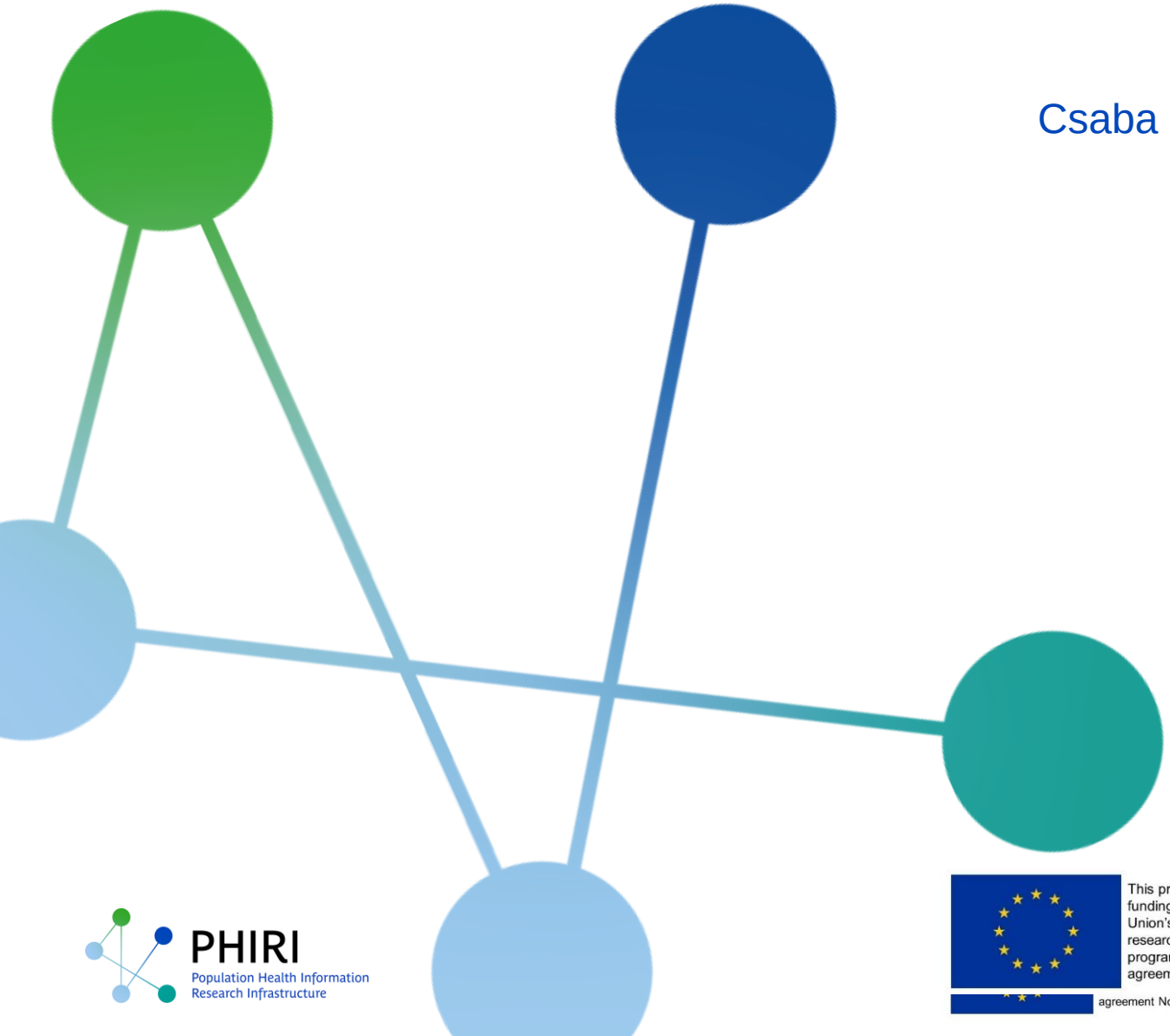
PHIRI
Population Health Information Research Infrastructure

A toolbox how to transfer existing practices and guidelines on ethical and legal aspects

D4.5 – October 2023

Csaba Kiss



PHIRI
Population Health Information Research Infrastructure

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

agreement No 101018317

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

PHIRI: A toolbox how to transfer existing practices and guidelines on ethical and legal aspects

Contributors: Csaba Kiss

I. Introduction

The ELSI (Ethical, Legal, and Social Issues) Toolbox aims to guide researchers on existing practices and guidelines on ethical and legal aspects of handling and exchanging health information. The toolbox provides recommendations on how to translate these learnings into practical implementation.
The Toolbox was built based on outcomes from studies and reports produced under grant and service contracts with CHAFEA and DG SANTE regarding possible differences between Member States' rules governing processing of health data and identifying elements (e.g. through code of conduct) that might affect the cross-border exchange of health data in the EU.

A. Legal and ethical framework

This section of the ELSI Toolbox offers a summary of the **legal framework** implemented in the EU/EEA area, which regulate the sharing of personal data, as well as legal interpretation and practical issues within the EU data protection framework. Furthermore, the ELSI Toolbox contains a collection of **ethical recommendations and rules** in the field of scientific research.
In addition to the framework of legal and ethical rules, the **legal practice** concerning the research and transmission of personal health data in the European Union has been established. This includes the opinions and recommendations of the European Data Protection Board and the European Data Protection Supervisor regarding the interpretation of the GDPR and its legal practice.
A summary has also been compiled of the data protection (General Data Protection Regulation; GDPR) issues and challenges of scientific and other research, regarding research projects within the European Union. In the summary, we collected information about the basis for possible transfers of data outside the EU or EEA too.

B. Research on available best practices, guidelines and recommendations

This section of the Toolbox contains web research, and online workshops with providers of available guidelines and best practices on ethical and legal aspects of transmission and exchange of healthcare-related data/ health information on COVID-19 in and out of the EEA area, as well as consulting with stakeholders including national authorities.
The systematic research approach is described in the uploaded article '*A systematic approach to searching: an efficient and complete method to develop literature searches*'. The key **research documents** and articles that were identified have been **uploaded** on the Health Information Portal.

C. Use case-related best practices and recommendations

Through PHIRI, a sustainable and coherent supply of European comparative health data and research will allow for identification of common challenges, exchange of best practices and generation of new research insights on the impact of COVID-19. The PHIRI Work package 6 (WP6) contains Use cases that focus on selected aspects of:

a) vulnerable population groups and risk factors
b) delayed medical care in cancer
c) perinatal health outcomes, and
d) mental health outcomes.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

General learnings about ethical and legal interoperability of cross-border exchange of health, healthcare and health related data are complemented by **findings** about data sharing, access and processing related to the specific Use cases of PHIRI WP6. The best practices on processing of health data are based on results of online **survey** interviews and country visit findings of the Use case groups in respective countries and authorities.

The Use cases may demonstrate how a broad variety of health data (e.g. administrative) can be pooled and/or reused in a federated way across Europe to produce actionable insights.

II. Legal – ethical framework

- Legal framework
  - Scientific research and data protection
  - Data protection
    - Definition of Key Terms
    - Data protection principles
    - Personal data
    - Pseudonymised and anonymised data
  - Legislation
  - Secondary use of personal health data
  - Cross-border processing special categories of personal data
  - Legal practice
  - Scientific research roadmap
- Ethical guidelines

PHIRI serves researchers as well as primary users which are in COVID-19, public health and population sciences or other connected fields. The Research Infrastructure enables researchers and their communities to perform excellent cross-disciplinary and data-intensive research on the direct impact of COVID-19 on COVID-19 patients, and on the indirect impact of COVID-19 on the general population.
The research projects are necessarily situated in a legal environment. A series of legal and ethical rules determine the feasibility of such scientific research projects. The most important element of the legal framework is the **data protection provisions**.

Scientific research and data protection

The protection of personal data is part of the common European constitutional structure, its basic principles are laid down in Article 8 of the Charter of Fundamental Rights of the European Union. The GDPR provides a high degree of protection.
Scientific research depends on the exchange of ideas, knowledge and information. Where it involves the processing of data concerning people in the EU, scientific research is subject to the applicable rules including the **General Data Protection Regulation**, the Regulation 1725/2018 for EU institutions and the national data protection legislation. The rules contain a special regime affording a degree of flexibility for genuine research projects that operate within an **ethical framework** and aim to grow society's collective knowledge and wellbeing. How this special regime should operate in practice is under discussion. Some argue that the GDPR offers too much flexibility, others that the rules threaten vital research activity.
Digitisation has made the generation and dissemination of personal data easier and cheaper than ever and transformed how research is carried out. The boundary between private sector research and traditional academic research is blurrier than ever, and it is ever harder to distinguish research with generalisable benefits for society from that which primarily serves private interests. Corporate secrecy, particularly in the tech sector, which controls the most valuable data for understanding the impact of digitisation and specific phenomena like the dissimilation of misinformation, is a major barrier to social science research.
In the particular field of health science, medical research and clinical trials generally take place within an established framework of professional ethical standards. The interaction between this framework and the GDPR is being discussed within the European Data Protection Board.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

Data protection

Data protection protects individual rights when personal data is processed. Everyone has the right to the protection of their personal data. The purpose of data protection is to define when and under what conditions personal data can be processed. The processing of personal data must always be based on legislation. Compliance with the regulations on the protection of personal data is supervised by independent national authorities. Any sharing of personal data, whether at a national or international level, involving European jurisdictions and data subjects, must comply with the provisions of the GDPR.

