Coordination and support actions H2020

Project Number: GA - 101016216

Project Acronym: unCoVer

Project title: Unravelling data for rapid evidence-based response to COVID-19

Deliverable No. 2.1

Legal and ethical guidelines: a scoping exercise

The COVID-19 pandemic has created significant confusion for researchers in terms of whether, and in which way, existing ethical and legal principles remain relevant. The COVID pandemic does not serve to remove the basic validity of the rights and interests on which these documents and principles are based - in particular between a research subject's right to privacy and the public interest in the outcome of research. This deliverable addresses this issue by undertaking a scoping exercise to identify and collate existing recommendations and guidelines on legal and ethical issues in public health emergency taking into account country or region-specific differences in policy or legal instruments. This scoping exercise will collate country-specific health research regulations (if any) and triangulate the resources into a common ethical and legal guidance report for the Consortium and lay down some common obligations in terms of data processing activities using health or health-related data that are found in many laws and ethical guidelines across EU and beyond.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

Document Properties

Deliverable No.	2.1
Deliverable Title	Legal and ethical guidelines: a scoping exercise
Lead beneficiary	UCC (University College Cork)
Due date of deliverable	14th February 2021
Actual submission date	16th February 2021
Dissemination level	PU

Dissemination Level

PU = Public
PP = Restricted to other programme participants (including the Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for member of the consortium (including the Commission Services)

Document History

Version	Date	Issued by	Description
V1	05/02/2021	Z Kabir [UCC]	1st draft
Final	15/02/2021	Z Kabir [UCC]	Final document

Disclaimer

This document has been produced in the context of the unCoVer Project. The unCoVer Project is funded by the European Union's Research and Innovation Programme European under Grant Agreement No 101016216.

All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view.

Additional Disclaimer

This guidance has been prepared by the UCC researchers to help the researchers within each beneficiary of this unCoVer Project comply with GDPR requirements. It is intended to be general guidance for educational and informational purposes only. It is not legal advice.

Any liability, including liability for infringement of any proprietary rights, relating to use of information in this document is disclaimed. No license, express or implied, by estoppels or otherwise, to any intellectual property rights are granted herein. The members of the unCoVer Project do not accept any liability for actions or omissions of unCoVer Project members or third parties and disclaims any obligation to enforce the use of this document. This document is subject to change without notice.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS 5
1. INTRODUCTION 6
1.1 Purpose and scope of the document 6
1.2 Relation with other documents 6
1.3 Deliverable structure 6
2. GDPR: AN OVERVIEW 6
2.1 GDPR in a wider legal framework 7
2.2 Charter of Fundamental Rights of the European Union (CFR) 8
2.3 Treaty of the Functioning of the European Union (TFEU) 8
2.4 The European Convention on Human Rights (ECHR) 8
2.5 Universal Declaration of Human Rights (UDHR) 9
3. DATA PROTECTION: THE BASICS 9
3.1 Data Protection Principles 9
3.2 Compliance 10
3.3 Data protection by Design and by Default 11
3.4 Transparency 11
3.4.1 Providing Transparent Information 11
3.5 Obligations 12
3.6 Accountability Obligation 13
3.7 Lawful Processing 13
3.8 Special Category of Personal Data 14
3.9 Data Protection Impact Assessments (DPIA) 15
3.9.1 Key points 15
3.9.2 What is a Data Protection Impact Assessment? 15
3.9.3 When is a DPIA not required? 15
3.9.4 Is a DPIA mandatory for existing processing operations, existing before the GDPR becomes effective on the 25 May 2018? 16
3.9.5 When in a project lifecycle should a DPIA be conducted? 16
3.9.6 Who should be involved in conducting the DPIA? 17
3.9.7 What steps are involved in carrying out a DPIA? 18
3.10 International Data Transfers 18
3.10.1 To a country within the European Economic Area (EEA) 18
3.10.2 Transferring data outside of the EEA 18
4. SEEKING ETHICAL AND DATA PROTECTION GUIDANCE 20
4.1 Anonymisation 21

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

4.1.1 Recommendations on Anonymity 22
4.1.2 Anonymisation techniques 22
4.1.3 Tools of Anonymisation 23
4.2 Consent 23
4.3 The 5 Safes UK Model 24
4.4 Vulnerable Groups 25
5. SELECTED FAQs 26
6. EUROPEAN DATA PROTECTION BOARD (EDPB) GUIDANCE ON DATA PROCESSING 26
7. CYBER-SECURITY/TECHNOLOGY SECURITY 27
8. NATIONAL DATA PROTECTION AND HEALTH RESEARCH REGULATIONS 27
9. PRACTICAL STEPS FOR THE DATA PROCESSORS ACROSS THE UNCOVER PARTNER COUNTRIES ... 28
9.1 Data workflow details for a Data Processor (in accordance with Article 30 of the GDPR)- a generic guideline 28
10. CONCLUSIONS 29
11. REFERENCES 29
ANNEX 1: Table 1 - MASTER CHECK-LIST OF DATA PROCESSING ACTIVITIES IN THE UNCOVER NETWORK PARTNERS 31
ANNEX 2: A TEMPLATE OF INFORMED CONSENT 35
ANNEX 3: A TEMPLATE OF DPIA 38
ANNEX 4: A TEMPLATE OF DATA WORKFLOW FOR A DATA CONTROLLER 42
ANNEX 5: A TEMPLATE OF DATA WORKFLOW FOR A DATA PROCESSOR 43

