Deliverable 5.2

Recommendations for European countries when planning national legislation on secondary use of health data

1 March 2023

This project has been co-funded by the European Union's 3rd Health Programme (2014-2020) under Grant Agreement no 101035467.

0 Document info

0.1 Authors

Author	Partner
Michael Peolsson	Swedish eHealth Agency, Sweden
Tina Chavoshi	Swedish eHealth Agency, Sweden
Maria Bergdahl	Swedish eHealth Agency, Sweden
Michel Silvestri	Swedish eHealth Agency, Sweden
Tine Leutholtz	Region Midtjylland, Denmark
Charlotte Rønde Mikkelsen	Region Midtjylland, Denmark
Hanne Louise Høimark	Region Midtjylland, Denmark
Zdenek Gütter	Ministry of Health, Czech Republic
Barbora Dubanská	Ministry of Health, Czech Republic
Anna Gelety	Ministry of Health, Czech Republic
Randi Lilletvedt	Directorate of e-health, Norway
Ragnhild Angell Holst	Directorate of health, Norway
Florine Wettly	Directorate of health, Norway
Ingvild Eide Graff	Norwegian institute for health, Norway

0.2 Keywords

Keywords	TEHDAS, Joint Action, Health Data, Health Data Space, Data Space, HP-JA-2020-1

Accepted in Project Steering Group on 31 January 2023. The European Commission gives final approval to all joint action's deliverables.

Table of Contents

1 Executive summary

This report is a document presenting basic recommendations intended to facilitate the planning (and implementation) of national legislation on secondary use of health data. These recommendations are based on a documented summary on a multinational level of the experiences and conclusions of pioneering European countries that already have such national legislation, in combination with the needs of other European countries in this respect.

GDPR is of specific importance when considering data exchange for secondary purposes. The document analyses and describes differences in Members States and how these affects enabling health data for secondary use. Six EU countries were interviewed about best practices and lessons learned in the context of preparing and implementing national legislation, specifically regarding certain legal provisions in the context of national structure and processes in relation to secondary use of health data. As a resuilt an analysis of different interpretations of GDPR as well as differences in national legislation supplementing the GDPR was carried out.

The report presents nine recommendations for Member States. These are legal interoperability, common interpretation of anonymisation and pseudonymisation, regulating secondary use, harmonising legislation, choosing a suitable legal basis, understanding controller and processor relationships, importance of addressing security from start and having a good communication with the public as well as ensuring enough resources for implementation.

2 Introduction

The 2020 European Strategy for data initiates the Commission's plans for the European data spaces. European Health Data Space, EHDS, aims to create a European infrastructure and coherent processes facilitating cross-border secondary sharing and use of health data. The initiative is a result of the challenges in harnessing the power of health data by policy makers, researchers and other stakeholders. At the same time, enormous amounts of health data are produced and stored in various sources every day for possible use.

Thus, from an EHDS perspective and in collaboration with Member States, the ambition is to create a common infrastructure, a network for connecting health data sources among Member States, with harmonised accessing procedures.

From a legal perspective, the sharing of data for secondary use is challenging for most countries in several respects. Different Member States have different infrastructures, governance models, data hosts/ownership and health data stewardships which are all part of a legislative and regulatory framework. European laws such as the General Data Protection Regulation, (GDPR), the Data Governance Act (DGA), the Cybersecurity framework (NIS2 directive), and the Medical Device Regulation (MDR), as well as proposals under negotiation at the time of writing, such as the Data Act (DA) and Artificial Intelligence Act (AI Act) impact national laws and safeguards. In addition, the new proposal from the Commission for the EHDS Regulation is under negotiation with the European Parliament and the Member States.

Work Package 5 (WP5): "Sharing data for health" is related to different perspectives on sharing data for secondary use and thus, takes into consideration all aspects introduced above.

2.1 TEHDAS WP5 – Sharing data for health

Four Tasks comprise WP5. "Define and develop the evidence base for the secondary use of health data in EHDS, user perspectives", (5.1) "Enabling the secondary use of data by aligning the interpretation of GDPR", (5.2), "Best practises for EU cross-border sharing of personal health data", (5.3), "Developing options for governance models for the EHDS", (5.4). WP5, Task 5.2, initiates partially from the analysis of use cases in Task 5.1 where stakeholders' experiences about barriers in the context of data sharing are described. Task 5.2 aims to enable cross-border exchange and secondary use of health data through guidelines/recommendations for European countries when planning national legislation.

The work includes mapping different nationally designated bodies permitting and/or providing health data access, with the aim of forming the conditions for future multilateral constructive networking. Information and knowledge from previous studies (e.g., the EUHealthSupport Study, the so called Nivel study[1]) was supplemented by a survey and deep interviews with legal experts to provide a good understanding of Member States' legal prerequisites and choices.

A compilation of collected information is presented in the TEHDAS Milestone M5.3 report, displaying a compiled image of the situation in several Member States regarding laws, regulation, and administration of health data for secondary use. This material is further

[1] https://www.nivel.nl/sites/default/files/bestanden/1003988.pdf

processed and analysed in order to provide the foundation for the Deliverable 5.2, in the form of recommendations for European countries when planning national legislation on secondary use of health data.

WP5 is concerned with both the user perspective – in this case limited to the scientific researchers' and the policy-makers' perspectives – as well as, data controllers', data providers' perspectives. The analyses of these perspectives feed into the parallel work of forming a governance model for the EHDS (Figure 1).

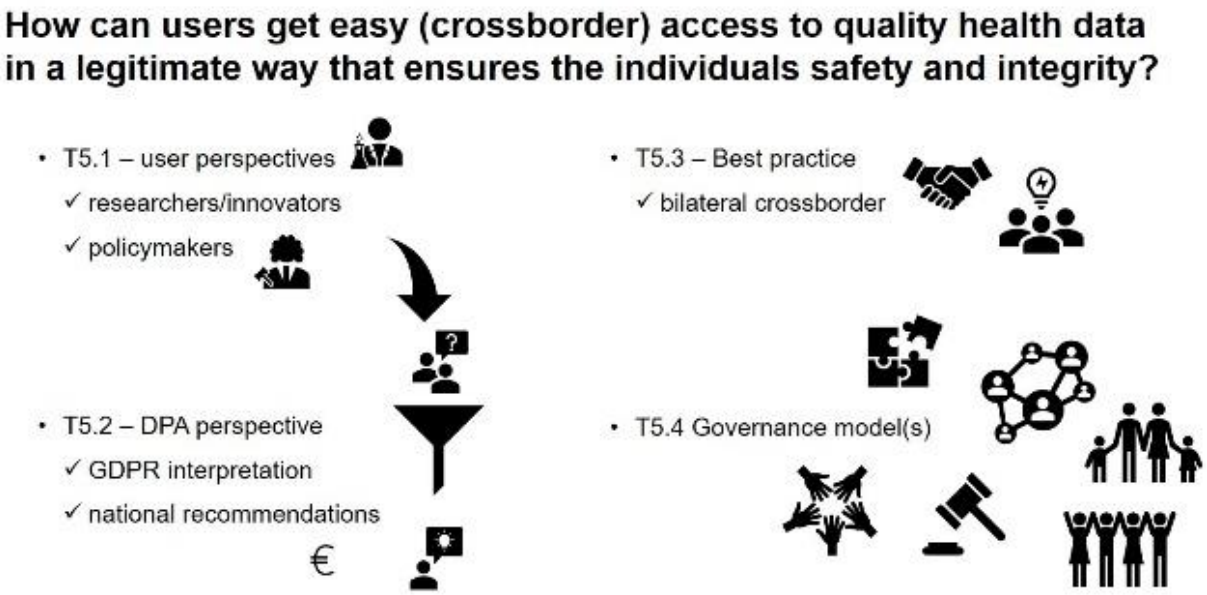

Figure 1: The context of work package 5, depicting the four different tasks.