Definition of Key Terms

- **Personal data**
- Processing - The term “processing” refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.
- Data Controller - A “data controller” refers to a person, company, or other body which decides the purposes and methods of processing personal data.
- Data Processor - A “data processor” refers to a person, company, or other body which processes personal data on behalf of a data controller.
- Consent - Some types of data processing are carried out on the basis of consent. Under the GDPR, consent to processing of personal data must be freely given, specific, and informed. Individuals cannot be forced to give consent, information regarding what purpose(s) the data will be used for must be given. Consent should be given through a ‘statement or as a clear affirmative action’ (e.g. ticking a box).

  Consent is not the only lawful basis on which individuals personal data can be processed. Article 6 of the GDPR sets out the complete list of lawful reasons for processing personal data as:

  1. Consent.
  2. To carry out a contract.
  3. In order for an organisation to meet a legal obligation.
  4. Where processing the personal data is necessary to protect the vital interests of a person.
  5. Where processing the personal data is necessary for the performance of a task carried out in the public interest.
  6. In the legitimate interests of a company/organisation (except where those interests contradict or harm the interests or rights and freedoms of the individual).*

  *It is important to note that Article 6(1)(f) provides that the "legitimate interests" reason is not available to public authorities where the processing is being conducted in the exercise of their functions.
- Profiling - Profiling is any kind of automated processing of personal data that involves analysing or predicting your behaviour, habits or interests.
- Special categories of personal data - Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as “special categories” of personal data. The special categories are:

  1. Personal data revealing racial or ethnic origin;
  2. Political opinions;
  3. Religious or philosophical beliefs;
  4. Trade union membership;
  5. Genetic data and biometric data processed for the purpose of uniquely identifying a natural person;
  6. Data concerning health;
  7. Data concerning a natural person’s sex life or sexual orientation.

  Processing of these special categories is prohibited, except in limited circumstances set out in Article 9 of the GDPR.
- Data Protection Officer (DPO) - The GDPR requires data controllers and data processors to appoint a Data Protection Officer (DPO) in certain circumstances. A data controller can also voluntarily decide to appoint a DPO.

Data protection principles

The data protection principles must always be observed when processing personal data. The controller must also be able to demonstrate the effective implementation of the data protection principles in the processing of personal data.
The data-protection principles state that personal data must be

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected and processed for a specific and lawful purpose;
- collected only to the amount necessary with regard to the purpose of the processing;

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101018317

- updated when required – inaccurate personal data must be erased or rectified without delay;
- kept in a form which only permits the identification of data subjects for as long as is necessary for the purposes of processing the personal data; and
- processed confidentially and securely.

All activities involving personal data, from the planning of processing to the collection, processing and erasure of personal data, constitute processing of personal data. The data protection principles must be adhered to for the entire duration of processing.

Personal data are any information which are related to an identified or identifiable natural person. (GDPR Article 4 (1)). In other words, data that can be used to identify a person directly or indirectly, such as by combining an individual data item with some other piece of data that enables identification, are personal data. Persons can be identified by their name, personal identity code or some other specific factor.
The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data.
Since the definition includes "any information" one must assume that the term "personal data" should be as broadly interpreted as possible. This is also suggested in case law of the European Court of Justice, which also considers less explicit information, such as recordings of work times which include information about the time when an employee begins and ends his work day, as well as breaks or times which do not fall in work time, as personal data. Also, written answers from a candidate during a test and any remarks from the examiner regarding these answers are "personal data" if the candidate can be theoretically identified. The same also applies to IP addresses. If the controller has the legal option to oblige the provider to hand over additional information which enable him to identify the user behind the IP address, this is also personal data. In addition, one must note that personal data need not be objective. Subjective information such as opinions, judgements or estimates can be personal data. Thus, this includes an assessment of creditworthiness of a person or an estimate of work performance by an employer.
Last but not least, the law states that the information for a personnel reference must refer to a natural person. In other words, data protection does not apply to information about legal entities such as corporations, foundations and institutions. For natural persons, on the other hand, protection begins and is extinguished with legal capacity. Basically, a person obtains this capacity with his birth, and loses it upon his death. Data must therefore be assignable to identified or identifiable living persons to be considered personal.
In addition to general personal data, one must consider above all the special categories of personal data (also known as sensitive personal data) which are highly relevant because they are subject to a higher level of protection. These data include genetic, biometric and health data, as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership.
The GDPR protects personal data regardless of the technology used for processing that data – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

Examples of personal data

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

*Note that in some cases, there is a specific sectoral legislation regulating for instance the use of location data or the use of cookies – the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002(OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004) of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1)

Examples of data not considered personal data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

- a company registration number;
- an email address such as info@company.com;
- **anonymised data**.

Pseudonymised data

'Pseudonymisation' of data (defined in Article 4(5) GDPR) means replacing any information which could be used to identify an individual with a pseudonym, or, in other words, a value which does not allow the individual to be directly identified.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information. Such additional information must be kept carefully separate from personal data. Pseudonymised data can still be used to single individuals out and combine their data from different records.

The encoding of personal data is an example of pseudonymisation. Encoded data cannot be connected to a specific individual without a code key. For the holder of the code key, however, decoding the records and identifying each data subject remains a simple task. Personal data can also be protected with false names. For example, a data item related to the individual can be replaced with another in a database. Pseudonymisation is a commonly employed method in research and statistics.

They are still personal data and their processing is subject to data protection regulations.

Example of Pseudonymisation of Data:

	Student Name	Student Number	Course of Study
Original Data	Joe Smith	12345678	History
Pseudonymised Data	Candidate 1	XXXXXXXX	History

Anonymised data

Anonymisation refers to the processing of personal data in a manner that makes it impossible to identify individuals from them. For example, the data can be rendered down to a general level (aggregated) or converted into statistics so that individuals can no longer be identified from them. The prevention of identification must be permanent and make it impossible for the controller or a third party to convert the data back into identifiable form with the information held by them.

Anonymisation must take into account all reasonably viable methods for converting the data back to an identifiable form. Factors such as the costs of identification, time required to identify the data subjects and available technologies must be taken into consideration in the assessment of the possibility of identification. The controller must also prepare for the eventuality that the passage of time and advancement of technology could weaken the anonymisation.

Fully ‘anonymised’ data does not meet the criteria necessary to qualify as personal data and is therefore not subject to the same restrictions placed on the processing of personal data under GDPR. Data can be considered ‘anonymised’ when individuals are no longer identifiable. It is important to note that a person does not have to be named in order to be identifiable. If there is other information enabling an individual to be connected to data about them, which could not be about someone else in the group, they may still ‘be identified’. In this context, it is important to consider what ‘identifiers’ (pieces of information which are closely connected with a particular individual, which could be used to single them out) are contained in the information held.

Where data has been anonymised, the original information should be securely deleted to prevent any reversing of the ‘anonymisation’ process. In most cases, if this deletion does not take place then the data is classified as ‘pseudonymised’ rather than ‘anonymised’, and is still considered personal data.

Data protection law does not prescribe any particular technique for ‘anonymisation’, so it is up to individual data controllers to ensure that whatever ‘anonymisation’ process they choose is sufficiently robust.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

Legislation

The legislative background of (scientific) research projects sharing of personal data within the EU in relation to Covid also defines the **legal framework** of (scientific) research for the future. A list of key pieces of legislation can be found **here**:

1. GDPR - 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)
2. REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
3. Data Governance Act - REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868
4. REGULATION (EU) No 536/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.
5. REGULATION (EU) 2022/2371 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2371
6. Law Enforcement Directive - DIRECTIVE (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
7. Directive on privacy and electronic communications - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
8. Open Data Directive - Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L1024
9. DECISION No 082/2013/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC
10. European Commission Adequacy decisions on the adequate protection of personal data, Article 45 of the GDPR)

Proposals

11. Data Act - REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068
12. EHDS - European Health Data Space* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0197
13. A European strategy for data - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066

* - legislation in the preparation stage

Secondary use of health data

Health data is a term used to describe all the information generated through the process of delivering healthcare to populations, including disease registries, public health surveys, clinical trial data, insurance claims and electronic health records. The primary use of health data is when health data is used to deliver healthcare and to make decisions about the care of the individual from whom it was collected.

Secondary use of health data is the processing of health data for purposes other than the initial purposes for which the data were collected, thorough the use of aggregated health data from population-level sources –

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

such as electronic health records, health insurance claims data and health registry data – to improve personal care planning, medicines development, safety monitoring, research, and policymaking. An example of this is when researchers re-process clinical and health insurance data to investigate the cost-effectiveness of a service or product. Secondary use of health data, including data on various determinants of health, provides an important resource for decision-making, health system management and improvement, and research.
In the EEA countries based on the GDPR (see Recital 50), the secondary use of personal data is regulated as follows:

- The processing of personal data for purposes other than those for which the personal data were initially collected (original, primary purposes) should be allowed **only** where the processing is **compatible** with those original purposes;
- **No separate legal basis** (other than that which originally allowed the collection of the personal data) is required.

The following should be taken into account:

- any **link** between the **original, primary purposes** (for which the personal data have been collected) and the **secondary purposes** of the intended further processing;
- the context in which the personal data have been collected: relationship between data subjects and the controller, the reasonable expectations of data subjects;
- the nature of the personal data: data concerning health is a special category;
- the possible consequences of the intended further processing for data subjects;
- the existence of appropriate safeguards, e.g. encryption or pseudonymisation of data further processed.