LIST OF FIGURES

Figure 1: GDPR in an Irish context 7
Figure 2: GDPR in a broader scope 7
Figure 3. Organisational responsibility and compliance with GDPR. 10
Figure 4: The GDPR workflow 29

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation/Acronym	Meaning
BCRs	Binding Corporate Rules or Binding Corporate Rules for Processors
CFR	Charter of Fundamental Rights of the European Union
DOT	Department of Transportation
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EEA	European Economic Area
EU	European Union
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IRB	Institutional Review Board
NHS	National Health Service
REBs	Research Ethics Boards
REC	Research Ethics Committee
SDC	Statistical Disclosure Control
TFEU	Treaty of the Functioning of the European Union
UN	United Nations
UK	United Kingdom
US	United States
WP	Work Package

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

1. INTRODUCTION

The unCoVer project includes the integration and processing of retrospective health data collected for the medical treatment of patients suffering COVID-19. To respect the sensitive nature of personal data concerning health, ethical and legal aspects must be considered for the design and implementation of the technical, as well as medical processes carried out within the unCoVer project.

1.1 Purpose and scope of the document

The document aims to report about ethical and legal requirements analysed for the unCoVer project, as well as the strategy and guidelines for meeting those requirements. The objective is to design and implement the unCoVer ecosystem with due consideration of its legal and regulatory issues concerning data protection, privacy, and information security.

To this end, legal research was conducted to analyse the ethical, legal, regulatory and technical requirements. The uniform European basis comprises the General Data Protection Regulation 2016/679/EU of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (GDPR) and the European Charter of Fundamental Rights as well as guidance by European Data Protection Board, former Article 29 Working Party.

The work carried in the first phase of the project will also enable the monitoring of support of compliance with these requirements throughout the project's lifetime.

1.2 Relation with other documents

This document will be updated by a second deliverable (D2.2) covering the approach taken to address all activities raising ethical and legal issues or authorising such activities. Moreover, WP7 sets out 'Ethics requirements' that the project must comply with.

1.3 Deliverable structure

This deliverable is structured into 10 main sections - section 11 outlines some key references, and there are relevant annexes. Section 2 provides an overview of the GDPR. Section 3 deals with data protection principles, including Data Protection Impact Assessment (DPIA). Section 4 outlines key data processing activities, such as anonymization, consent, and vulnerable groups. Section 5 summarizes some frequently asked questions related to the GDPR. The role of the European Data Protection Board (EDPB) is briefly discussed in section 6. Section 7 refers to cyber security. Section 8 signposts the national and local data protection rules and regulations in the light of the GDPR (both EU and non-EU partner countries). Concluding remarks are captured in section 9. Section 10 provides key practical steps for the Partner countries of the uncover Consortium.

2. GDPR: AN OVERVIEW

The General Data Protection Regulation (EU) 2016/679 (GDPR) came into force across all of Europe on 25th May 2018. It replaces the EU's previous Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regarding the processing of personal data and on the free movement of such data.

GDPR governs the collection, use and storage of all personal data of living individuals. As GDPR is a regulation instead of a directive, it has binding legal force throughout every member state and is directly applicable to all member states.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

Read the General Data Protection Regulation (EU) 2016/679 full text **here**.

"If you collect, use or store personal data, digital, manual, handwritten or any type of record, then GDPR affects you".

Personal data relates to any information relating to a living individual, whether it relates to his or her private, professional or public life. It can be anything from a name, photo, email address, bank details, posts on social media, medical information, even a computer IP address or a combination of indirectly identifiable data. It should be noted that local interpretations of GDPR can apply and EU member states have flexibility in certain areas and can make their own laws in these areas (Figure 1).

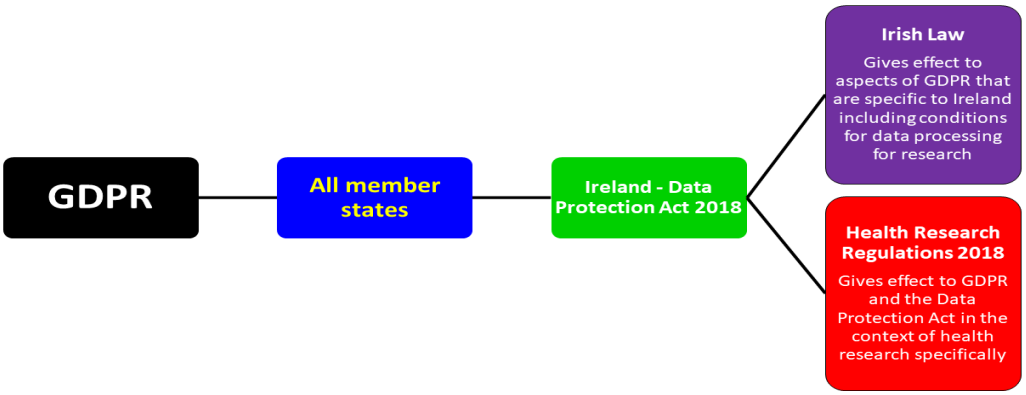

Figure 1: GDPR in an Irish context

2.1 GDPR in a wider legal framework

Figure 2: GDPR in a broader scope

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

2.2 Charter of Fundamental Rights of the European Union (CFR)

Non-discrimination has been identified by the consortium as a fundamental value in the unCoVer project within the context of the processing of research participants' personal data belonging to vulnerable categories of the population. The right to non-discrimination has been defined in the following ways:

Article 21. Non-discrimination

1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.