3 Background and aims

This deliverable is a document presenting basic recommendations intended to facilitate the planning (and implementation) of national legislation on secondary use of health data. These recommendations are based on a documented summary on a multinational level of the experiences and conclusions of pioneering European countries that already have such national legislation, in combination with the needs of other European countries in this respect.

This Deliverable D5.2 report builds upon the results results of prior work in the internal Milestone report M5.3 report, focusing on GDPR interpretations and data access bodies. Results from other Tasks have also been included. More specifically, results from Task 5.1, focusing on stakeholders' perspectives on barriers when considering data sharing to be used for secondary purposes were important inputs to be investigated more deeply in Task 5.2. Furthermore, results from Task 4.1, mapping 12 countries' health data landscape and infrastructures for secondary use of health data have provided important inputs when considering the legislative frameworks as a corner stone for cross-border sharing and secondary use of data.

4 Method and analysis

The material in Milestone report M5.3 has been further processed and analysed in order to provide the foundation for the Deliverable 5.2, in the form of recommendations for European countries when discussing and/or planning national legislation on secondary use of health data.

4.1 Overview of methods

The method for this second phase is based on further literature reviews collected inthe Milestone report M5.3, but also scrutinising the Nivel study in order to bridge some identified gaps. The D5.1 report on stakeholders' experiences concerning working under the GDPR and described barriers and challenges was also utilised[2]. Further, deep interviews were performed with six selected countries based on a questionnaire investigating the current legal situation in Member States. There were several workshops with TEHDAS legal partners to discuss and anchor the questionnaire that formed the basis for the interviews. As a result, three thematic topics for semi-structured questions formed the basis for the interviews: What is the process like in your country adopting a national legislation for secondary use of health data? Is there a discussion on national level creating a national node for secondary use of health data? and finally, a discussion about certain legal provisions. The interviewees were asked to speak freely about these topics. Follow-up questions were asked for clarification and specifications.

Six countries were selected for deep interviews. The interviewees were representatives at a national level for planning, discussing, or having been in a responsible position in the process of realising the legislation. The country selection was made according to the criteria: progress in national legislation for secondary use of health data, EU regional distribution, centralised/de-centralised national system, and legal basis for primary collection of health data, respectively. This information collected represents the following countries: the Aragon region (Spain), Czech Republic, Finland, France, Germany, and Latvia, respectively.

A meeting was also organised with the European Data Protection Board (EDPB) subgroup, Compliance, e-gov and health, that is working on the EDPB guidelines on secondary use for research purposes to convey the work carried out within Task 5.2.

Finally, we chose one article and one report of high relevance in the context of sharing data for secondary purposes and summarised them and used them as inspiration in our work (appendix 1).

[2]https://tehdas.eu/app/uploads/2022/08/tehdas-report-on-secondary-use-of-health-data-through-european-case-studies-.pdf.

4.2 Overview of analysis

The topics chosen for analysis are based on the work package description and results from the internal milestone report M5.3. These topics reflect the structure of this report.

The analysis covers:

- Analysis of different interpretations of GDPR in order to describe how interpretations of GDPR differ and how these differences affect the possibility to create harmonisation and secondly how cross-border health data sharing is affected.
- Analysis of national legislation supplementing the GDPR in order to describe examples of supplementary legislation and how it affects cross-border health data sharing.
- Analysis of Member States infrastructure for sharing health data in order to describe differences and how differences affect health data sharing.
- Analysis of barrier case studies from WP5, T5.1 i.e., in order to describe stakeholders´ concerns about legal barriers in a secondary use of health data perspective.
- Analysis of six EU countries deep interviews discussing three themes:
    - Questions about best practices and lessons learned in the context of preparing and implementing national legislation.
    - Questions related to certain legal provisions in the context of national infrastructure and processes.
    - Questions concerning certain legal provisions.

The first output from Task 5.2 was an internal milestone report on GDPR interpretations in secondary use of health data in different Member States and other participating countries. The milestone constituted:

- A literature study on public information about guidance and legislative frameworks on how to approach sharing and secondary use of health data.
- An analysis of the Assessment of the EU Member States' rules on health data in the light of the Nivel study and the potential gaps within that study.
- Use cases described in the survey in Task 5.1 on stakeholders' experiences of barriers when it comes to the sharing of health data for secondary purposes.
- A survey mapping the organisation and bodies in the TEHDAS partner countries which grant access to health data for secondary purposes.

5 Terms and definitions

5.1 Secondary use of health data

Given that there is no common definition of secondary use of health data and that the term is not defined in the GDPR, our interpretation has taken its stance from what is commonly understood within the data protection community and framework as secondary use; the reuse of data for a different purpose than it was originally collected for.

This is also the definition used in the survey and the deep interviews. However, the current EHDS proposal defines “secondary use of electronic health data” as the processing of electronic health data for purposes set out in Chapter IV of this Regulation. The data used may include personal electronic health data initially collected in the context of primary use, but also electronic health data collected for the purpose of the secondary use.

5.2 Permitters and providers of data for secondary use of health data

There is no common definition of the terms permitters and providers in the Member States. Since the system of permitters and providers differ in the Member States one would in each case need to investigate who is the controller of the data from a GDPR perspective. The focus of Task 5.2 is the authorities that have the legal right to decide whether data access is approved for the applicants. Therefore, we do not include ethical committees’ approvals in this report. The actual legal power of whether to grant access to the data in most instances lie with the data controller and sometimes with the data provider, e.g., as the case is with Findata as the data provider.

6 Summary of Milestone report M5.3

The internal (not public) M5.3 report, the precursor of this deliverable D5.2 report, comprises a literature review on public publications on secondary use of health data in the context of research and policy making. Especially, searches for publications according to topics as legislation/GDPR on secondary use of health data and use of such legislations has been in focus. Results show frameworks for ethical guidance and guidelines for technical considerations fulfilling legal frameworks, frameworks for interpretation of the GDPR, techniques for preparing data sharing by anonymising health data, technical aspects of data sharing and technical infrastructure for transfer and sharing data in a secure way. The resulting matrix of publications can be summarised into three meta levels: 1) legal frameworks, 2) guiding frameworks and 3) frameworks for preparing health data sharing. The publications were then further categorised into thematic blocks.

Next, the report: "Assessment of the EU Member States' rules on health data in the light of GDPR", the so called Nivel study was reviewed (https://www.nivel.nl/nl/publicatie/assessment-eu-member-states-rules-health-data-light-gdpr, 2021, feb). This analysis forms an important foundation for this deliverable, D5.2, clarifying any gaps. The Nivel study states that there are differences in how the Member States have interpreted the GDPR. The differences extend from the direct use of the legal basis of GDPR, to the use and understanding of concepts, e.g., when personal data is considered either anonymised or pseudonymised. However, the Nivel study does not delve into a thorough examination and comparison of where different interpretations lie, and therefore gives no overview of the specific parts of GDPR that cause differences in interpretations.

GDPR further allows Member States to maintain or introduce further conditions, including limitations, for the processing of health data, genetic and biometric data. However, recital 53 of GDPR also states that this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data. In practice, this possibility constitutes an obstacle to the sharing of and access to health information. The Nivel study does not elaborate on this fact despite the possibilities available under the GDPR to share health data.

Another result from the analysis of the Nivel study, is the lack of focus on national legislations and how these may act as primary barriers for the cross-border sharing of health data. The fact that many Member State have national laws for health data protection is a challenge towards achieving uniformity across the countries. and thereby an important basis for a cross-border health data space. Therefore, the national laws have to be addressed and analysed more in-depth.

In Task 5.1, a literature review complemented with expert interviews identified barriers to cross-border data sharing of health data for secondary use. This resulted in a list of eleven priority barriers. Out of these, the barriers based on a legal nature are used as a starting point in this D5.2 report.