The GDPR creates the legal basis of the secondary use of data processing:

8. If the processing is necessary for **the performance of a task carried out in the public interest** or **in the exercise of official authority vested in the controller**, **Union or Member State law** may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful;
9. Further processing for **scientific research purposes** are considered to be compatible lawful processing operations;
10. The **legal basis provided by Union or Member State law** for the processing of personal data may also provide a legal basis for further processing.

One of the main challenges in the secondary use of data is the GDPR. While it provides a strong foundation for secondary use of health data, governance tools are needed to enable data reuse. For example, codes of conduct, ethics committees, infrastructure for real-world data and real-world evidence, stronger data institutions, and clearer legal frameworks. Greater clarification is needed to harmonise and support the GDPR implementations that enable secondary use of health data. Because secondary use of health data can make use of anonymised, aggregated data at a population-wide level to advance scientific research, several Recitals (such as Recital 157) aim to provide greater clarity on when sensitive personal data (like Health data) can be used for health research. However, individual EU member states may interpret these in different ways. Some accept the findings of Recital 157 and some do not. To clarify some areas of legislation, individual member states have enacted national data-privacy legislation that reflects key characteristics of GDPR but also strengthens or defines other areas such as secondary use of health data. For example, Finland has introduced new legislation to enable secondary use of health data, but in France, legislative guidelines limit recognition of anonymised health data and its use for future research.
At present, GDPR requirements and interpretations across Europe rarely grant approval to data access for research purposes. Greater clarity is needed at a Europe-wide level on appropriate interpretation of GDPR and its implementation for reuse of anonymised health data for research, diagnostic, and personalised healthcare purposes. The recently enacted European Data Governance Act (DGA) opens up new opportunities in this area. The DGA proposes new models for data altruism, meaning citizens agreeing to share their data for research or social good. There is a regulation for a new, dynamic consent-mechanism model that would allow citizens to consent for multiple purposes at the same time.
The Section I of the toolbox deals with the good practices and guidelines on health data transfers. The list of scientific articles includes a summary on the report of the Open Data Institute on the Secondary use of health data in Europe. It presents a tool on how the EEA countries handle the policies for secondary use of health data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

Cross-border processing special categories of personal data

The GDPR applies in the European Economic Area. One of the key goals of common data protection legislation is to ensure the free flow of personal data within the EEA. For this reason, the same rules apply to the transfer of personal data to an EEA Member State as to transfers within a particular EEA Member State. (GDPR Article 4(23))
The rules of the GDPR for the transfer of data to third countries or international organisations are built upon each other in stages. In relation to data transfer, you essentially have to go through these steps until the data manager finds the appropriate legal basis for data transfer. (GDPR Chapter V, Articles 44-49)
The data transfer bases vary according to the situation and the priority of application, and each basis is subject to its own, specific criteria.

1. **Commission decisions on an adequate level of data protection (Article 45 - adequacy decisions)**
   The European Commission shall issue a decision on an adequate level of protection for personal data to the respective jurisdiction or country, a territory or sector within such a country, or an international organisation. A decision by the Commission takes priority over other bases for transfer. **Here** you can find an up-to-date list of adequacy decisions and other current information available.
2. **Standard clauses approved by the Commission (Article 46(2), point (c) and Article 46(2), point (d))**
   Personal data can also be transferred out of the EU and EEA under the standard contractual clauses (SCC) adopted by the Commission. The SCCs specify the obligations of both the exporter and importer of the data.
3. **Binding corporate rules (Article 47)**
   These are common binding rules on the transfer of personal data to third countries within companies in the same group of undertakings or group of enterprises engaged in a joint business activity. The rules are legally binding on both the companies belonging to the group of enterprises and to the employees of these companies.
4. **An approved certification mechanism (Article 42 and Article 46(2), point (f)) or an approved code of conduct (Article 40 and Article 46(2), point (e)) together with binding and enforceable commitments**
5. **A legally binding and enforceable instrument between public authorities or bodies (Article 46(2), point (a)), and Provisions for administrative arrangements between public authorities or bodies (Article 46(3), point (b))***
   If no adequacy decision has been given, data can be transferred with administrative arrangements or international agreements between public bodies. For detailed instructions and additional information on the bases for transfer of data by public bodies, please see the corresponding EDPB guideline.
6. **Contractual clauses subject to the authorisation of the data protection authority (Article 46(3), point (a)) (between controller-processor) ***
7. **Derogations for specific situations (Article 49)**
   In the absence of the above mechanisms, the GDPR allows derogations for special situations:
   a) The data subject has given his or her **explicit consent** to the transfer
   b) The transfer is necessary for the **performance of a contract** or **establishment of a legal claim**
   c) The transfer is necessary for **important reasons of public interest** or
   d) The transfer is necessary to **protect the vital interests** of the data subject or of other persons (where the data subject is physically or legally incapable of giving consent)
   e) The transfer is **made from a register established by law** and intended for consultation by the public or persons having a legitimate interest.

* Subject to the authorisation of the competent national supervisory authority.

Legal practice - guidelines

In addition to the framework of legal and ethical rules, the **legal practice** concerning the research and transmission of personal health data in the European Union has been compiled. This mainly contains the opinions and recommendations of the European Data Protection Board (EDPB) and the European Data Protection Supervisor regarding the interpretation of the GDPR and its legal practice.

- A European strategy for data – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the committee of the Regions, 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

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

- EDPB – Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak - Adopted on 21 April 2020
- EDPB – Guidelines 07/2020 on the concepts of controller and processor in the GDPR - Adopted on 02 September
- EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research - Adopted on 2 February 2021
- EDPS - A Preliminary Opinion on data protection and scientific research – adopted on 06 January 2020
- EDPB - Statement on the processing of personal data in the context of the COVID-19 outbreak - Adopted on 19 March 2020
- EDBP- EDPS - Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries
- EDPB - Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 - Adopted on 25 May 2018
- EDPB - Guidelines 07/2022 on certification as a tool for transfers - Adopted on 14 February 2023
- EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf
- EDPS - Security Measures for Personal Data Processing, Article 22 of Regulation 45/2001
- EDPB-EDPS - Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate)
- Recommendation CM/Rec(2016)8 of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, 26 October 2016
- COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield
- Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, Adopted on 15 December 2020

Scientific research roadmap

A summary has also been compiled of the data protection (GDPR) issues and challenges of scientific and other research, regarding research projects within the European Union and checking the basis for possible transfers of data outside the EU or EEA.

1. Define the research scheme and purpose for processing personal data.

Processing personal data for purposes of scientific research must comply with the requirement of purpose limitation. The purpose of processing personal data must be planned and defined precisely before the start of processing to ensure its lawfulness.
The requirement of purpose limitation specifies that personal data must be collected for a specific, explicit and legitimate purpose. The data may not be processed in a manner inconsistent with this purpose at a later date. Expressions such as "future research" or "your personal data may be used for research purposes" do not convey the purpose of processing personal data clearly enough.
For scientific research, the purpose is usually specified more precisely in the research plan, which specifies the research scheme, material and methods, among other things. The research plan also specifies the data needed for carrying out the study and why such data is necessary for answering the research question. The research plan should also specify whether the study is a cross-sectional study, or a follow-up study that could require the processing of personal data for a longer time. The research plan can also support you in demonstrating compliance with the requirement of accountability.

2. Minimise the processing of personal data.

The necessity of personal data for scientific research must be assessed at the earliest possible stage. Efforts must be made to minimise the processing of personal data. Both the amount and nature of the personal data processed for the study need to be considered.
The GDPR emphasises the need to minimise data, particularly when the personal data is being processed for purposes of scientific research. The personal data must be adequate, relevant and necessary for the purpose of the processing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

Studies should be carried out without using personal data whenever possible. If the data processed for the study is anonymous, such as aggregated statistics, it is not subject to data protection regulations. The goal of anonymisation is to render the data unidentifiable so that individual events cannot be distinguished from it. The prevention of identification must be permanent and make it impossible for the controller or a third party to convert the data back into identifiable form with the information held by them.
The processing of anonymous data is less restricted and safer also from the researcher's perspective. Anonymous data facilitates international cooperation, as differences in the data protection regulations of different countries will not complicate the implementation of the study.
In scientific research, the minimisation of data is often implemented by pseudonymising the data necessary for the study.

3. Choose the basis for processing personal data and ensure the lawfulness of processing.

As a rule, the controller is free to choose the basis for processing (GDPR: *the consent of the data subject; a contract; the controller's legal obligation; the protection of vital interests; a task carried out in the public interest or the exercise of public authority; and the legitimate interests of the controller or a third party*) that is most applicable to the implementation of the study. The processing of special categories of personal data requires a specific basis.
Specific legislation applying to the controller (such as state research institutes) or research project (e.g. clinical trials) can restrict the choice of processing basis.
You should take the rights of the data subject into consideration when choosing the right processing basis, since they vary according to the basis. For example, the chosen basis for processing can make it easier to recruit subjects for the study if the subjects' confidence in the appropriate processing of their personal data is secured through transparency and opportunities to influence the processing. You should also be aware that flexibility in the definition of the purpose of the research is only possible if the basis for processing personal data is consent.
The GDPR permits the processing of personal data for purposes of scientific research on the basis of:
1. The data subject's freely given, specific, informed and unambiguous consent.

- The processing of personal data for scientific research cannot be based on consent if the research subjects are in a vulnerable position, for example due to their illness or age.
- In research, consent is not necessarily related to the basis for processing personal data. Consent can be related to
  - the study's ethical requirements (e.g. consent for participating in the study);
  - another protected interest (e.g. infringing on the research subject's physical integrity such as by taking a blood sample, generally requires consent); or
  - safeguards.