Articles 7 and 8 of the European Union's Charter of Fundamental Rights provide for express rights to privacy of the individual, their home and communications as well as their personal data.

Article 7 Respect for private and family life

"*Everyone has the right to respect for his or her private and family life, home and communications*".

Article 8 Protection of personal data

"*1. Everyone has the right to the protection of personal data concerning him or her.*

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority".

2.3 Treaty of the Functioning of the European Union (TFEU)

The TFEU is one of two primary treaties of the European Union which forms the basis of European law.

Article 16(1) of the TFEU provides that:

"*Everyone has the right to the protection of personal data concerning them*".

2.4 The European Convention on Human Rights (ECHR)

Article 8 of the ECHR protects your right to respect for your private life, your family life, your home and your correspondence (letters, telephone calls and emails, for example).

What the law says:

Article 8: Right to privacy

''Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

2.5 Universal Declaration of Human Rights (UDHR)

Article 12

"*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*".

Not an absolute right

The right to privacy is not an absolute right.

It is balanced against other fundamental human rights, including (i) the common good in accordance with the law and (ii) the principles of necessity and proportionality.

3. DATA PROTECTION: THE BASICS

This guidance note, on 'Data Protection Basics', aims to address some of the most common questions about data protection law and to clarify the basic principles underlying data protection. This guidance covers the different laws which apply in a data protection context and when they apply, as well as the meaning of 'personal data' and 'processing', and how to identify a 'data controller' and what their obligations are. It aims to explain the requirement for a 'legal basis' to justify the processing of personal data and outline the rights which individual 'data subjects' have and how they can exercise them.

3.1 Data Protection Principles

Article 5 of the GDPR sets out key principles which lie at the heart of the general data protection regime. These key principles are set out right at the beginning of the GDPR and they both directly and indirectly influence the other rules and obligations found throughout the legislation. Therefore, compliance with these fundamental principles of data protection is the first step for controllers in ensuring that they fulfil their obligations under the GDPR. The following is a brief overview of the Principles of Data Protection found in article 5 GDPR:

- **Lawfulness, fairness, and transparency**: Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.
- **Purpose Limitation**: Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. However, further processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes (in accordance with Article 89(1) GDPR) is not considered to be incompatible with the initial purposes.
- **Data Minimisation:** Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum (see also the principle of 'Storage Limitation' below).

- **Accuracy:** Controllers must ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In particular, controllers should accurately record information they collect or receive and the source of that information.
- **Storage Limitation**: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.
- **Integrity and Confidentiality**: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability:** Finally, controllers must take responsibility for their processing of personal data and how they comply with the GDPR and be able to demonstrate (through appropriate records and measures) their compliance.

3.2 Compliance

GDPR Article 5(2) requires that the data controller "*be responsible for, and be able to demonstrate, compliance with the principles*".

All employees, researchers or students in an organisation, who collect and/or control the content and use of personal data are individually responsible for compliance with GDPR.

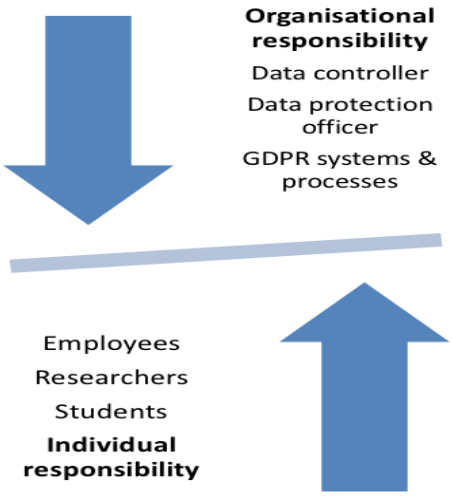

Figure 3. Organisational responsibility and compliance with GDPR

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

3.3 Data protection by Design and by Default

The GDPR provides for two crucial concepts for future project planning: Data Protection By Design and Data Protection By Default. While long recommended as good practice, both principles are enshrined in law under the GDPR (Article 25).

- **Data Protection by design** means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.
- **Data Protection by default** means that the user service settings (e.g. no automatic opt-ins on customer account pages) must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all. It is linked to the principles of data minimization and purpose limitation.

3.4 Transparency

One of the key principles of GDPR laid out in Article 5 and Recitals 39 and 58 is that of transparency.

A data controller must not only adhere to this principle, he or she must be able to demonstrate that personal data are processed in a transparent manner. The transparency requirements in the GDPR are required irrespective of the legal basis for processing and apply throughout the life cycle of processing.

In addition, GDPR Article 12 sets out the transparency requirements which apply to:

- the provision of information to data subjects (under Articles 13 - 14)
- communications with data subjects concerning the exercise of their rights (under Articles 15 - 22); and,
- communications in relation to data breaches (Article 34).