All of the above form the basis for developing the questions of the deep interviews with countries, that have either already implemented a national legislation or discussing this option. The outcomes of this Task feed into Task 5.4, thereby contributing to the legal interoperability in relation to EHDS.

7 Business models

Recommendations given in this report should include examples of sustainable business models. In this context, according to answers in the interviews and surveys in work package 5.2, most of the countries that either have established, or are in the process of establishing nodes managing processes for secondary use of health data on a national level, have also, in their national legislation permitted such authorities to charge fees for their services or enabled them to establish companies under their remit for selling additional services. The fees that the authorities can charge are e.g., attached to services where they gather, categorize, refine or prepare data before handing out the data sets. In some cases, fees may also apply when data is gathered from different data holders in order to be integrated. However, most authorities and organisations have not yet started using the possibilities to charge fees or set up additional services. Their focus has been to get their organisation in place and be able to offer the initial basic services. The primary focus is to enable secondary use and first when that is enabled to look at the potential of the business models that will be necessary to keep the system running. Hence, this report does not include analysis on economic sustainability. Its primary focus is instead to enable the secondary use in order to even look at the potential for business models.

8 Legal barriers identified in Task 5.1

Eleven priority barriers were identified by WP5.1 in their T5.1 report. T5.1 draws the conclusion that six of those barriers are caused by differing interpretations and implementation of GDPR (see below). They were therefore considered of direct relevance to Task 5.2.

In addition, our analysis has highlighted that barrier 4 is also fundamental to address in the guidelines or recommendations from WP5.2 and is therefore added as a barrier to analyse in this deliverable.

The recommendations given in this report are directly linked to these described barriers:

1) There is no common European interpretation of what constitutes 'sufficient anonymisation' to transform personal data to non-personal data.
2) There is no common European interpretation of what constitutes 'pseudonymisation'.
3) There is no common European interpretation of what is, and what is not, 'secondary use' of data.
4) European countries have national laws/rules on health and research data in addition to GDPR.
5) European countries have the ability to set their own derogations under GDPR.
6) European countries have different preferences as to the choice of legal basis for processing under GDRP.
7) Health data is considered sensitive data e.g., special category data under GDPR and is treated differently from other types of data when it comes to health data ethics, management and use.

9 Analysis of the different barriers

GDPR provides for a consistent approach for data protection rules throughout the EU. However, despite these harmonised rules we still see a degree of fragmentation and diverging approaches. Primarily, this is caused by the possibilities that GDPR presents for Member States to adopt national legislation. The possibility to introduce derogations, limitations or additional criteria applies to several articles, for example, articles 6(1)(e), 6(2), 6(3), 9(4) and 89(2). Furthermore, several of the provisions of GDPR require either national or EU law to apply (for example articles 6(3), 9(2)(g)(h)(I), 9(3)). This approach has led to divergence in the implementation of GDPR in diverse national contexts as evidenced by TEHDAS[3] and discussed in European literature[4,5]. In addition, other national legislation, unrelated to GDPR might also have an impact on health data and its use (e.g., the Swedish Access to Information and Secrecy Act[6]). Moreover, there are Member States in which the legal infrastructure that was created by existing law relating to health data and the law that implements GDPR, are perceived both by the data holders´ and users´ as unclear even at national level expressing unclarities in governance and processes for accessing health data.

Adding to this, the differing choices of legal basis driven by national preferences for processing personal data (articles 6 and 9 GDPR) as well as differences in semantics and data quality at national level, creates practical challenges to cross-border data sharing as further evidenced by TEHDAS.[7]

9.1 Anonymisation and pseudonymisation

This section addresses the two barriers 1 and 2 together since they are closely linked.
There is a legal definition of Pseudonymisation in article 4(5) GDPR and anonymisation is mentioned only once in GDPR, recital 26 lists the criteria for when a natural person is no longer identifiable. GDPR does not include a detailed description of how to properly achieve pseudonymisation or anonymisation and some of those criteria have proven challenging to apply in practice. The practice of both anonymisation and pseudonymisation, however, predates GDPR and many Member States already had national practices on what is considered sufficient anonymisation or pseudonymisation.Pseudonymisation is a practice used by health data permitters, sometimes together with an ethical approval, in situations where sensitive health data needs privacy protection when shared. In some countries, and to some extent, the terms have developed and been formalised as for example within Finland’s

[3] TEHDAS suggests options to overcome data barriers. [Online] 2022. [Cited: 15 May 2022.] https://tehdas.eu/results/tehdas-suggests-options-to-overcome-data-barriers/.
[4] EDPB-EDPS. EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space. [Online] 2022. [Cited: 19 09 2022.] https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en.
[5] National Interoperability Framework Observatory (NIFO). The European Interoperability Framework in detail. [Online] 2022. [Cited: 19 09 2022.] https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail.
[6] Ministry of Justice (2020). Public access to information and secrecy. Available at: Public access to information and secrecy – The legislation in brief (regeringen.se)
[7] TEHDAS (2022). Deliverable 5.1. Report on secondary use of health data through European case studies. Barriers on cross-border sharing of data for secondary use and options to overcome these. Available at: https://tehdas.eu/results/tehdas-suggests-options-to-overcome-data-barriers/

Findata and the French Health Data Hub. They have, however, been developed or formalised without wider consultation among Member States to agree on a common understanding.

Also, it is essential for smaller EU/EEA countries, such as Norway and Sweden, to be granted access to such clarifications, in order to ensure harmonisation of sufficient anonymisation.

9.2 Lack of common interpretation of secondary use of data

This section addresses barrier 3, lack of a common European interpretation of what is and what is not 'secondary use' of data. Within the TEHDAS work, secondary use of data is commonly understood as reuse of data, i.e., data collected for one purpose and then used for another purpose.

Secondary use of health data is not prohibited under GDPR as the regulation enables such use whenever certain conditions are met. The terminology used within GDPR is not 'secondary use' but 'further processing', as seen in articles 5(1)(b) and 6(4). The question arises how the terms ´secondary use´ and ´further processing´ in a legal sense are to be understood. Do the terms mean the same thing in a legal context and are they used equivalently in practice?

9.3 National rules and derogations

We have decided to address the two barriers 4 and 5 together since they are closely linked. Barrier E states that European countries have national rules on health and research data in addition to GDPR. Barrier F states that European countries have the ability to set their own derogations under GDPR.

When it comes to genetic data, biometric data or data concering health GDPR allows for Member States to maintain or introduce further conditions and limitations, thorugh national legislation, than the conditions and limitations stipulated by GDPR, article 9(4). This can be illustrated by the French example where the new legislation regarding secondary use of health data and establishment of the Health Data Hub does not include genetic data, for which other conditions and limitations apply.

Some of the provisions of GDPR require either national law or European law as a basis to be able to use it. Based on the interviews, the survey in milestone report M5.3 as well as the survey carried out in this second phase of work package D5.2, most of these are laid down in national law that were in force before GDPR and remained in force, without amendments.

The result of additional legislation at national level in each member state, is that a difference in e.g., the terms agreed upon for getting access to and retrieve health data will exist. Hence barriers will be present in the current national laws throughout the Member States, but new (not yet drafted) legislation may also potentially contribute to more differences and challenges for cross-border sharing of health data.

As long as the possibility of additional legislation at national level in key areas for health data sharing is present in GDPR, it will be a major challenge to reach an operational model for cross-border sharing of health data. One must, however, recognise that the need for the possibilities for special legislation at national level to maintain or introduce further conditions or limitations has probably been introduced to facilitate the implementation of GDPR in the diverging national settings and structures of the Member States.

As was concluded in Milestone M5.3, the Nivel study mentions and describes this at an overall level in the Appendix, but there is no thorough examination on the different national laws and no comparison on how or at what level each member state has national laws.