2. Pursuing the controller's legitimate interests if permitted by the results of a balance test.

EU or national legislation can also permit processing on the basis of:

a) The controller's legal obligation
b) The controller's performance of a task in the public interest.

In certain situations, the processing of personal data for the purposes of scientific and historical research can be considered compatible with the original purpose if the appropriate technical and organisational safeguards are implemented in the processing. The controller's processing of personal data for compatible purposes can be based on the same processing basis as the original processing, in which case a new basis is not required. The processing must also be lawful from the perspective of other data protection regulations; a compatible purpose does not justify non-compliance with other data protection regulations. When a controller intends to process personal data for purposes other than the original purpose of processing, it must notify the data subjects of this before starting processing.
As a rule, the processing of special categories of personal data is prohibited. Data such as health information and genetic data belong to special categories of personal data that can be processed if an exception to the prohibition has been provided for in the GDPR or specifically in Union law or national legislation. It is important to recognise whether data can be processed by virtue of the GDPR or whether processing will require separate legislation or agreements in addition to the GDPR.

4. Implement the rights of the data subject.

The rights of the data subject arising from the basis for processing should be considered at the planning stage of the study. Research subjects must be informed of how their personal data will be processed, as well as their rights and how to exercise them. The controller must seek to facilitate the exercise of the data subjects' rights.
When a data subject contacts the controller about their rights, the controller must respond to the data subject without undue delay and not later than one month from receiving the request. In the reply, the controller shall indicate the measures taken due to the request. If the requests are numerous or complex, the controller can reply that it needs more time to process them. In such cases, the deadline can be extended by a maximum of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

two months. Justifications must be provided for the extension. As a rule, the exercise of the data subject's rights is free of charge.
Derogation from the rights of the data subject is only rarely possible. The research subjects must be informed of their rights and the limitation of these rights as early as possible. If the controller refuses the data subject's request, it must notify the data subject of this within one month of receiving the request. The refusal must be justified to the data subject. In addition, the controller must also inform the data subject of the possibility of lodging a complaint with the supervisory authority and the availability of judicial remedies.
With the following three steps, you can determine the rights of research subjects with regard to the processing of their personal data.

a) Determine the rights arising from your chosen basis for processing. Design procedures and define responsibilities for responding to requests related to the rights of data subjects. Data subjects can monitor and influence the processing of their personal data for research purposes by exercising their rights.
b) When planning your study, think about whether the research scheme involves a particular reason for restricting the rights of data subjects. Justify any restrictions of rights and take the necessary measures. Inform the research subjects of the restrictions so that they will not be a surprise. Respond to the queries of research subjects appropriately and tell them why the exercise of their rights is not possible.
c) Even if the research scheme does not require the restriction of data subjects' rights, some requests for the exercise of rights may need to be refused or limited on the basis of general grounds for restriction. Determine the basis for limiting the exercise of rights and notify the data subject of it.

5. Identify the roles and responsibilities for the processing of personal data.

A research project can involve a variety of parties in different roles. Personal data may be processed for research purposes by one or more research organizations, persons in charge of the study, customers, researchers and other personnel. The roles of the various parties with regard to the processing of personal data and the controller's responsibility must be defined clearly before the start of the study.

6. Check the basis for possible cross border transfers of data outside the EEA.

Research is an international activity, and a need to transfer personal data out of your respective country may arise during a project. There is legislation to ensure that the level of data protection does not deteriorate even if a research project requires the transfer of personal data to third countries. These transfer requirements also apply to pseudonymised data.

7. Demonstrate compliance with data protection legislation.

Compliance with the provisions of the GDPR is required when processing personal data. Accountability means that the controller must be able to demonstrate its compliance with data protection legislation and is a key principle of the GDPR.

8. Destroy, anonymize or archive the materials appropriately upon the conclusion of the study.

When a study ends, the controller must ensure that data is appropriately destroyed, anonymised or archived. The GDPR does not specify precise storage times for personal data. The controller must assess the storage time and necessity of the personal data in relation to the purpose of processing in question.

9. Make sure that you are familiar with data protection methods and requirements.

Data protection tools are a necessary part of the researcher's work and competence. Compliance with data protection regulations builds trust and lays the groundwork for future research.

Data protection regulations are an important area in the professional competence of any researcher processing personal data. Data processed in a study can reveal highly sensitive information about the research subjects. Researchers must be worthy of the research subject's trust and update their data protection competencies on a regular basis.

Ethical rules and guidelines

The Toolbox contains a collection of **ethical recommendations and rules** in the field of scientific research.

1. European Convention on Human Rights. 1950. https://www.echr.coe.int/documents/d/echr/Convention_ENG

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

2. Charter of Fundamental Rights of the European Union, 2012. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT
3. Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, 1997. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000 0168007cf98
4. Oviedo Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No. 164) Oviedo 04/04/1997 https://www.coe.int/t/dg3/healthbioethic/Activities/Bioethics%20in%20CoE/ https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=164
5. World Health Organization - Standards and Operational Guidance for Ethics Review of Health-Related Research with Human Participants, 2011. https://www.who.int/publications/i/item/9789241502948
6. WORLD MEDICAL ASSOCIATION DECLARATION OF HELSINKI Ethical Principles for Medical Research Involving Human Subjects https://www.med.or.jp/dl-med/wma/helsinki2013e.pdf
7. All European Academies (allea)..The European Code of Conduct for Research Integrity, 2023. https://allea.org/code-of-conduct/
8. CIOMS.International Ethical Guidelines for Health-related Research Involving Humans. 2016. https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf
9. Council of Europe. Recommendation No.Rec(2004)10 of the Committee of Ministers to member States concerning the protection of the human rights and dignity of persons with mental disorder and its Explanatory Memorandum, 2004. https://www.coe.int/t/dg3/healthbioethic/Activities/08_Psychiatry_and_human_rights_en/Rec(2004)10%20EM%20E.pdf

The **Data Ethics Canvas** methodology by Open Data Institute projects has been used in the **Section I** of this toolbox focusing ethical, legal and societal guidelines and best practices in scientific articles. The D.E.C. helps identify and manage ethical issues – at the start of a project that uses data, and throughout. The Data Ethics Canvas provides a framework to develop ethical guidance that suits any context, whatever the project's size or scope.

External Links
European Data Protection Supervisor ► Security Measures for Personal Data Processing (Link)
European Commission ► What is personal data? (Link)
European Commission ► What personal data is considered sensitive? (Link)
EU publications ► Handbook on European data protection law – Personal data, page 83 (Link)
...

III. Article review - guidelines and good practices regarding the ethical and legal use of data related to the Covid-19 pandemic

About the **selected articles** in the ToolBox – based on the systematic web research - some guidelines and good practices occur regarding the ethical and legal use of data related to the Covid-19 pandemic. The **Table** we have developed breaks down the subjects and essence of the articles in the matrix of the **Data Ethics Canvas** (DEC) by Open Data Institute. (The DEC is a tool for anyone who collects, shares, or uses data. It helps identify and manage ethical issues and encourages us to ask important questions about projects that use data and reflect on the responses. The DEC provides a framework to develop ethical guidance that suits any context, whatever the project's size or scope).

Not only EU coverage, but also USA and Canada jurisdiction have been explored in the selected scientific articles. American regulations regarding data sharing are different, but the personal scope of the GDPR also applies outside the EU. Furthermore, ethical and legal good practices of other legal systems can prove to be good examples comparing to European experiences. In addition to the research ethics aspects (DEC), questions of practical treatment and containment of the COVID-19 epidemic were monitored several times in

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

the articles. It contained the data management issues of the patients and contact persons affected by the epidemic.

GDPR determination

The legal framework of the GDPR and other relevant legislation govern the practical examples and guidelines of the EEA area arising from the articles in the ethical and legislative context.
It is also an important approach that while non-anonymous data are necessary to understand individual risks in an epidemic situation, most research does not require most or all of the personal data. Taking this into account will make it easier to overcome future obstacles generated by the GDPR and various national regulations.
Keeping the focus on EEA jurisdiction, the limitations in data sources cover:

1. The criticism over the adequacy, efficacy, and efficiency of the GDPR, as well as other legal and regulatory mechanisms, which enable the use and sharing of European digital health data (GDPR critiques); national legislation and boundaries.
2. Consent theories and
3. The Cross Border Data Transfers to third countries (not EEA).

Guidelines and good practices upon the articles

The good practices on ethical and legal aspects of transmission and exchange of health information on COVID-19 arising from scientific articles can be compiled as follows. (The findings and good practices are summarized using the Data Ethics Canvas methodology in the attached Excel table /Annex/.)
A relatively new way of sharing data is the **Health Data Cooperative** (HDC). In this case citizens control how their health data should be shared with other entities, citizens hold the right to choose whether they would like to share their personal health data with private industries, hospitals, clinics, research centres, and health policymakers, for clinical trials and academic purposes. The reason for using data is to share health data, such as symptoms, medication course, and the immune response to treatments. In HDC-s, preferably contributed to Cloud (HDCC), data shall be stored in an open cloud platform so that researchers around the globe can share health data and work collaboratively; HDCs ecosystem provides citizens with full control over their health data.
Most research indicates that the simplest way to exchange data is to ask for the patient's consent to the widest possible use of their data at the time of collection. Making changes afterwards can be extremely difficult. Therefore, knowledge of the HDC is particularly important for citizens.

The clinical information systems (CIS) can be and have been utilized to support and enhance the response of healthcare systems to pandemics: electronic health record (EHR); Telehealth; Case Identification; Remote Monitoring, and Screening can also be taken into account. (Storage of patient data, electronic health record (EHR) system utilized; Diagnostic Testing: consent).