3.4.1 Providing Transparent Information

Businesses and organisations that process personal data must provide individuals with information on the type of processing that is taking place and who is carrying it out. At a minimum, this information must clearly state:

- Who you (the organisation) are.
- Why you are processing the data.
- What legal basis you rely on to legitimise the processing.
- Whether or not the data will be transferred on to other organisations or individuals.
- How long the data will be stored.
- The existence of the individual's rights under data protection, including the rights to access, correction, erasure, restriction, objection and portability.

The following information must also be supplied, if it is the case that your business or organisation comes within the scope of these provisions:

- If you are required to appoint a Data Protection Officer then the contact information of the DPO must be provided.
- If you are relying on legitimate interests as your legal basis for processing, you must explain what the legitimate interest is.
- If you are transferring the data outside of the EU, you must explain why.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

- If you rely on consent as your legal basis for processing, you must explain how consent can be withdrawn.
- If there is a legal obligation to provide the data, that must be explained.
- If you are processing by means of automated decision-making, you must provide information about the logic underpinning the automated process, and any consequences arising out of a decision that has been arrived at through automated means. Be aware that the right to object to automated processing in the guidance for individuals section is one of the rights granted to individuals under the GDPR.

3.5 Obligations

Research projects using human data must be approved by an independent research ethics board (or research ethics committee, or institutional research board) prior to the recruitment of participants and the collection of data, in compliance with local requirements. Accredited research ethics boards have broad powers to approve, reject, require modification of, and terminate research projects.

All research projects using human data should comply with local legal obligations as outlined below:

1. The obligation to respect confidentiality.
2. The obligation to ensure data accuracy.
3. The obligation to limit the identifiability of personal data as far as possible - including via pseudonymisation techniques.
4. The obligation to use anonymised data instead of personal data, or minimise personal data use, or de-identify where possible.
5. The need to process for a specific, authorised, purpose and only to process for secondary purposes provided certain conditions are fulfilled and not processing for purposes beyond scientific research / healthcare; e.g. not sharing with employers or other agencies unless mandated by law.
6. The obligation to inform individuals about the processing of their data in compliance with local/national requirements or health research regulations.
7. To hold oneself accountable to, and remain transparent towards, the individuals concerned by the data used.
8. To provide individuals access to their data, and to rectify errors or biases in the data on request.
9. To allow individuals to object to the processing of their data if required by law.
10. To provide individuals the opportunity to request the deletion or return of their data in certain circumstances if this is possible or required by law.
11. The obligation to ensure that data are collected from representative sub-populations and not confined to one group.
12. The obligation to ensure equal treatment across cohorts to:
    a. Prevent marginalisation of vulnerable groups;
    b. Encourage engagement from vulnerable groups;
    c. Display trustworthiness and warrant trust.
13. The obligation to share data and the benefits of research outcomes fairly and without regard to discipline, region or country.
14. The obligation to apply legal and ethical practice to all stages of data collection, processing, analysis, reporting and sharing.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

15. The obligation for data providers as well as data users to validate and verify the provenance of data and ensure appropriate consent or other legal basis for the data's use.
16. The obligation to ensure that de-identified or aggregated data made public does not contain data elements or rich metadata that could reasonably lead to the identification of specific persons. De-identification sometimes refers to stripping of any direct identifiers in some jurisdictions (USA, for instance), but that is often not sufficient for making publicly available.
17. To validate that data sharing respects the applicable legal requirements, e.g. conclusion of sharing agreements and/or verifying the legality of a data transfer abroad.
18. To consider the legitimacy of the public emergency and use of data on persons collected during a following the emergency.

3.6 Accountability Obligation

Accountability is a common principle for organisations across many disciplines; the principle embodies that organisations live up to expectations for instance in the delivery of their products and their behaviour towards those they interact with. The GDPR integrates accountability as a principle which requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested.

Organisations, in consultation with their respective data protection authorities, must demonstrate that they are compliant with the law. Such measures include:

- Adequate documentation on what personal data is processed;
- How, to what purpose, and how long data will be processed for;
- Documented processes and procedures aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; and
- The presence of a Data Protection Officer (if required) who is integrated in the organisation planning and operations etc.

The Controller's GDPR registry can detail all personal data processing activities: an inventory of all personal data you hold and examine it under the following headings:

- Why are you holding it?
- How did you obtain it?
- Why was it originally gathered?
- How long will you retain it?
- How secure is it, both in terms of encryption and accessibility?
- Do you ever share it with third parties and on what basis might you do so?

This is the first step towards compliance with the GDPR's accountability principle, which requires organisations to demonstrate (and, in most cases, document) the ways in which they comply with data protection principles when transacting business. The inventory will also enable organisations to amend incorrect data or track third-party disclosures in the future, which is something that they may be required to do.

3.7 Lawful Processing

In order to process personal data you must have a lawful basis to do so. The lawful grounds for processing personal data are set out in Article 6 of the GDPR. These are:

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

- The consent of the individual;
- Performance of a contract;
- Compliance with a legal obligation;
- Necessary to protect the vital interests of a person;
- Necessary for the performance of a task carried out in the public interest; or
- In the legitimate interests of company/organisation (except where those interests are overridden by the interests or rights and freedoms of the data subject).