The fact that each Member State has national (special) laws will be a challenge towards achieving uniformity across the countries and thereby as a basis for a cross-border health data space. Therefore, the national laws have to be addressed and analysed more thoroughly.

9.4 Legal basis

This section addresses barrier 6, that European countries have different preferences as to the choice of legal basis for processing under GDPR. This is particularly visible in relation to the primary collection of the data. There is a clear divergence in whether Member States rely on consent, contract or a combination of legal obligation and public interest[8].

Some of the provisions of legal basis in GDPR require either national law or EU law as a basis to be able to use the data. Tasks in the public intrest as well as legal obligations, articles 6(1)(e) and (c), require the basis for the processing to be laid down in either Member State law or Union law. Based on the interviews, the survey in milestone report M5.3 as well as the survey carried out in this second phase of Task 5.2, most of these are laid down in national law that were in force before GDPR and remained in force, without amendments.

Depending on which legal basis you rely on for the primary use, it naturally gives different possibilities for further use for a secondary purpose.

When relying on consent for the primary collection, Member States mostly have to rely on reconsent for the secondary use.

When relying on a contract, that would also entail a need for reconsent for the secondary use, this would be the case since further processing for e.g., research purpose would in most cases not pass the compatibility test under article 6(4) GDPR.

What we see, however, is that when the legal basis is a legal obligation and/or public interest there is no need for reconsent, to enable the secondary use. This is normally when secondary use is enabled by national legislation.

We have seen some examples in the interview of retroactively trying to legislate a secondary use of data that was initially collected with consent as a legal basis in an attempt to not require reconsent from the data subjects.

The choice of legal basis also entails different rights for the individual, for example article 17 in the GDPR (the right to erasure) is not applicable if the legal basis for the processing is to comply with a legal obligation (article 6(1)(c)) or for reasons of public interest in the area of public health, article 9(2)(h) and (i) or research purposes in accordance with article 89(1).

Even when Member States rely on legal obligation or public interest for both the primary use and the secondary use, they might still give the individuals opt out possibilities. Opt out is not the same as relying on consent as a legal basis. Even if opt out possibilities are in place, this

[8] As seen for example by the Nivel study, table A1.1 and surveys and deep interviews carried out by WP 5.2

still gives the possibility to derogate from certain rights of the individuals as well as not requiring reconsent for every further processing of the data (article 23).

9.5 Sensitive health data

This section addresses barrier 7, that health data is considered a special category data under GDPR and hence is treated differently from other types of data when it comes to health data ethics, management, and use.

We need to acknowledge that personal health data is sensitive data, and rightfully so. Health data therefore must be treated differently from other types of data when it comes to health data ethics, management, and use. For example, by way of higher levels of protection connected to it. If work is conducted properly with the other barriers identified, and there is effort to resolve them as much as possible, for example through the recommendations in this report, then this will no longer be a barrier. For example, if work is conducted towards equalising the use of safeguards at national level, this will lead to a possibility for Member States to recognise other Member States' safeguards. This would likely be a step in the right direction.

10 Results from interviews

The results of the interviews are presented according to different themes arising in the interviews.

10.1 Controller and Processor relationships

When interviewing Member States[9] that have implemented legislations, setting up specific structures for enabling secondary use through a national node, it is clear that one aspect that these Member States did not reflect on when drafting or adopting legislation for secondary use is the provisions of controller and processor in line with GDPR. These aspects are complicated and were often left out of the preparatory work. Consequently, a major aspect is left out of the implemented legislation.

In one of the interviews, it was even pointed out that this might be one key success aspect for implementing and applying the national legislation, whether at national or EU level. Controller and Processor are central concepts of the GDPR allocating responsibilites and accountability. If the aspects of who is responsible and accountable, from a legal point of view, for different aspects of the data cycle, are not investigated and reflected on, then process and systems might be established that do not reflect the actual and factual controller and processor relationsships. As a consequence, if this relationship is not reflected on in the preparatory work or in the legislation, then the hard work is left to the organisations implementing the legislation.

10.2 Addressing security from start

Another conclusion drawn from the in-depth interviews and especially from those countries that recently have deployed legislation for secondary use of health data, is the importance of considering and addressing security issues from the start. This encompasses all aspects of security: cybersecurity, information security and IT security. If these issues are not looked into and addressed at an early stage, they will probably lead to challenges during the implementation stage later on.

10.3 Good communication with the public

The importance of considering how to communicate to the public on any new functions or when enabling secondary use of data, is another of the conclusions drawn from the in-depth interviews. The public needs to understand why and how their personal health data might be made available for example for research or innovation purposes and that security measures are in place to protect their personal health data. The public might also have a fear that their health data is being sold to, for example, private companies. One of the interviews pointed to communications with the public as being one of the key aspects of gaining success and acceptance.

10.4 Enough resources for implementation

One of the most important conclusions drawn from the in-depth interviews with the Member States that have passed and implemented legislation enabling secondary use of health data, is the importance of having enough resources for implementation of the provisions of the law

[9] France and Finland

as well as the practical execution of those provisions. This relates both to the resources needed for setting up for example new structures, organisations, human resources and technical abilities as to the need to make sure that the data holders have enough resources to set up a structure and organisation to handle a request for access to data.

Sufficient resources were a main topic mentioned in the deep interviews with Members States that have passed and implemented legislation for secondary use of health data. Resources were reported to be needed for the implementation of the provisions of the law, as well as, the practical execution of those provisions. More specifically, the resources needed are related to, for example, setting up new structures or organisations, hiring human resources and investing in technical abilities. In addition, it was reported that sufficient resources would also be needed by the data holders in order to handle the request for data access.

11 Conclusions

On a general level different interpretations of EU regulations are quite common across all sectors and not a phenomenon only within GDPR practice. A law, whether national or European, will be interpreted differently by different actors, the interpretation might even differ within the national level. It is always ultimately the European Court of Justice that gives interpretative priority to the EU legislation There are also examples where Member States have not regulated other secondary purposes for which data can be used. This has had a restrictive impact on the possibilities for further processing according to article 5(1)(b) GDPR.[10]

From our survey and interviews, as well as literature findings, a conclusion is that it is not Member States' actually having diverging interpretations of key aspects of GDPR, but rather the context of a country's infrastructure, organisation of healthcare, legislation in force prior to GDPR etc. that gives rise to the differences in implementation of GDPR.

A conclusion that we have drawn from our interviews and answers to the survey is also that Member States tend to regulate the secondary purposes for which data can be used. Against this backdrop, (national) legislators can leave it up to those wanting to use the data to directly apply the provisions from articles 5(1)(b) and 6(4). The controller, in turn, would then need to assess wether a compatibility test is required and consecently carry one out before pursuing the processing activity, i.e. a legal test regulated by the GDPR, art 5.1.b and 6.4, in accordance with art 6.4 GDPR. Nonetheless, (national) legislators seem to prefer to introduce legislation on secondary use and necessary safeguards as a form of further processing. In this case, the legislator conducts the compatibility test and assesses compliance in relation to article 23 GDPR on restrictions. While article 5(1)(b) and 6(4) can be applied both directly by the controllers and by regulation through national law, most Member States seem to solely see secondary use as the product of legislating the possibilities for further processing. This might be perceived as restricting the possibilities for further processing that are given according to article 5(1)(b) rather than enabling them, which is the purpose when Member States choose to regulate it.

11.1 Further processing

Another conclusion concerns the legal term 'further processing'. When the purposes for secondary use are regulated by national law it is at times understood, as if further processing is limited to and only allowed for the secondary purposes mentioned by the legislation. Thus, when for example research or statistics are not stated as purposes for which secondary use is allowed, it could consequently be interpreted as prohibited. While there still might be a possibility for the data to be further processed according to article 5(1)(b) GDPR. There are however examples of where national law stipulates that the data cannot be further processed for other purposes than those mentioned in the law. There are also examples of laws that stipulate that the data can be further processed but only if, often as an additional safeguard, the consent of the person whom the data concerns is sought. All in all, the tendencies are that from the Member States' point of view it is not the preferred option to rely on the possibility for further processing that article 5(1)(b) GDPR might give.