Contact tracing applications and movement monitoring using mobile devices are also lucrative ways to collect data on pandemics. The European Commission published its Communication (2020/C 124 I/01) on Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection. The GDPR legislation and general rights to anonymity must be taken into consideration. (Voluntary and mandatory use of mobile applications.)

The determination by GDPR in the EEA jurisdictions has significant impacts on the sharing of health information during the pandemic. Member States, researchers, and data subjects will undoubtedly face **GDPR challenges** : The balancing exercise and interplay between serving the public interest and state surveillance: “ethical trade-offs” must be verified: some limitations on liberty and privacy may be justified in the context of global health emergencies. Privacy first vs data first approaches collide, embedded into prosocial motivations, transparency, and solidarity, causing restriction of individual rights in the name of a public emergency.
Further review/research is recommended to firstly ensure that an understanding of the state of the art in data protection during the pandemic is maintained and secondly support the call that has been expressed for a common multinational database that would support a GDPR and data protection compliant effort into global

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

research. Regarding the reuse of data, the public interest basis has also received criticism due to the lack of a uniform application and interpretation that exists on a national level.

Given the lessons learned, there is a clear and distinct need for a harmonised and collective effort and approach to global research. There was an ethical obligation to use the GDPR scientific research exemption clause during the COVID-19 pandemic to support global collaborative health research efforts. Databases collecting identifiable data for research purposes will be excluded from the scope of the GDPR if the data are later rendered anonymized. There is a strong ethical case that countries use the regulatory leeway the GDPR provides for enabling health data to be used for research purposes and that they support health care organizations and investigators to invoke the research exemption confidently.

Cross-border exchange and transfer of health data from the EEA area for research (ALLEA, EASAC and FEAM initiative)

The GDPR addresses the protection of personal data in the EU and EEA, and the international transfer of personal data outside these areas to "third" (non-EEA) countries and international organisations. It has become apparent that the implementation of GDPR restrictions has created new impediments for academic researchers, health-care professionals, and others in the public sector. Data sharing between the EEA countries and outside remains difficult. Previous advisory groups to the European Commission have emphasised how health research depends on high-quality cross-border collaboration within Europe and beyond, but the impediments to wider international collaboration have remained unresolved. Expectations and messages from the academic organizations include:

- Sharing pseudonymised personal health data for public sector research is essential: it makes best use of limited resources and must be encouraged to maximise the individual and societal benefits to be obtained from the contribution of patients and volunteers to research;
- Data must be shared safely and efficiently, taking account of privacy concerns;
- Implementation of the GDPR has resulted in impediments to data sharing with researchers outside the EU/EEA. The objective of a harmonising framework provided by the GDPR, for processing personal data for research purposes within the EEA, is known. However, there are significant hurdles for sharing data with researchers outside the EU/EEA. It is essential to introduce an operational data transfer mechanism, functioning without further delay.
- There must be increased commitment to finding a solution to overcome the barriers in sharing data: the preferred option is to find a solution under Article 46 of the GDPR with additional operational guidance provided by the European Data Protection Board accompanied by tangible examples to show how to apply the guidance to health research;
- There must also be increased commitment to enabling the use of shareable data;
- Privacy-enhancing technologies are relevant;
- Recommendation for continuing monitoring and assessment AND further international discussion and coordination are needed.

Research under the GDPR – a level playing field for public and private sector research?

Scientific research is indispensable inter alia in order to treat harmful diseases, address societal challenges and foster economic innovation. Such research is not the domain of a single type of organization but can be conducted by a range of different entities in both the public and private sectors. The data protection framework plays an important role in determining not only what types of research may occur but also which types of actors may carry it out. The EU's General Data Regulation determines which types of actors can conduct research with personal data. The GDPR provides a wealth of legal bases for researchers, a 'one size fits all' notion of scientific research however does not exist. Several bases are available to varying types of actor, and the informational obligations/data subject rights may vary according to the legal base used. Many forms of research may use sensitive data, and the GDPR foresees a special regime for sensitive data. Health data is an important example and provides a good illustration of the potential breadth of sensitive data.

The GDPR drafters clearly intended to provide opportunities for various actors, in various contexts to conduct research when certain forms of conditionality are met. This raises the questions as to whether various types

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

of actors (universities; other public bodies; commercial entities) enjoy a level playing field in terms of their ability to conduct research with personal (including potentially sensitive) data.

Among the various legal bases that are available, the GDPR cannot be said to favour research in either the public or private domains. Whilst (assuming there is no serious imbalance in power relations) consent as a legal base is available to all types of entities wishing to conduct research (i.e. both public and private), the same may not be true for other legal bases that are important for research. This incudes bases for processing in the public interest (non sensitive data) and for scientific research (sensitive data). Whilst private sector research may be disadvantaged in terms of its ability to utilise these bases, it has others (e.g. 'legitimate interest') which are not available to researchers acting in the public sector. The 'Further processing' for scientific research option is an extremely broad important provision in the GDPR that should be considered alongside the availability of legal bases.

Secondary use of health data - Covid challenges in Europe

An independent report researched and produced by the Open Data Institute examined the EEA countries (25 EU member states and Israel, Norway, Switzerland, and the UK) in the context of the secondary use of health data as country policy. The report has its findings that open and trusted health data systems can help Europe respond to the many urgent challenges facing its society and economy today. The global pandemic has already altered many of our societal and economic systems, and data has played a key role in enabling cross border and cross-sector collaboration in public health responses. By reusing health data in different ways, we can increase the value of this data and help to enable these improvements. Clinical data, such as incidences of healthcare and clinical trials data, can be combined with data collected from other sources, such as sickness and insurance claims records, and from devices and wearable technologies. This data can then be anonymised and aggregated to generate new insights and optimise population health, improve patients' health and experiences, create more efficient healthcare systems, and foster innovation.

The report clustered the countries in four broad groups: Leaders (where the quality of policy is stronger and the stage of implementation is more advanced), Limited energy (where the quality of policy is stronger but the stage of implementation is less advanced), Limited vision (where the quality of policy is weaker but the stage of implementation is more advanced) and Less prepared (where the quality of policy is weaker and the stage of implementation is less advanced). Overall, there are encouraging signs that European health data ecosystems are maturing to support secondary use of health data. However, many of the initiatives are still fragmented and significant work is needed to establish strong health-data ecosystems and infrastructure for reusing data. Though newer policy developments are looking to coordinate strategies across various stakeholders, initiatives and, importantly, member states (e.g. EHDS proposal).

However, one of the main challenges is the GDPR. While it provides a strong foundation for secondary use of health data, governance tools are needed to enable data reuse. For example, codes of conduct, ethics committees, infrastructure for real-world data and real-world evidence, stronger data institutions, and clearer legal frameworks. The European Commission's European Strategy for Data aims to create a consciously ethical approach, including strict data protection for people, and a commitment to strengthening data access and enabling data sharing for social benefit. Besides the European Strategy for Data, there is much hope placed on the ability of the proposed European Health Data Space (EHDS) to overcome current fragmentation, and create a new open health-data ecosystem for Europe. The EHDS is intended to become 'a system for data exchange and access, governed by common rules, procedures and technical standards to ensure health data can be accessed within and between member states, with full respect for the fundamental rights of individuals.

The ethical policy needs for secondary use of health data in Europe are:

- Standardised models of consent for sharing data
- Clearer harmonisation of GDPR to define processes for data-privacy methodologies
- Established ethics processes

Greater clarification is needed to harmonise and support the GDPR implementations that enable secondary use of health data. The European Data Governance Act proposes new models for data altruism, meaning

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

citizens agreeing to share their data for research or social good. There is a proposal for a new, dynamic consent-mechanism model that would allow citizens to consent for multiple purposes at the same time. At present, GDPR requirements and interpretations across Europe rarely grant approval to data access for research purposes. The establishment of an ethics committee, with patient and consumer participation, would help create the infrastructure needed.

IV. Use case-related best practices and recommendation on the ethical and legal use of data related to the Covid-19 pandemic

The Population Health Information Research Infrastructure (PHIRI) project aims to identify common challenges, exchange best practices and generates new research insights on the impact of COVID-19 pandemic. PHIRI Work package 6 (WP6) contains use cases that focus on selected aspects of:

a) vulnerable population groups and risk factors
b) delayed medical care in cancer
c) perinatal health outcomes, and
d) mental health outcomes.

The methodology of collecting guidelines and best practices has been set up through online survey, direct interviews and country contributions related to the focus group of the use cases.

The online survey collected information for the overview of existing practices and guidelines on ethical and legal aspects of performing and exchanging health information on COVID-19 in the framework of use cases.

Out of **23** partners, **13** filled in the survey (**56,5%**). If we investigate the different WP 6 use cases, **7** partner were participating in the Use case A (Vulnerable population groups and risk factors), **5** in Use case B (Delayed medical care in cancer), **7** in Use Case C (Perinatal health outcomes), and **9** of them in Use case D (Mental health outcomes).