3.8 Special Category of Personal Data

Encompasses personal data that reveals the following:

- race
- ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation.

GDPR Article 9 prohibits any data processing of special category personal data unless the data controller can meet one or more conditions in addition to having an appropriate legal basis for the data processing:

1. Explicit Consent
2. Necessary for legal claims or judicial purposes
3. Necessary for employment, social security and social protection law
4. Vital interests
5. Legitimate activities with a political, philosophical, religious or trade union aim
6. Personal data that is manifestly public
7. Substantial public interest
8. Provision of health care
9. Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Where the processing of special category personal data is necessary for:

- archiving purposes in the public interest
- scientific or historical research purposes or
- statistical purposes.

The processing must be:

- in accordance with GDPR Article 89(1)
- based on EU or Member State law
- proportionate to the aim pursued
- respect the essence of the right to data protection

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

- provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

Public interest in the area of public health, for example:

- Protecting against serious cross-border threats to health, or
- Ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

The data processing must:

- Have a basis in EU or Member State law.
- Must provide for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

3.9 Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments can be used to identify and mitigate against any data protection related risks arising from a new project, which may affect your organisation or the individuals it engages with.

3.9.1 Key points

- Under the GDPR, DPIAs will be mandatory for any new high risk processing projects.
- The DPIA process will allow you to make informed decisions about the acceptability of data protection risks and communicate effectively with the individuals affected.
- Not all risks can be eliminated, but a DPIA can allow you to identify and mitigate against data protection risks, plan for the implementation of any solutions to those risks, and assess the viability of a project at an early stage.
- If a DPIA does not identify mitigating safeguards against residual high risks, the Data Protection Authorities must be consulted.
- Good record keeping during the DPIA process can allow you to demonstrate compliance with the GDPR and minimise risk of a new project creating legal difficulties.

3.9.2 What is a Data Protection Impact Assessment?

When your organisation collects, stores, or uses personal data, the individuals whose data you are processing are exposed to risks. These risks range from personal data being stolen or inadvertently released and used by criminals to impersonate the individual, to worry being caused to individuals that their data will be used by your organisation for unknown purposes. A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

3.9.3 When is a DPIA not required?

A DPIA is generally <u>not required</u> in the following cases:

- Where the processing is not “likely to result in a high risk to the rights and freedoms of natural persons” (article 35(1)).
- When the nature, scope, context and purposes of the processing are very similar to the processing for which DPIAs have been carried out. In such cases, results of a DPIA for similar processing can be used (Article 35(1)).

This project is funded by the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

- Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulates the specific processing operation and where a DPIA, according to the standards of the GDPR, has already been carried out as part of the establishment of that legal basis (Article 35(10)).
- Where the processing is included on the optional list (established by the supervisory authority) of processing operations for which no DPIA is required (Article 35(5)). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorisations, compliance rules, etc. In such cases, and subject to reassessment by the competent supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned in the list and continues to comply fully with the relevant requirements.

3.9.4 Is a DPIA mandatory for existing processing operations, existing before the GDPR becomes effective on the 25 May 2018?

The GDPR is effective from the 25 May 2018, and DPIAs are legally mandatory only for processing operations that are initiated after this date. Nevertheless, the Article 29 Working Party strongly recommends carrying out DPIAs for all high risk operations prior to this date. Indeed a DPIA can be a powerful tool in ensuring that any operations commencing now will not leave you at risk of non-compliance once the law changes on the 25 May 2018, and save your organisation from operational disruption by allowing you to future proof new projects against the GDPR at an early stage.

Additionally, new DPIAs or reviews of DPIAs for existing processing that commenced before the 25 May 2018 may be required after that date in the following circumstances:

- Where a significant change to the processing operation has taken place after the GDPR takes effect. For example, when a new technology comes into use, or when data is being used for a different purpose. In these cases the processing is effectively a new operation and could require a DPIA.
- When there is a change of the risk presented by the processing operation. The risks and level of risk can change as a result of a change to one of the components of the processing operation (data, supporting assets, risk sources, etc.), or because the context of the processing evolves (purpose, functionalities, etc.). Data processing systems can evolve over time, and new threats and vulnerabilities can arise.
- The organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, new categories of natural persons become vulnerable to discrimination or the data is intended to be transferred to data recipients located in a country which has left the EU.

As a matter of good practice, the Article 29 Working Party recommends that all DPIAs should be re-assessed after 3 years, or sooner if circumstances have changed quickly.

3.9.5 When in a project lifecycle should a DPIA be conducted?

The DPIA should be carried out “prior to the processing” (GDPR Articles 35(1) and 35(10), recitals 90 and 93). It is generally good practice to carry out a DPIA as early as practical in the design of the processing operation. It may not be possible to conduct a DPIA at the very inception of the project, as project goals and some understanding of how the project will operate must be identified before it will be possible to assess the data protection risks involved.

This project is funded by the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

For some projects the DPIA may need to be a continuous process, and be updated as the project moves forward. The fact that a DPIA may need to be updated once processing has actually started is not a valid reason for postponing or not carrying out a DPIA.

3.9.6 Who should be involved in conducting the DPIA?

The data controller is responsible for ensuring the DPIA is carried out. It may be delegated to someone else, inside or outside the organisation, but the data controller is ultimately accountable.