[10] https://edpb.europa.eu/system/files/2022-01/legalstudy_on_the_appropriate_safeguards_89.1.pdf, *Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research, Final Report, EDPS/2019/02-08*

One could argue that there is no need to regulate certain other purposes, such as research, since you should be able to rely on the possibilities for further processing in accordance with article 5(1)(b).

11.2 Secondary use in accordance with national law

Another conclusion is that often the possibilities for secondary use in accordance with national law were already implemented in national law prior to the adoption of GDPR and its introduction of further processing. These national provisions were then not always changed nor adapted to consider article 5(1)(b). There are however some Member States that have adopted and implemented legislation on secondary use after the implementation of the GDPR, i.e. France and Finland.

11.3 Anonymisation processes

It is essential that bodies issuing guidelines on pseudonymisation and anonymisation work together on those topics, across Member States, especially regarding anonymisation techniques and their definition. This is a very complex area known by just a few experts in EU/EEA. Thus, the applicable law should not only appoint authorities in charge of issuing guidelines, but also require such authorities to cooperate cross-border and agree on a common definition of pseudonymisation and anonymisation, which also considers technical and practical issues.

12 Recommendations

12.1 Legal interoperability

When adopting national legislation, Member States need to consider how their national law will be interoperable with the laws of other Member States. This is foremost a question of how much Member States are willing to adapt their national law to other Members States' law. The second aspect is whether Members States are willing to look into the possibility of accepting other Member States' safeguards - as safeguards accepted under their own national laws. To a certain degree national laws across Member States can be interoperable and work hand in hand, as can be seen for example in the area of pharmaceuticals.

Legal interoperability between Member States' diverging national regulations is hard to achieve without at least some minimum set of understanding and structures around how secondary use of health data is enabled. One prerequisite for interoperability is the need to understand by which legal basis the original data set is gathered and processed. An understanding of the legal basis gives an understanding of the rights of the individual and any restrictions that might apply to the use and processing of the data.

However, since Member States can enact additional national rules applicable to health data, there is a need to understand each Member States' national rules, and how they function. It can for example be the possibility for the individual to opt out of certain secondary purposes, or restrictions for the controller as to the use of the data. Thus, there is a need, in an easy and publicly available way, to access and understand the rules applicable to different sets of data for secondary use. The EHDS proposal of a dataset catalogue (article 37) proposes to include details about the source and the conditions for making the data available, is a step in that direction.

If the aim is to reach as much interoperability as possible Member States should strive to use similar legal basis for the primary gathering and processing of health data, and as much as possible refrain from applying additional set of conditions for the data.

Even though Member States would strive as much as possible to use the same legal basis or to not introduce additional set of requirements under national rules, a certain degree of difference in the implementation of the provisions of GDPR will still remain - specifically tailored to the structures and organisations of each Member State. The use of for example safeguards are tailored to the cultures, structures, and organisation of each Member State. Following analysis of the in-depth interviews conducted as well as literature review[11].

In order to enable interoperability, Member States need to understand and use similar safeguards according to article 89 (1) GDPR, for example the needs for ethic review boards or authorities, pseudonymisations and to work towards accepting other Member States' safeguards. There is further a need to make sure that secrecy laws or other such laws (e.g., Classified Information Protection Acts) are respected for the purposes of sharing of data

[11] Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four Member States and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden, Seminars in Cancer Biology, volume 84, September 2022, pages 271-283), Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research (EDPS/2019/02-08)

across borders. Legitimate interests and protected rights (protection of trade secrecy, intellectual property rights (IPRs), i.e., patents, trademarks, designs, copyright and neighbouring rights, geographical indications, and plant variety rights, etc.) should also be fully protected. The EMA's Policy 0070 can serve as a model for preservation of trade secrets and IP by Data Holders, (for further reading, see Policy - Publication and access to clinical data (2019 revision) (europa.eu)[12]).

12.2 Common interpretation of anonymisation and pseudonymisation

Our recommendation for Member States when drafting national legislation for secondary use would be to regulate, or define, what is to be considered sufficient pseudonymisation or anonymisation. The law could make a reference to the need for such a safeguard and rather stipulate an authority or other such body to decide and issue such guidelines. Since technology is a fast-moving matter and advanced new techniques emerge more often than regulation can be changed, it is easier to have these more technical aspects set in guidelines. It is then also easier to try and reach consensus among the Member States on guidelines, that can be used across the Member States.

12.3 To regulate secondary use

Our recommendation to Member States would be to not only rely on the possibilities available according to article 5(1)(b) for further processing. Member States can and should, to a higher extent, try to regulate that data can be processed for other purposes.

Whether article 5(1)(b) also might be relied upon to a higher extent and in what circumstances, might be given further clarity if the subject is addressed by the upcoming EDPB guidelines on secondary use for research purposes.

The Commission's proposal for the EHDS is one step in this direction, regulating the possibility for secondary use through EU regulation. However, for the full potential of such regulation there is a need to address the possibilities for differing national regulations. As our work has shown this is one of the main reasons, aside from the technical and semantical ones that the full potential of sharing data cross-borders has not yet been able to be realised.

12.4 To further harmonise national legislation

Our recommendations for Member States when planning for national legislation for secondary use of health data, would firstly be to see if there are any national provisions adopted under the possibilities for derogations provided for under GDPR. If there are such derogations our recommendation would be for Member States to consider whether the derogations can be abolished. Secondly, for the provisions of GDPR where national legislation is needed in order for the provisions to be applicable, Member States should try and reach a common understanding on what for example constitutes safeguards in accordance with article 89 (1) This might, however, prove hard to accomplish. Member States should then consider revising national legislation to enable for equivalent safeguards according to other Member states' national legislation to be recognised as safeguards equivalent to their national ones when the application comes from another country.

[12] Policy - Publication and access to clinical data (2019 revision) (europa.eu)

There are also aspects of other national laws that are relevant to consider with regards to cross-border sharing of health data. There could be laws that would prohibit the exportation of the data out of the country, for example security legislation. Member States should consider revising these as well.

12.5 To choose a suitable legal basis

Member States should as much as possible try and refrain from relying on consent-based gathering of health data for primary use and to a higher degree look to enable the gathering and use of health data through legal basis in the form of public interest or legal obligation. This would to a higher level enable the possibilities for secondary use when needed.

12.6 To understand controller and processor relationships

Member States need to investigate and fully understand how the controllers´ and processors´ responsibilities within their existing infrastructure and organisation is set up and where such responsibilities are located. This area needs to be prioritised.

Member States should also make a thorough analysis of whether the need for any proposed new structures, stems from national legislation or from EU law. Enabling secondary use in practice change of controllers´ and processors´ relationships. Furthermore, they should consider whether there is need to clarify their roles in national legislation.

While GDPR permits the appointment of a controller or processor by law (article 4(7) and 4(8)), such designation should be in line with the provisions of a controller and conform with GDPR.

12.7 Important to address security from start

Our recommendation to Member States is that all aspects of security – cybersecurity, information security and IT security – should be included at an early stage. To avoid implementation and application difficulties, this is a very important step. Security by design should already be considered in the preparatory work, leading up to legislation on secondary use.

12.8 Important to have good communication with public

Our recommendation to Member States is to, already in the preparatory work leading up to national legislation on secondary use, address the need for setting up a plan on how to communicate with the public. This plan should be in place as soon as possible and enough resources should be set aside for implementing the communication plan.