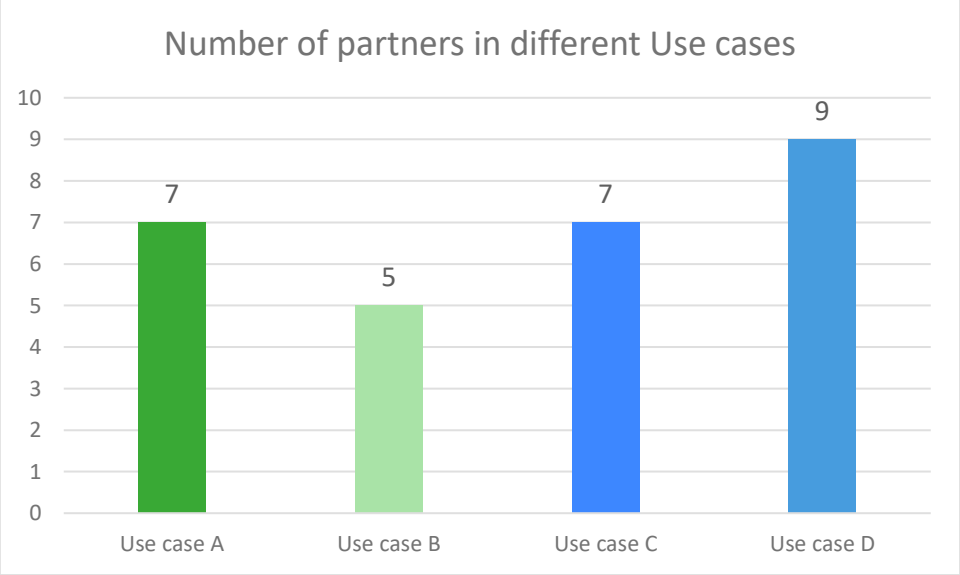


Figure 1: *Number of partners in different Use cases*

Most of them (**11** respondents) marked that, that there is difference between accessing pseudonymised, and anonymous data. '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

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

measures to ensure that the personal data are not attributed to an identified or identifiable natural person [GDPR Article 4 (5)]. 'anonymisation' means the process of changing documents into anonymous documents which do not relate to an identified or identifiable natural person, or the process of rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable [Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information].

Most of the respondents referenced the GDPR (General Data Protection Regulation) as the main reason of the differences between access to anonymized and pseudonymised data. Several partners however mentioned there was a significant difference in practice based on, who requested the datasets. Health professionals and members of national health institutions and their authorised special projects will have easier access to the data concerned. In contrast, there were respondents who indicated that access to personal health data in their country is almost non-existent.

There were questions about the different form of consents and which of them are relevant for scientific researchers in relation to personnel data (the response options were Most relevant; In use; Planned; and Not used). **Six** countries indicated the Opt-out forms as most relevant in practice, two of them indicated the Broad consents, and there was one-one most relevant answers to Targeted consents, Partnership models, and Dynamic consents. The **Figure 2** shows which consent types are still marked as In use by the partners, and how often.

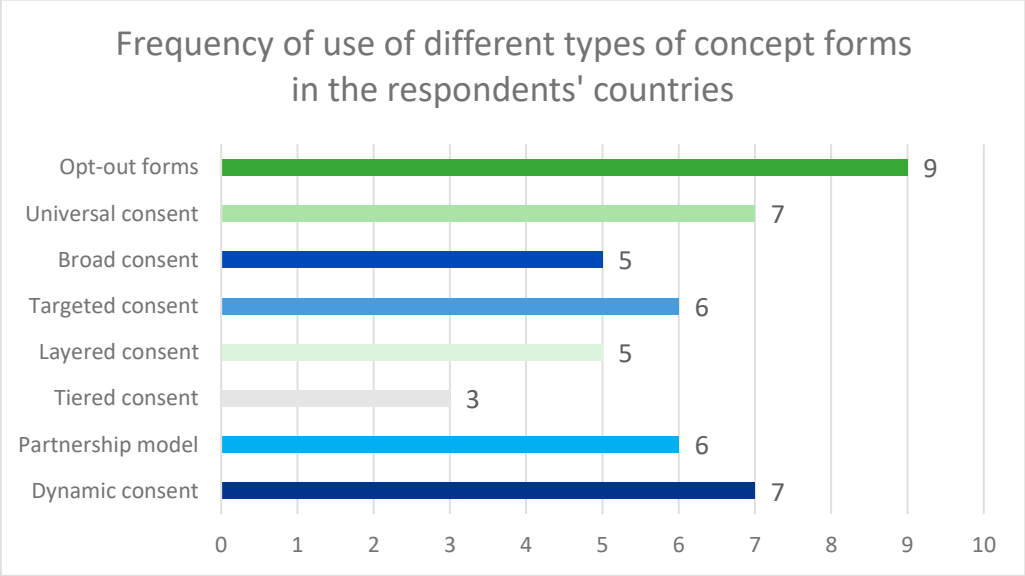


Figure 2: *Frequency of use of different types of concept forms in the respondents' countries*

We also asked about the level of regulation of access to different datasets. For Aggregated data, Social Health Insurance Data, Surveillance data of infectious diseases, and Administrative data, the answer was some kind of centralized, or national level regulatory solution in every cases. It is interesting to note that respondents most often mentioned some kind of decentralized or regional legislation in the topics of Hospital resources and Healthcare resources (**4 out of 13**), Outpatient utilisation data (**4 out of 13**), Biobank/sample/specimen data (**4 out of 13**), Observational study data (**6 out of 13**), and more frequently some kind of Survey/interview data (**7 out of 13**).

About the relationship between the COVID-19 outbreak and the different data sharing rules, **4** respondent mentioned that, there some guarantees have been set up to ensure data sharing, **3** of them mentioned there were developments of pseudonymisation standards/procedures in their countries. **Six** filler mentioned, there was some legislative amendments about the data in the period of the extraordinary regulations (in the pandemic situation), **7** said, there was no changes.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

We also asked respondents what data sources they had access to during the pandemic for the WP6 use cases. Of course, we don't have a clear view of the whole process here. Not all countries are involved in all Use cases, and of course the data needs of each Use case may be very different, and access to them varies from state to state. But it is clear that it was easier for the partners to access the Outpatient utilisation data, the Social Health Insurance Data, and the Administrative data, and maybe the easiest was to reach (marked by the most partner) the Hospitalization statistics of the hospitals of the National Health System, and the different Registry data.

About the mechanisms, which ones are granted the access to these data, the most of the respondents said, they had general permissions from national actors (Public health institutes or ministries), or in some cases, they were the owner of these data. **Three** partner wrote about different regional and local agreements, mostly with different committees, or universities. **Two** partner mentioned, they had some kind of data exchange contract, which shows very future-oriented and innovative attitude.

When asked if there was a specific risk when more than one database were linked, most respondents answered no. Only in two cases was it indicated that there could be a privacy risk, although the use of independent pseudonymised key (Unique personal ID) could be compromised by the link, and some anonymous data could regain personally identifiable properties. This could show that health data controllers are prepared for challenges of this depth.

To the question of using of PHIRI APP or to international data sharing (for example to WP6 use case leaders, or to Orchestrator hub (IACS)), most of the answers said, the IT departments were the responsible unit of internal validation (**6 out of 11** respondents marked this). In addition, one partner nominated the legal department and one the DPO (Data Protection Officer). **Three** partners answered, there was no internal requirement about international data sharing.

In addition to this survey, the countries of the focus group (use cases) interviews and Rapid Exchange Forum questions were conducted about ELSI (Ethical, Legal and Social Implications) practices of data transfer and on the guidelines and best practices, enablers and limitations, and coherent ELSI principles of the countries.

The summary of the relevant country best practices and experiences are shown below in Table 1.

The findings of the interviews and data disclosures were supplemented with data from the European Union member states related to secondary data use using **the countries Profile of ODI report**.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101018317

Table 1: Country responses – Ethical, Legal and Social Issues (ELSI) on Health Data Processing

Country	Topic: Ethical, Legal and Social Issues (ELSI) on Health Data Processing **Q1**: Are there any best practices or specific limitations? **Q2**: Are there efforts for more coherent ELSI principles? **Q3**: Which enablers or which barriers do you experience? **Q4**: Current changes in legislation (e.g. in light of upcoming EHDS regulation)? **+ Additional questions and answers**. • Secondary data use: legislation, challenges, opportunities, good practices
Austria	**Q2**: Some parts of the system can be seen as best practice examples (e.g. the system for individual consent management, or the linkage of many public registries), but to make full use of it the overall coherence and smooth interaction of all parts has to be improved. Currently, several changes to national legislation are being negotiated to reduce administrative and legal barriers. **Q4**: There are a lot of dynamics on the legislation side, also in regard of the EHDS, Austria is working on defining which institution will be appointed as Data Access Body + How have the possibilities / structure of data access changed in your country/region during Covid-19 epidemic? For certain data sources relevant for pandemic management (hospital data, incidence data from testing regimes, vaccination data) a temporary exeption to gather and link data has been enabled via national law. Linkage of individual socioeconomic data is not possible (lack of legal basis). + What is the construction of the general legal and ethical framework related to health data access, use and sharing? The "Forschungsorganisationsgesetz" (law on organizing research),in relation to GDPR, lays down a framework for processing of personal data for certain uses. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009514 • The Federal Ministry of Education, Science and Research (BMBWF) is currently working with the Federal Chancellery (BKA) to implement a government programme with the involvement of Statistics Austria to implement a government programme exploring the provision of a science- and research-friendly register of data for research, with the greatest possible data security. It states: 'Innovative research becomes possible when datasets can be combined and analysed that were previously closed to science. Evidence-based policy and scientific evaluations are also possible with a significantly improved quality. Therefore, an 'Austrian Micro Data Center' and data access for science is to be created.' This might imply that future research (both academic and industry) only enables use of aggregated data and that granularity based on specific characteristics might also be limited. • Two models that demonstrate how data can be managed within ethical and legal structures for secondary use are: Austria's Platform Register for Research (a platform for research based on registry data) and the emerging initiatives to create an 'Austrian Micro Data Center'. • Digital Health Wien initiative is a cooperative network that involves researchers, government, and patients to build a knowledge network on secondary use of health data. • The Covid-19 data platform has been developed by the Federal Ministry for Social Affairs, Health, Care and Consumer Protection and Health Austria, and makes data available relying on FAIR Framework principles. An advisory board has been established to oversee guidance and research teams must apply for access. Researchers are already publishing papers based on data published in the portal.
Croatia	**Q4**: There have been current proposals to the change of legislations (based on the COVID recommendations) in our country;