The DPIA should be driven by people with appropriate expertise and knowledge of the project in question, normally the project team. If your organisation does not possess sufficient expertise and experience internally, or if a particular project is likely to hold a very high level of risk or affect a very large number of people, you may consider bringing in external specialists to consult on or to carry out the DPIA.

A wide internal consultation process can benefit the DPIA, as some data protection risks will only be apparent to individuals working on specific aspects of the project. It will also allow you to gain feedback from those whose work will be affected by the project after implementation, such as engineers, designers and developers, who will have a practical knowledge of the operations. Involving your organisations public relations team will allow for effective communication of the DPIA's outcomes to external stakeholders.

Under the GDPR (Article 35), it is necessary for any data controller with a designated Data Protection Officer (DPO) to seek the advice of the DPO. This advice and the decisions taken should be documented as a part of the DPIA process. If a data processor is involved in the processing, the data processor should assist with the DPIA and provide any necessary information.

The Data Protection Officer (DPO) is a designated person appointed by an organisation to advise on data protection practices within the organisation. The DPO can be a staff member or an external service provider. Under the GDPR, appointment of a DPO is mandatory in the following circumstances:

- For public bodies carrying out data processing, except for courts acting in their judicial capacity;
- If the core activities of the organisation consist of data processing which, by virtue of their scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or
- The core activities of the organisation consist of processing on a large scale of special categories of data as outlined in Article 9 or personal data relating to criminal convictions as outlined in Article 10 of the GDPR.

The data controller is bound to "seek the views of data subjects or their representatives" (Article 35(9)), "where appropriate" in carrying out the DPIA. In some cases, the data subjects may be people within the organisation. Seeking the views of data subjects will allow the data controller to understand the concerns of those who may be affected, and to improve transparency by making individuals aware of how their information will be used.

The views of data subjects can be sought through a variety of means, depending on the context. Staff could be consulted through a trade union; customers could be consulted by means of a survey. If the data controller's final decision differs from the views of data subjects, the reasons should be recorded

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

as a part of the DPIA. If the data controller does not feel it appropriate to seek the views of data subjects, the justification for this should be documented.

3.9.7 What steps are involved in carrying out a DPIA?

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

- "a description of the envisaged processing operations and the purposes of the processing"
- "an assessment of the necessity and proportionality of the processing"
- "as assessment of the risks to the rights and freedoms of data subjects"
- "the measures envisaged to:
  "address the risks";
  "demonstrate compliance with this Regulation".

The GDPR presents a broad, generic framework for designing and carrying out a DPIA. This allows for scalability, so even the smallest data controllers can design and implement a DPIA; as well as for flexibility, so the data controller can determine the precise structure and form of the DPIA, allowing it to fit with existing working practices.

3.10 International Data Transfers

3.10.1 To a country within the European Economic Area (EEA)

There are no restrictions on the transfer of personal data to EEA countries as the GDPR applies throughout the EEA.

The EEA countries are as follows:

> Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden Iceland, Liechtenstein and Norway

3.10.2 Transferring data outside of the EEA

Transfers based on a European Commission "adequacy decision"

The European Commission has the power to determine, on the basis of GDPR Article 45 whether a country outside the EEA offers an adequate level of data protection.

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection.

Adequacy talks are ongoing with Japan and South Korea.

Note about the US Privacy Shield framework

It should be noted that the US Privacy Shield framework is a self-certification process that may be used by any US organisation that is subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT). These organisations do not usually have jurisdiction over not-for-profit organisations such as universities and similar. If you wish to use the US Privacy Shield framework to facilitate data transfers outside of the EEA, you will need to check with your partner organisation to see if they are certified under this framework.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

If the US organisation is not, or is not eligible to be, certified under the US Privacy Shield framework, then adequate safeguards may be put in place in a number of ways including using Model Contract Clauses, Binding Corporate Rules or Binding Corporate Rules for Processors (BCRs) or other contractual arrangements. Where "adequate safeguards" are established, the rights of data subjects continue to be protected even after their data has been transferred outside the EEA.

Brexit

The United Kingdom withdrew from the European Union on 31 January 2020. On the basis of the Withdrawal Agreement that has been ratified by both the European Union and the United Kingdom, a transitional period during which EU law will continue to apply in the United Kingdom will last until 31 December 2020. With regard to personal data, the situation remains unchanged and no transfer mechanism under Chapter V of the GDPR or of the Law Enforcement Directive is therefore required.

Unless the parties decide before 1 July 2020 to extend the transitional period by 1 to 2 years, as of 1 January 2021 all Union primary and secondary law will cease to apply to the United Kingdom. Transfers of personal data to the United Kingdom will then be subject to the requirements of Chapter V of the GDPR and of the Law Enforcement Directive. A number of notices setting out the consequences in a range of policy areas have been published by the European Commission with the aim of preparing citizens and stakeholders for the withdrawal of the United Kingdom.

More information is available on this here which was adopted on 15th December 2020.

Transfers subject to appropriate safeguards

GDPR provides mechanisms for cross-border data transfers in the absence of an adequacy designation if the controller or processor utilizes certain safeguards. These safeguards must ensure that the individual data subject has enforceable rights and that there are effective legal remedies for the individual available following the data transfer.