12.9 To ensure enough resources for implementation

Our recommendation to Member States is to make sure that preparatory work leading up to proposals for law on secondary use, has a thorough analysis of the resources needed for the implementation of the law. The analysis should not only consider the financial resources needed to set up new agencies or IT solutions. It is important to thoroughly analyse the human resources needed to operate the new structures, agencies and tasks. The need for additional resources for the data holders should also be analysed as they often will have new requirements to comply with.

We strongly encourage the elaboration of practical and easy-to-use guidelines, elaborated across Member States, which will give more concrete and asserted elements to base the anonymisation assessment on.

Appendix 1. Summary: "Study on the appropriate safeguards under Article 89(1) GDPR"

Here we present a summary of one article and one report that were deemed of importance to the work in the D5.2. Firstly, a summary of a study commissioned by the EDPB on the appropriate safeguards under article 89(1) GDPR for the processing of personal data för scientific research[13], and secondly a short summary of an article: "Divergences in the rules for genetic and health data sharing in four Member States and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden[14].

Summary on report 2019/02-08 "Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research"

The EDPB study analyses both national and sectorial legislation referring to and implementing Article 89(1) and other relevant sources, such as guidelines, opinions, industry codes etc. from 12 countries within the European Economic Area (EEA), based on a questionnaire (responded to by each involved country) on the implementation of appropriate safeguards in national and sectoral legislation as well as in other non-binding instruments and sources. The study focuses on explicit references to safeguards for the processing of personal data for scientific research purposes.

As only 12 countries where asked to respond to the questionnaire, the study does not mirror the situation in all 30 countries within the EEA, but still asses that interesting observations has been made and that some best practices and challenges have been identified.

The study sets out by presenting the national legislation implementing Article 89(1) of the GDPR. In addition, it also looks at the relevant national guidelines and codes of conduct adopted in the selected countries. Finally, the study addresses the case law of national courts and the related guidelines and codes of conduct.

From the review of the just above mentioned, the study presents some overall similarities in the countries, but also some converging elements and trends[15] in both EU and national legislation and soft law. The most important converging elements identified include: pseudonymisation and anonymisation techniques; technical measures for security management; confidentiality and integrity, including encryption, organisational measures and measures for publication and dissemination. Additionally, the identified tendencies include research or data management plan, the role of the DPO, DPIA, requirements after the completion of the research and medical secrecy.

Furthermore, the study results show, that there is variation in the relevant interpretation and handling of central definitions and concepts. For example, "scientific research" is understood

---

[13] https://edpb.europa.eu/system/files/2022-01/*legalstudy_on_the_appropriate_safeguards_89.1*.pdf, *Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research, Final Report, EDPS/2019/02-08*

[14] https://www.sciencedirect.com/science/article/pii/S1044579X21002947; *Divergences in the rules for genetic and health data sharing in four Member States and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden*, Seminars in Cancer Biology, volume 84, September 2022, pages 271-283).

[15] Defined in the study, page 48: *"The term "converging element" is used if a certain safeguard was present in more than six countries, whereas the term "trends" is used to clarify emerging tendencies in fewer countries."*

differently, and in that context, whether public interest prevails or not, or whether a single country sets out requirements concerning the need for specific methodology as a condition in research projects.

To that, the study lines up that further variations between countries are considerable in several areas, e.g., regarding requirements for the processing of personal data and personal data of special categories (sensitive personal data), the (fragmented) regulation of requirements and safeguards of biological samples and biobanking and the varying role and governance of research authorities, just to mention a few.

The study gives examples on the differences, but also on the impact of the presence of variations. As GDPR has an objective to harmonise the level of protection of data all over EU, each single country's competence to regulate at a national level leaves the landscape of framework fragmented, which (quoted in the report as) *"may negatively impact the ability to conduct cross-border research, and research in general"*.

Therefore, the study draws recommendations from the findings of divergences, and initially emphasises the needs – on a general level –, such as the importance of uniformity in the EEA states' understanding of 'scientific research' and an increased dialogue between the states.
One of the main specific recommendations is the need for legislation and establishment of guidelines, practices and/or rules of conduct both in general and sector specific areas[16]. The legislation shall specify when there is a need for both pseudonymised and anonymised data and how to reach this as such, and legislation that should clearly provide requirements for safeguards for sensitive data in general and in specific domains.

The study concludes that a policy decision must be made on whether the harmonisation shall be on an overall level or it should be focuses on the more detailed requirements such as varying or strict interpretations of the concept of scientific research. Overall level here means when to require data anonymisation, pseudonymisation, technical or organisations measures and distinct requirements for special categories of personal data. Detailed requirement refers to whether harmonisation should focus on the more detailed requirements such as varying or strict interpretations of the concept of scientific research, the importance attached to public interest, and consent requirements. The study espouses to the last mentioned – as it is where harmonisation is most lacking and would be welcomed.

The conclusion of the study also shortly points out, that EEA States shall adopt national law specifying the safeguards when personal data is used for scientific research. However, because of the diversity of different ‘scientific research’ categories, the safeguards should always be developed and be seen against the needs and characteristics of each of the scientific research purposes processing operations.

Finally, the study underlines that creating unified rules should be an objective in itself in order to foster cross-border research.

[16] The specific recommendations are lined up at the study's page 64-66

Summary of the article: "Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four Member States and ways to overcome them by EU measures. Insights from Germany, Greece, Latvia and Sweden."

The conclusions (in the article) assume that the GDPR regulation is not fit for the purpose of harmonising the legal framework of data protection. The room for interpretation hence differentiation in national implementation is huge and does not support the potential in 'one-single-rulebook' for data protection. Such problems are identified by analysing four different Member States within different areas of the GDPR enforcement and access to the use of genetic and health data. The foundation among the Member States are similar however, differences in legal approach and structures in the national implementation contribute to diversity.

To solve the major challenge that lies in the lack of harmonisation, the article points out suggestions to handle the future use and access to genetic and health data across the EU. One approach is the structure of the European Health Data Space, EHDS, (anchored in the European Data Strategy), which will create a one-sise-fits-all system intended to be used across the EU. EHDS should be built on three main pillars, 1) unified governance system with clear rules for data exchange, 2) guarantee of high data quality and 3) development of digital infrastructure.

A way forward is to build on the already existing eHealth Network and its infrastructure, but it needs to be supported by initiatives to secure a clearer legal framework – e.g., by implementing Code of Conduct and strengthening the harmonisation by secondary acts. The latter in respect of the principles and limitations that lies within the area of shared competence, which is the case for the GDPR-regulation. Eventually the current GDPR legal framework and lack of harmonisation leads to the necessity of establishing centralised tools which gives the potential to deal with uncertainties that lies in the national implementation – however it will all rely on the willingness among Member States to support a more centralised system.

Appendix 2. Summary of country specific interview answers

Appendix 2 is a summary of six countries answers to selected questions in the deep interviews in work package 5.2. The following questions comprise the summary:

- Has your country a national legislation on secondary use of health data?
- What is the legal basis for the legislation in your country?
- Are there any protective measures applied in your country?
- Does your country have, or plan for, a node for handling secondary use of health data on a national level?

Below summaries of the questions part of the interviews with Aragon (Spain), Czech Republic., Finland, France, Germany and Latvia, respectively

France

Has France a national legislation on secondary use of health data?

Yes, secondary use of health data in France is provided through a new law which was passed in July 2019. The French Health Data Hub is a result of that law. The law was in turn a result from a report about AI technology in 2018 by the deputy of the French parliament Cédric Villani exploring the different facets of AI technology, particularly in the health sector. As an outcome from the report, the French government decided to write a bill, preceded by a prefiguration report of a health data hub made by the French ministry of health. (DECREE Arrêté du 29 novembre 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé » - Légifrance (legifrance.gouv.fr))

What is the legal basis for the legislation?