	1. Law on primary and secondary occupation 2. Amendments to the law on the amendments of general data administration 3. New procedure for the data protection agency 4. Mandatory application of privacy design (user privacy) – so there has been some analysis done Based on Active citizens fund Croatia's „Analysis of practices for data collection and processing during the COVID pandemic - the case of Croatia.“ the key recommendations are: - Amendments to the Law on the Protection of the Population against Infectious Diseases in accordance with Recital 52 of the Regulation, defining a legal basis for exceptions to the prohibition of processing special categories of data for the purpose of preventing or controlling infectious diseases. - Amendments to the Law on the Protection of the Population against Infectious Diseases (or other national regulations, such as the Law on Primary and Secondary Education or the Law on Occupational Safety), in accordance with Recital 45 of the Regulation, to ensure that the legal framework contains all the necessary elements as prescribed by Recital. - Amendments to the Law on the Implementation of the General Data Protection Regulation, eliminating the exemption from the application of administrative fines for public bodies. - A more proactive role for the Data Protection Agency, along with an expansion of the technological capabilities of the body and the implementation of a new procedure for appointing the head of the independent supervisory institution. - Mandatory application of the "privacy by design" principle, the design and development process of digital solutions in which user privacy is the fundamental rule of solution development and the most basic functional pillar, especially when such solutions are commissioned by public authorities. The aim of this analysis is to eliminate unlawful pandemic data collection practices and establish principles of good governance and transparency among institutional actors shaping public privacy policy. The analysis is intended for institutional actors responsible for shaping public privacy policy, independent institutions protecting citizens' human rights, civil society organizations, as well as citizens and the general public. • Croatia’s new ‘National strategic framework against cancer’ recognises the value of health data for secondary uses in early diagnostic cancer screening and personalised healthcare. • National reports for various disease areas are published regularly on the Croatian Public Health Institute (CPHI) website. However, the Cancer Registry has not been updated since 2013. • While Croatia has policy strengths in some areas and is working to create regular reporting of health data registries, especially for cancer, in other areas, such as creating patient-participation schemes for healthcare, strategies are completely silent.
Czech Republic	**Q4**: There has been a recent legislation change, so we can provide health data (as our institute is responsible to provide health data), currently we are oriented mainly on open data (for processing and providing), which we are publishing on our homepage (as discussed with our GDPR experts), so it is not clear yet who is going to be the health data access body. But most probably UZIS. • While aspects of the strategic framework are thorough and comprehensive, it is silent on key issues including establishing an ethical/accountability framework, and on initiatives to ensure public/patient participation in healthcare. • A number of pilot initiatives are currently being implemented that could have national and European-wide importance, including an ehealth platform, for sharing data on individual treatment procedures, and patient-reported health outcome studies.

	• Generally, the collection and protection of secondary data include GDPR principles, and are well developed. Data atomisation is not quite as developed however, and thus is limited in its benefit to society.
Finland	• Finland prioritises the secondary use of health data in legislation (Act on the Secondary Use of Health and Social Data 2019) and sees it as an opportunity to become an international leader in the development of new industry, products and services. • The act makes it explicit that personal data can be protected while also enabling secondary use where data (with appropriate data protection safeguards) is anonymised and de-identified. (Pseudonymised data can be used for scientific research and anonymised and aggregated-level data can be used for research, innovation, teaching, statistics, supervision, regulation, and development and innovation). • Generally, Finnish citizens have high levels of trust in the government and this has aided the success of new legislations and supportive operation models. • The Social and Health Data Permit Authority provides a legal framework for the facilitation of data permit processing and data protection of Finnish individuals.
Hungary	**Q4**: There are no significant law amendments. The EU legislation and recommendation of the instruments, regarding the questions, who is going to be the health data access body (for secondary use) was implemented. The national data protection office will most probably be the national health data access body, but it is not sure yet. • While the creation of an 'artificial intelligence (AI) and ethics knowledge centre' has been earmarked to help resolve legal issues and ethical matters related to secondary use of health data in AI use-cases, it is unclear when this body will be established. • Environments that will require secondary use of health data have been highly prioritised by the Hungarian government: A Digital Healthcare Development Strategy has been identified as a key strategy to be developed as part of Hungary's Digital Success Programme. • Hungary's medicine and pharmaceutical product registers regularly publish new data.
Ireland	• In relation to the secondary use of health data, the Health Research Regulations 2018 set out specific safeguards (as required under General Data Protection Regulation) which must be in place before personal data can be processed for health research, including requirements for explicit consent and prior approval by a research ethics committee. Where the requirement to obtain consent cannot be met, data controllers may apply to the Health Research Consent Declaration Committee for a declaration that explicit consent is not needed as the public interest in carrying out the research significantly outweighs the need for consent. A 2020 government study into the use of health information notes that the Department of Health intends to develop two further sets of regulations on the use of health information for individual care and service planning. • Datasets regularly maintained include the national medicines register and health insurance data and employment sickness data is regularly reported. • The Health Information and Quality Authority (HIQA) in partnership with the Department of Health and the HSE, is conducting a number of public engagement activities to gather the views of people living in Ireland on the collection, use and sharing of health information. These activities include a National Public Engagement Survey on Health Information, interviews with health and social care professionals, meetings with key stakeholders and focus groups with the public, patients and special interest groups.
Italy	**Q1**: Italy moves in the framework of Europe and Italy has accepted the European GDPR regulation. The scientific research/studies which have access and can use health personal data are implemented under an ad hoc decree (in Italian language only): https://www.epicentro.iss.it/politiche_sanitarie/DpcmSorveglianze2017

	https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario;jsessionid=cKSknD1IbT2dY-9SDiNhmA__.ntc-as3-guri2a?atto.dataPubblicazioneGazzetta=2017-05-12&atto.codiceRedazionale=17A03142&elenco30giorni=true Recently, a survey regarding the need of health data interoperability in the research studies was launched among researchers of the National Institute of Health. This initiative is going forward the issue related to the secondary use of health data and related ELSI. **Q2**: However, all the scientific studies collecting personal health data directly on patients and general population, need to collect informed consent signed by the participant; the informed consent, according to the specific study, are becoming as much as complex and comprehensive according to the ELSI issues and the GDPR regulation. **Q3**: Even though the National Institute of Health-ISS is the scientific arm of the Ministry of Health, researchers do not have access to individual personal and health data, except for studies under ad hoc laws/regulations/programs; two examples: - the COVID-19 integrated surveillance system was set up under a special low related to the 'national emergency status' that expired on March 2022; - the national Health Examination Survey is included in the National Statistical Programme; thanks to that, the study has access to mortality individual data including identifier, but only to anonymised Hospital Discharge Records. **Q4**: Italy is collaborating in preparing the proposal for the European Health Data Space (EHDS) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197) with the aim of establishing the European Health Data Space (EHDS) in order to improve access to and control by natural persons over their personal electronic health data in the context of healthcare (primary use of electronic health data), as well as for other purposes that would benefit the society such as research, innovation, policy-making, patient safety, personalised medicine, official statistics or regulatory activities (secondary use of electronic health data). • In December 2018, the General Data Protection Authority introduced new guidelines for secondary use of health data for scientific purposes which appeared to state that it is possible to use data for research purposes if consent has been given or if: A) the researcher undergoes a research ethics assessment and can show that every attempt was made to obtain consent, B) OR can show that pseudonymisation – or another aggregated data process – has been used so the researchers cannot identify the individual, and therefore cannot contact them to obtain consent. • There are currently discussions around whether data institutions should be regional or centrally managed. This creates opportunities to establish data models, standards, guidelines and implementation practices that could be applied at a regional level in ways that support interoperability and the creation of a centralised approach, if a centralised data infrastructure is not proposed. • Regional data sharing platforms have been created and are operating successfully, and could be called up nationally. An oncology data interoperability platform is available to support personalised healthcare decision-making. • Italian GDPR guidelines for secondary use of health data for scientific purposes permit the use of data for research purposes if consent has been given, or if the researcher undergoes a research ethics assessment and can show that every attempt was made to obtain consent. Data must be pseudonymised in instances where the data subject cannot be contacted. • A clear accountability framework is in place with the Italian Data Protection Authority periodically releasing additional guidelines on health data sharing and use.
Poland	**Q4**: The works on the legislative framework are still an ongoing process, because Poland has submitted many comments to the regulation to the proposal, the regulation is still perceived as something positive (ePrescription will definitely make the system better), biggest data owner is the ministry of health, the national public health institute. More recent information with an update will follow.