The appropriate safeguards are:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Transfers that do not have either an adequacy decision nor adequate safeguards

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);
- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.
  In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

4. SEEKING ETHICAL AND DATA PROTECTION GUIDANCE

In times of pandemic or other public emergencies, it is important to be aware of existing and *ad hoc* resources and guidance. For example:

1. Researchers attached to an academic institution may find guidance from the following (if available at a particular institution):
   1.1. Research Ethics Boards (REBs), such as an Institutional Review Board (IRB) or Research Ethics Committee (REC), will provide guidance; in some cases, they will review, require modification, approve or stop a research project;
   1.2. The Information Governance Board will provide support on data management;
   1.3. The Data Protection Officer will provide support and guidance on data protection issues;
   1.4. Data and Biospecimen Access Committees will advise on sharing or providing access to data, as well as Intellectual Property issues;
   1.5. Technology transfer offices provide guidance regarding intellectual property and related issues;
   1.6. If such bodies are not available at the researcher's home institution the UN Ethics office or national ethics office may be contacted for further support (The United Nations, 2020).
2. For professionals affiliated to a professional body, the latter will provide guidance on ethical research activities.
3. For medical or other clinical staff, the institution (such as a hospital) will provide research integrity support, including ethical approvals required and ad hoc mechanisms to support emergency research efforts; or the appropriate governing body (e.g. the National Health Service [NHS] and the Information Commissioner Office (ICO) in the UK) will provide training and support both ongoing and in exceptional circumstances.
4. Hospitals, much like academic institutions, are often staffed by a Data Protection Officer, personnel specialised in research ethics including REBs, and administrators responsible for authorising the sharing of health data.

Researchers and other professionals should always consult their institutional support personnel as well as professional bodies. Often in cases of health emergencies such as the COVID-19 pandemic, fast track procedures are put in place, allowing the approval processes to be accelerated without diminishing the protection of the rights of persons.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

4.1 Anonymisation

Data will generally be anonymous if they cannot be used to identify a person by all means likely reasonably to be used (Article 29 Working Party on Data Protection, 2007, 2014, 2015). It should be noted, however, that anonymisation is not a binary event and various jurisdictions define the threshold for anonymity differently (for example, the USA). Assessment of all the means reasonably likely to be used must consider not only the data on its own but also the possibility of combination with other accessible data, including by third parties.

The consequence of rendering data anonymous will often be that certain ethical and legal obligations which usually apply to identifiable data will no longer apply. In particular, anonymisation will usually render data protection law inapplicable. With large datasets, and especially where datasets are cross-correlated, absolute anonymity will often be very hard to achieve. Researchers may need to take into account the possibility of future re-identification, and manage this risk by means of a risk assessment.

In the European Union, for example, anonymous data falls outside the scope of data protection legislation (GDPR, 2016). A number of tools are available which claim to anonymise personal data, such as sdcMicro. However, there are a number of considerations when dealing with data which is said to be anonymous or anonymised. If data are not fully anonymised, then they will usually fall within the scope of data protection legislation (GDPR, Recital 26) and so therefore require closer controls and management.

For the purposes of this document:

1. Anonymised data refers to data where direct and indirect personal identifiers have been removed. Anonymised data poses only a minimal risk of individual re-identification, in considering the context of the data's use and the means reasonably likely to be used to perform re-identification.
2. De-identified data refers to data where direct personal identifiers have been removed (e.g. US HIPAA). However, there is still some risk that such data may lead to re-identification especially if combined with other data. Generally, de-identification refers to the process of reducing data identifiability rather than the identifiability of the resulting data.
3. Pseudonymised data refers to data where personal identifiers have been changed or removed (i.e., personal names and locations obscured). There is a separate key, index, or technological process which links the pseudonymous id code to an individual. The pseudonymisation of data will not reduce the data protection obligations in the data but can be a requirement to the lawful use of data in some jurisdictions and ethical regimes, where practicable (e.g. GDPR).
4. Data that cannot be Re-personalised: Some jurisdictions, such as the EU, recognise a median status for data that remains identifiable by law, but that the controller is not able to reidentify (GDPR Art. 11). For instance, pseudonymised data that the controller does not hold the 'reidentification key' to. Controllers still need to safeguard such data but have more relaxed obligations regarding the rights of the concerned individuals.
5. Qualitative data are difficult to anonymise because there may be indicators such as the combination of a location and an employment type which could make it easier to identify an individual or small cohort of individuals.
6. Data analytics describes a collection of data processing methods which use large amounts of data (big data) to derive models and predictions about future behaviours or activity. Data analytics introduce some risk of re-identification:

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

   a. Cross-referencing or Cross-correlation: when data are aggregated or correlated with other data, then the likelihood of being able to identify an individual, especially an outlier, increases;
   b. Comorbidities: for clinical data, where multiple conditions may present for an individual, this also increases the likelihood of being able to identify that individual.
7. Statistical Disclosure Control refers to methods used to reduce the risk of re-identification. They are encouraged when sharing or publishing data, and when publishing research outcomes.

4.1.1 Recommendations on Anonymity

Check with your institution, data protection officer or authority, and institutional review board to determine local definitions of the terms (e.g. anonymous, pseudonymised, de-identified etc.).