The legal basis for the legislation is “public interest”, but there is no definition of public interest in the law. It is stipulated in the law that the ethical review board is the authority in France who decide whether or not a project involving health data is in the public interest. The French law states that when there is a public interest, there is no need for consent from the data subjects, but their prior information is required by the GDPR.
Private entities can also rely on public interest as a legal basis. In France private companies can get access to the data by proving their research fulfils public interest. They must describe in their request to the ethical review board how their project relying on health data have a public interest. There can be both public and private interests at the same time. Finally, it is the ethical review board who decide if the arguments fulfill public interest.

Are there any protective measures?

In France there is an authorization system to be passed in order to get access to health data. The project leader must file a request to the Health Data Hub for access to data for a project. The authorization system doesn’t rely on the Health Data Hub, which is only the one-stop shop, but there is an independent ethical review board who gives an opinion based on what the data should be used for, the goal of the the project, who will have access to the data, how long data will be used etc, and then it is the French authority for data/privacy protection (CNIL) who gives the authorisation.
The data is pseudonymised by the data holder before it is provided to the project leader by the Health Data Hub on its technological platform or directly by the data holder if another secure environment is available. The French law does not allow access to raw personal data (i.e.,

directly identifying data) and therefore the French Health Data Hub doesn't handle raw (personal) data (i.e no first name, no last name, no date or place of birth, no social security number, no contact information).

Does your country have, or plan for, a node for handling secondary use of health data on a national level?

The French Health Data Hub is a national node for health data and was launched in 2019 and replaced the national institute for health data (INDS) who didn't have a technological infrastructure and didn't process data. The French Health Data Hub does not have the role in France to give permission for secondary use of health data. Their role is to enable project leaders to easily access non-nominative data hosted on a secure platform, in compliance with regulations and citizens' rights. Thus, project leaders are able to cross-reference and analyse the data in order to improve the quality of care and patient support.

Finland

Has Finland national legislation on secondary use of health data?

Finland has an act on secondary use of health and social data. The legislation came into force April 2019. At the same time, Finland revised the act on national institute for health and welfare. There were two aims for the development of the legislation; one was about how to develop the social and healthcare databases for the renewing the social and health care system and for the patients' benefit and the second was how we can develop the legislation for secondary use of health data especially for research, development and innovations.
The legislation forms from several backgrounds: two national strategies, the social healthcare reform in preparation process at that time, an international review on Finland's use of health data, and a legal perspective. From a legal perspective old health care register legislation has to be revised to follow constitutional law, and GDPR. The result was the Act on secondary use of health and social data and a revised act on national institute for health and welfare. The first national strategy on the use of social and health care data (2014) focused on how to utilise better social and healthcare data. The second strategy on the health growth, also in 2014, was concentrating on the development of research and innovation system in Finland.
Three related acts in Finland complement the acts mentioned above. Firstly, a reformed biobank legislation has been drafted and is prepared for the Finnish parliament late 2022. Secondly, a genome centre legislation is prepared and thirdly, an act on clinical trials has been revised which involve both primary use and secondary use.

What is the legal basis for the legislation?

The legal basis for secondary use is the legal obligation to secure and protect the individual sensitive data. Primary data collection has different legal basis which are defined in the social and health service legislation and in the client and patient data legislation.

Are there any protective measures?

Findata gives the permit for the use of data and combines data from different data controllers. Other authorities for example university hospitals, can give permit for accessing their data, but if data is needed from different sources for combination, Findata needs to be involved. When a permission is received from Findata data is collected, pseudonymised or anonymised and transferred to a safe and secure process environment (SPE) within the Findata system or to another audited safe and secure environment.

Findata provide services for pseudonymisation of data and store the pseudonymisation key to the data. They also control the data access and who has the right to access to the safe and

secure environment. When applying data for research purposes from Findata an ethical approval is needed. Ethical committees in Finland are in research organisations. Findata decides what data variables will fulfil the applicants needs. As a result, data user can have pseudonymised data, anonymised data or aggregated statistics.

Does your country have, or plan for, a node for handling secondary use of health data on a national level?

Findata has been a national node for secondary use of social and health data since 2019.

Aragon (Spain)

Has Spain a national legislation on secondary use of health data?

Spain doesn't have one legislation but several that addresses the secondary use of health data. In Spain there is legislation on medical research (Law 14/2007 on Biomedical Research), GDPR and legislation on Protection of Personal Data and guarantee of digital rights (the Organic Law 3/2018).

Several legal texts have been enacted, adjusted or interpreted regarding the secondary use of data. In particular, the Organic Law 3/2018, of December 5, of Protection of Personal Data and guarantee of digital rights, specifically tackles the use of pseudonymised personal data for research in biomedical research in its Additional Provision 17ª.2.

For the regional dimension, the BIGAN platform was established by the Aragón Regional Health Authority by Executive Order (SAN/1355/2018).

What is the legal basis for the legislation?
For BIGAN public interest and legal obligation are the basis for the legislation.

Public interest. According to the Protocol for access to data for research approved by the BIGAN Oversight Committee (December 2019), the pseudonymised data is accessible, within the context of a research project, directly to researchers within the "R&D Aragonese system" (as defined by regional law 17/2018); and indirectly accessible by other researchers (either public or private), when an agent of the R&D Aragonese system actively participates.
Direct access to non-R&D Aragonese agents and other stakeholders can be also granted, although requires specific authorisation by the BIGAN Oversight Committee in the light of the criteria of relevance, security and social interest.

There is an opt-out system: according to article 3.2 of the BIGAN Executive Order, is the patient right to opt out from the BIGAN infrastructure making possible to decide on whether they want to allow researchers to use their data.

Are there any protective measures?
The Spanish data privacy legislation is very specific about all steps on safeguards; the impact assessments, the ethical review, minimisation, the technical and functional separation.
In Aragon, when you want to have the data from BIGAN for research you have to define the purposes within a research protocol and present a Data Management Plan. Then you will have your application submitted to the ethical board in Aragon (CEICA) as an additional safeguard for the process. In Spain, there is mutual recognition on ethical board´s decisions in different Spanish autonomous regions.
There is a technical and functional separation between the research team (users), the BIGAN personnel at the BIGAN Platform, and those (data controllers) who carry out the initial pseudonymisation and keep the information that enables re-identification.

Does your country have, or plan for, a node for handling secondary use of health data on a national level?

There is no national node yet. Aragon is an autonomous region responsible for a regional node called BIGAN. The Spanish government is paving the way towards the Spanish national health data space.

Czech Republic

Has the Czech Republic a national legislation on secondary use of health data?

Currently, in 2022, there is no specific national legislation regarding on secondary use of health data. There is a legal framework regulating the provision of health services, Act 372/2011 Coll. on health services, which, among other things, regulates "health documentation", dealing with it, viewing it, making extracts or copies of it. This act also defines the National Health Information System (NHIS). The NHIS is a unified national information system of the public administration intended to process data on the health status of the population, on the activity of providers and their economy, on reimbursements for health services covered by public health insurance and for other purposes, all in order to support management and development of healthcare in the CR. Tasks in the area of ensuring operation of the NHIS are performed by the Institute of Health Information and Statistics of the Czech Republic (IHIS CR). NHIS also includes management of the National Health Registers and other essential registries used in healthcare.

The Act regulates certain aspects of the use of the data in NHIS also for the needs of science and research in the field of health. There are basic rules for requesting data and for providing data from the NHIS for research. Any reimbursement for the effort expended is in an amount that may not exceed the costs associated with the collection or preparation of the data.