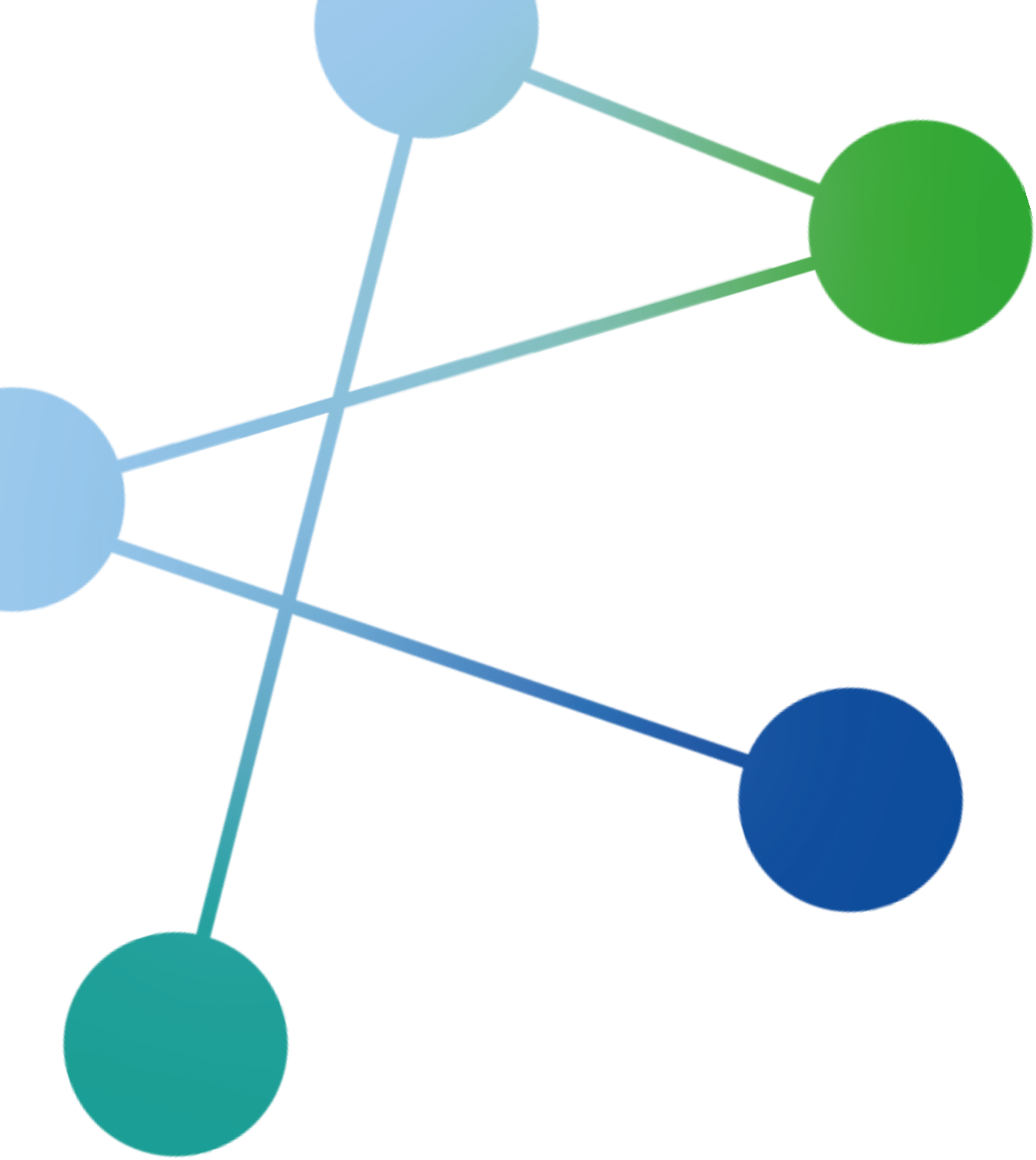
	• Public trust in the healthcare system in Poland is rated one of the lowest in Europe. Legislation in this area is newly established, but further improvement is needed to enable full and complete benefits. • The Polish Act on Patient Rights, and the role of the Patient Ombudsman, do not include specific regulations on the use of secondary data (apart from the basic data object rights as defined in General Data Protection Regulations (GDPR).
Portugal	**Q4**: Ministry of health is holding all the data, they have issued a document with the portugal strategy (end 2022) – one of the major challenges is to integrate the digital ethics – she will send it also for the minutes. Link to the National Strategy for the Health Information Ecosystem: https://www.spms.min-saude.pt/wp-content/uploads/2019/10/ENESIS2022_Version-for-Public-Consultation_Out2019.pdf • 'From Big Data to smart data: putting data to work for the public's health' is the strategy for the next generation of the Portuguese National Health Service. It outlines the vision, key areas, and principles for secondary use of data, advanced analytics and artificial intelligence (AI) to improve the population's health. This strategy is part of the wider eHealth national strategy for 2020 – 2022, that includes a strong focus on the implementation of AI in public and private activities within healthcare. The strategy also identifies new infrastructure and models to build secondary use of health and real world data (RWD) management systems in the medium to long-term. • While Portugal's approach to secondary use of health data suggests one of the most advanced policy environments in Europe, it is also at a nascent stage, where the strategies are well-defined but there is yet to be substantial progress on implementation. A lot of investment will be required, for example, to upgrade EHR infrastructure to enable many of the policy visions. • The national Health Data Strategy recognises the importance of data ethics when establishing secondary use of health data systems. The National Health Data Strategy recognises that AI and secondary use of health data could play a role in understanding bias and social inequities.
Serbia	**Q4**: There are interesting articles about data in Serbia health system: Article 'Impact of the European General Data Protection Regulation (GDPR) on Health Data Management in a European Union Candidate Country: A Case Study of Serbia': https://medinform.jmir.org/2020/4/e14604/ **Case study on Serbia**: - GDPR has also had a notable effect on the European Union (EU) candidate countries, which are undergoing the process of harmonizing their legislature with the EU as part of the accession process. The Republic of Serbia is an example of such a candidate country, and its 2018 Personal Data Protection Act mirrors the majority of provisions in the GDPR. - Serbia generally does not have well-established procedures to support international research collaborations around its health data. - For smaller projects, contractual arrangements can be made with health data providers and their ethics committees. Even then, organizations that have not previously participated in similar ventures may require approval or support from health authorities. - The lack of a framework for preparation, anonymization, and assurance of privacy preservation forces researchers to rely heavily on local expertise and support. - Given the current limitation and potential issues with the legislation, it remains to be seen whether the move toward the GDPR will be beneficial for the Serbian health system, medical research, protection of personal data and privacy rights, and research capacity. - Although significant progress has been made so far, a strategic approach is needed at the national level to address insufficient resources in the area of data protection and develop the personal data protection environment further.

The Netherlands	• In the Netherlands, there is no clear policy on secondary use of health data available in one cohesive place. A Chief Information Officer (CIO) has been appointed in the Ministry of Health. There are several projects focused on data registries including a 'registry of registries'. The Netherlands is one of four countries participating in the public-private partnership H20 IMI, an effort to build a health observatory for IBD/Cancer and diabetic care. • The UAVG is a specific Dutch policy (May 2016) that describes how personal data in general, and health data in particular, should be registered and stored. This law contains specific rules for interchanging digital personal data regarding health issues, such as patient control and consent for data sharing and data protection. Recent studies show broad acceptance of secondary use amongst Dutch citizens. • Covid-19 initiatives have created new data infrastructure for use of Real World Evidence (RWE). There is room in decision-making for RWE, but focus is RWE collected in NL and at the moment it is still seen as phase III studies. Acceptance for the secondary use of health data is growing, especially for very rare diseases, where studies are not possible due to sample size. • Establishing the CIO within the Ministry of Health creates a clear accountability channel and policy advocacy opportunity. Projects with promise, such as DRUP, the Netherlands' participation in IMI initiatives, and work with BeNeLuxA to standardise data registries and related data models, is promising in creating the data infrastructure necessary for secondary
United Kingdom	Welsh Government funds the SAIL (Secure Anonymised Information Linkage – www.saildatabank.com) system for the ethical and legal sharing of data for research purposes whilst protecting privacy through design and the implementation of the five safes. On the social side members of the public (SAIL Consumer Panel) are involved in all decisions on whether a proposed project should be approved (also need to show it is in the public interest and protects the privacy of individuals data). This system works very well, for example we were able to link up to 54 different databases to answer policy relevant questions on responding to the COVID-19 pandemic. • The National Data Strategy was announced in May 2021, and identified the value of secondary use of health data as a top priority, setting out several strategy goals related to expanding the use of health data for research innovation and to respond to challenges such as Covid-19. • A national opt-out register was established in 2018, giving all patients the right to opt-out from usage of their data for research for planning purposes. The Health and Social Care (National Data Guardian) Act 2018 publishes guidance about processing of health and social care data, including genetic data. It includes encouraging data sharing in genomic medicine acknowledging the need to share generic data more widely than is customary for personal medical data. • The Clinical Practice Research Datalink (CPRD) is an initiative to collate data from general practices in England and link it with hospital data, around 50 disease registries and clinical audits, UK Biobank and the loyalty cards of a large supermarket chain. CPRD currently includes data from over 600 general practices and over 10 million patients. • A national opt-out register was established in 2018, giving all patients the right to opt-out from usage of their data for research for planning purposes. The Health and Social Care (National Data Guardian) Act 2018 publishes guidance about processing of health and social care data, including genetic data.

V. Disclaimer

Disclaimer excluding Agency and Commission responsibility

The content of this document represents the views of the author only and is his/her sole responsibility. The European Research Executive Agency (REA) and the European Commission are not responsible for any use that may be made of the information it contains.



National Directorate General for Hospitals (OFKO)

Jasz u., Budapest
1135 Hungary
www.phiri.eu
@PHIRI4EU