Biomarkers & Prevention* 2015, 24(4):708-712.

Middleton A *et al.* “Global Public Perceptions of Genomic Data Sharing: What Shapes the Willingness to Donate DNA and Health Data?”. *The American Journal of Human Genetics* 2020, 107(4):743-752.

Mikkelsen RB, Gjerris M, Waldemar G & Sandøe P. "Broad consent for biobanks is best – provided it is also deep". *BMC Medical Ethics* 2019, 20(1):71.

Molnár-Gábor F & Korbel JO. "Genomic data sharing in Europe is stumbling – Could a code of conduct prevent its fall?". *EMBO Molecular Medicine* 2020, 12:1-7.

Munung NS *et al.* "Obtaining informed consent for genomics research in Africa: analysis of H3 Africa consent documents". *Journal of Medical Ethics* 2016, 42:132-137.

Murray TH. "Is Genetic Exceptionalism Past Its Sell-By Date? On Genomic Diaries, Context, and Content". *The American Journal of Bioethics* 2019, 19(1):13-15.

Nienaber A. "Consent to and authorisation of the export and use of human biological specimens for future research - perspectives from three African countries". *The Comparative and International Law Journal of Southern Africa* 2011, 44(2):225-254.

Nordling L. "Africa's science academy leads push for ethical data use", *Nature* 2019, 570:284-285.

Nordling L. "South African law may impede human health research". *Science* 2019, 363(6429):802.

Page SA, Manhas KP, and Muruve DA. "A survey of patient perspectives on the research use of health information and biospecimens". *BMC Medical Ethics* 2016, 17:48.

Peloquin D, DiMaio M & Barnes M. "Disruptive and avoidable. GDPR challenges to secondary research uses of data", *European Journal of Human Genetics* 2020, 28:697-705, p. 700.

Petersen I, Desmedt C, Harris A, Buffa F & Kollek R, "Informed consent, biobank research, and locality: perceptions of breast cancer patients in three European countries", *Journal of Empirical Research on Human Research Ethics* 2014, 9(3):48-55.

Pormeister K. "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* 2018, 5(3):706-723.

Rage V. "La base juridique du traitement des données de santé dans le cadre des recherches impliquant la personne humaine". *Panorama de droit pharmaceutique* 2019, 6:163-180.

Richter G, Borzikowsky C, Lieb W, Schreiber S, Krawczak M & Buyx A. "Patient views on research use of clinical data without consent: Legal, but also acceptable?". *European Journal of Human Genetics* 2019, 27:841-847

Rocher L, Hendrickx JM & de Montjoye Y-A. "Estimating the success of re-identifications in incomplete datasets using generative models". *Nature Communications* 2019, 10(3069):1-9.

Sariyar M & Schlünder I. "Reconsidering anonymization-related concepts and the term 'identification' against the backdrop of the European legal framework". *Biopreservation and Biobanking* 2016, 14(5):367-374.

Shabani M & Marelli L. "Re-identifiability of genomic data and the GDPR". *EMBO Rep* 2019, 20(6):e48316.

Shabani M & Borry P. "Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation". *European Journal of Human Genetics* 2018, 26:149-156.

Staunton C *et al.* "Safeguarding the future of genomic research in South Africa: Broad consent and the Protection of Personal Information Act No. 4 of 2013". *S Afr Med J* 2019, 109(7):468-470.

Staunton C, Slokenberga S & Mascalzoni D. "The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks". *European Journal of Human Genetics* 2019, 27:1159-1167.

Stokstad E. "Major UK genetics lab accused of misusing African DNA". *Science* 2019.

Thaldar D. "One material transfer agreement to rule them all? A call for revising South Africa's new standard material transfer agreement", *Humanities and Social Sciences Communications* 2020, 5(105):1-5.

Tindana P & De Vries. "Broad Consent for Genomic Research and Biobanking: Perspectives from Low- and Middle-Income Countries". *Annual Review of Genomics and Human Genetics* 2016, 17:2.1-2.19.

Van Veen E-B. "Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate". *European Journal of Cancer* 2018, 104:70-80.

von Thenen N, Ayday E & Cicek AE. "Re-identification of individuals in genomic data-sharing beacons via allele inference". *Bioinformatics* 2019, 35(3):365-371.

Willison DJ. "Alternatives to Project-specific Consent for Access to Personal Information for Health Research: What Is the Opinion of the Canadian Public?". *Journal of the American Medical Informatics Association* 2007, 14(6): 706-712.

Fu Y *et al.* "Pan-cancer computational histopathology reveals mutations, tumor composition and prognosis". *Nature Cancer* 2020,1:800-810.