The legal framework for secondary use of health data in general is considered not sufficient both by the data holders and the users. There is significantly prevailing opinion that the national legal framework should be clearer and access to health data for secondary use should have proper governance. There is awareness that legislation for secondary use of health data needs to be developed or improved. The concept of future HDAB as defined in the proposal for Regulation on EHDS is still under discussion in 2022.
A national project financed by EU RRF funds “Secondary use of health data” is planned by the Ministry of Health for 2023 to 2025. It also includes – as a first Task – a revision of the legal conditions and a proposal for a new legal framework for the secondary use of health data in the Czech Republic, prospectively compatible with the Regulation on EHDS. There is awareness that legislation secondary use of health data needs to be developed soon.

What is the legal basis for the legislation?

Currently it is generally based on explicit patient’s consent for use of health data (besides data collected in health registries). Other models for accessing health data for research are occasionally discussed, particularly by data users. There is an argument for using a different legal basis, e.g., so-called legitimate interest where patient consent cannot be obtained. However, public interest can hardly be used as a legal basis – it lacks a national legislative framework for what falls within the public interest, it is so-called vague legal term. In other fields, for example when deciding on the location of new buildings, the content of this term

must be assessed on a case-by-case basis by an administrative body itself in each individual case.

Within the national registries of NHIS there are possibilities for reuse of the data based on certain obligations set in Act No. 372/2011 Coll. The applicant can apply for access to the data at Institute of Health Information and Statistics of the Czech Republic (IHIS CR).
There is no other legal regulation for the re-use of personal health data of health service providers and other entities in the health sector for research, apart from Act No. 110/2019 Coll. (Personal Data Processing Act – GDPR), provisions of which are considered insufficiently clear and detailed for unambiguous application.

Are there any protective measures?

Ethical reviews are mandatory, they but follow pertinent international standards. The Ethical committees are at different places, typically at hospitals– and the researchers can used which ever they want. Sometimes it is up to the Data Protection Officer (DPO) of the data granting institution to give the permission, and sometimes ethical consent is sufficient.

Does your country have, or plan for, a node for handling secondary use of health data on a national level?

There is a lot of work done for establishing the national contact point for primary use of health data and its interconnection with other contact point in EU countries – the basic infrastructure for cross boarder sharing health data – but it is rarely used as there is no established EHR and the most connected subjects to the point in the CR are advanced hospitals with their hospital information systems (HIS). These healthcare providers can send nationally specified patient summary, which is based on selected specifications developed within eHealthNetwork.

Current national contact point for primary use of health data is capable to handle patient summary and ePrescription/Dispensation. Vast majority of health data holders, particularly in primary care is not connected. Discussion about national contact point for secondary use of electronic health data are about to start soon in 2023.

Biobank research Infrastructure (BBMRI.CZ) is active in the establishment of the Czech National Node of the European biobank infrastructure BBMRI-ERIC, which was founded by the Ministry of Education, Youth and Sports. The goal of the Czech BBMRI infrastructure is to operate a network of medical research biobanks that store biological samples from oncology patients for a long time under secure, standardised and accredited conditions. This activity is complemented by efforts to catalogue available data sets on biomaterials and make them available for research. Establishment of this research infrastructure in the CR follows Commission Implementing Decision 2013/701/EU of 22 November 2013 on setting up the Biobanks and Biomolecular Resources Research Infrastructure Consortium (BBMRI-ERIC) as a European Research Infrastructure Consortium. The biobank is operated under Agreement on the provision of targeted support on the solution of a large research infrastructure project with the Ministry of Education, Youth and Sports.

Latvia

Has Latvia a national legislation on secondary use of health data?

There is an initial draft on a law for secondary use and will be reviewed by a working group in the parliament. Previous legislation for secondary use of data was outdated and the possibility to collect data was in separate laws and not in one central. In addition to the law there was

also several decentralized lower lever of laws. The laws where there to limit the use of the data – most of it needed consent for research.

What is the legal basis for the legislation?

Public interest that can be used for the granting the access to the secondary use.
The law will not make a distinction between whether it is a public or private entity – it must meet certain criteria for public interest.

Are there any protective measures?

The institution would give the data permit. In the draft law Findata was taken as an initial model. It is not yet cleared when to give access to anonymized or pseudonymized data and are not defined yet. Linkage of data could be through the institution. To get access to data in Latvia there is ethical review boards to pass.

Does your country have, or plan for, a node for handling secondary use of health data on a national level?

They have not come this far yet, but the draft suggests that there should be an institution that gives data permit like Findata. They have had videoconference with Findata and based on their experience created their ideas and guidelines that now are drafted in to the new law suggestion. The law will have a broad approach on which data sources it will host.

Germany

Has Germany a national legislation on secondary use of health data?

There is sector specific legislation on secondary use of health data on both the federal level and on the level of the 16 federal states.

On the basis of the federal competence on social security and social insurance there is legislation in the Social Code Book V (health insurance), which allows the secondary use of “social data”, for example the use of claims data from the statutory health insurance for research, for improving health care and other purposes.

Apart from this, there are number of sector-specific laws that regulate data processing in health and/or secondary use of data, either in federal law (e.g. on gene diagnostics, clinical trials, medical products, pharmaceuticals, etc.) or in the state laws of the 16 different states (i.e. state hospital and data protection laws).

In order to promote secondary use of data two legal measures are part of in the current government agreement in order to further develop the secondary use of health data, both legal measures are currently in preparation. One will address health data use in general with the aim of improving the conditions for secondary use of data, the other legal measure is specifically aiming to clarify the legal basis on which medical registries can process data.

What is the legal basis for the legislation?

Depending on the respective purposes, the federal and state laws governing secondary use of health data have their legal basis in the German constitution, which clarifies, which areas

are governed by federal or state law. With regard to the General Data Protection Regulation (GDPR), the respective laws are based on Art. 6 (1) c or e in combination with Art. 9 (2) h, i or j of the GDPR. As many areas of data protection and healthcare provision fall within the competence of the federal states, there are different legal bases for data use at state level, which make use of the respective opening clauses of the GDPR but lack coherence when applied across different states. Without specific sectoral European legislation on secondary use of health data, implementation of GDPR remains heterogeneous between states.
Thus, often the legal requirements for secondary use is not very clear, as GDPR, as well as sectorial federal and state health law need to be consulted. The sole reliance on informed consent, as used in e.g. clinical research, is widely used, but also has its limitations in situations where getting informed consent from the patient is difficult, for example when registries that need data from patients in acute care and intensive care, but also in the general hospital setting.

In general, the perceived lack of legal certainty and clarity sometimes leads to researchers not using data because they fear legal consequences. Hence, a common coherent governance on data access and data use is needed.
One major influence on further developing national legislation will be the European Health Data Space Act (EHDS).

Are there any protective measures?
Data processing is in line with GDPR and the national data protection regulations. The laws foresee extensive legal, technical and organisational measures. Data protection measures concerning the technical and organizational aspects are developed in close cooperation with the federal data protection office and the federal office for information security.
For the claims data, health data access is provided through a secure processing environment based on national regulation in the Social Code Book V. The protective measures include (amongst others):

- Double pseudonymization
- Use of a trusted third party for the pseudonymization process to separate data containing medical information from potentially identifying data in order to minimize the risk of re-identification
- No handing over of the data to the researcher, but use of secure processing environments where the technical specifications are designed in close collaboration with the federal office for information security
- Anonymization checks with respect to the results being published
- Sanctions and penalties of any attempts to re-identify individuals from health data with up to one year of imprisonment

Does your country have, or plan for, a node for handling secondary use of health data on a national level?

There is no national node yet. The coalition agreement announced a decentralized system where the data stays with the various data holder. This is considered favourable compared to a centralized data node especially concerning data security and data protection.

The vision is to centralize information on accessible data and access procedures in order to get an overview of what health data actually exist in Germany and what are the prerequisites for using it. This centralized platform could then refer to the various data holders.

Germany (represented by the Health Data Lab at the Federal Institute for Drugs and Medicinal Products) is also part of the EHDS2 pilot project, led by the French Health Data Hub, where cross-border use of secondary data is being piloted.