1. Check what the local (national) expectations are: a data subject will usually expect their data to be processed in compliance with local instruments.
2. Check with the controller or data user what they claim the status of the data to be (anonymous, de-identified, pseudonymised, etc.). Nonetheless, as data identifiability can shift from jurisdiction to jurisdiction, and relative to the factual circumstances of its use, it is prudent not to rely on any representations made by third parties regarding the identifiability of their data.
3. Carry out a re-identification risk assessment before
   a. Combining one or more datasets
   b. Sharing or publishing data or publishing research findings quoting examples of the data.

In carrying out a re-identification risk assessment regarding the impact on the data subject (the individual identified) before disclosure or publication and introduce additional measures (Statistical Disclosure Control) to mitigate the risk. The statistical disclosure control methods used, and the re-identification risk assessment, should account for privacy risks to groups and communities. The potential for sensitive attributes to be revealed absent individual re- identification should also be accounted for. We should also make a distinction between anonymisation requirements for primary entry of data in the unCoVer database and anonymisation when data is going to be used (internally or externally).

4.1.2 Anonymisation techniques

Deciding on an appropriate anonymisation technique has to be done on a case by case basis, having regard to all of the relevant risk factors, and to the intended purpose of the anonymised data. Organisations have to balance the need to retain all information necessary for the purpose for which the anonymised data is to be used with the identification risks presented by the inclusion of more detailed information in a dataset. Where personal data cannot be effectively anonymised they must still be regarded and treated as 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 document does not provide a comprehensive overview of all available anonymisation techniques, and cannot give detailed guidance on individual cases. Organisations should consult the Article 29 Working Party's opinion on Anonymisation Techniques (Opinion 05/2014), and in particular

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

the technical annex thereto for more detailed information about the anonymisation techniques which may be relevant.

Organisations should also be aware of their obligations regarding data protection by design and by default (per Article 25 GDPR) as well as regarding the security of processing of personal data (per Article 32 GDPR).

There are, broadly speaking, two different families of anonymisation technique: "**randomisation**" and "**generalisation**". Other techniques, such as "**masking**" or "**pseudonymisation**", which are aimed solely at removing certain identifiers, may also play a role in reducing the risk of identification. In many cases, these techniques work best when used together, so as to combat different types of identification risk. The following resources and guidance are available for additional details on these techniques.

a) https://www.dataprotection.ie/sites/default/files/uploads/2020-09/190614%20Anonymisation%20and%20Pseudonymisation.pdf
b) https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

4.1.3 Tools of Anonymisation

a) sdcMicro: Statistical Disclosure Control Methods for Anonymization of Data and Risk Estimation
b) Amnesia

4.2 Consent

Consent is the act by which a participant, patient or data subject indicates that they permit something to happen to them, or to their data, which would otherwise not be able to happen.

It covers a number of different specific contexts:

1. **Clinical**: a patient agrees to undergoing a procedure, including taking part in a trial;
2. **Data Protection**: a data subject agrees to personal data being processed for specified purposes;
3. **Research**: a participant agrees to take part in a research study or experiment.

In both cases, the informed consent sheets for clinical or research purposes would explicitly set out how data protection will be handled, as well as samples or biobanking, rights to self- images and others.

Giving consent should be informed (e.g. the individual knows what is going to happen and why), freely given (there is no coercion or similar motivation), given by somebody with capacity, unambiguous and auditable (the consent is recorded somewhere). Depending on the jurisdiction and the research domain, there may be an additional requirement to seek consent. This may include a representative community board as well as participants themselves.

Ideally, consent should be sought for collecting, processing, sharing and publishing data. However, there are other legal bases for processing personal data. Some specific examples from the European General Data Protection Regulation (GDPR, 2016) are described below. Our recommendation would therefore be as follows:

1. Where possible, use data where the data subject has provided a valid consent that includes or is compatible with intended use of the data and complies with the requirements on consent in the specific country or region.
2. Where these are not possible, there are other reasons why data may be used. For example,

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

there may be a different legal basis for using personal data.

3. If using personal data, check whether there may be another basis for using the data. In Europe, for instance, the GDPR provides other legal bases for processing personal data:
    a. Vital Interests (Art. 6(1)(d), and Art. 9(2)(c)): it may not be practical, feasible or possible to contact the data subject. However, to protect the vital interests of other natural persons the data needs to be interrogated and used.
    b. In addition, there are other provisions for both personal data:
        i. Public Task (Art. 6(1)(e)). and special category data:
        ii. Public Interest (Art. 9(2)(g));
        iii. Preventive Medicine (Art. 9(2)(h));
        iv. Public Health (Art. 9(2)(i));
        v. Public Interest, Scientific or Historical Research Purposes or Statistical Purposes (Art. 9(2)(j)).

There is adequate provision, therefore, in the current regulation and its derivatives. In other jurisdictions, there may be other provisions which could be used. Their potential applicability in a specific case should be carefully examined.

4.3 The 5 Safes UK Model

The 5 Safes Model was developed by staff working at the Office for National Statistics (UK) to be an easy to implement sensitive data management framework (Ritchie, 2008). It has subsequently been adopted by numerous Research Data Centres around the World, along with Statistical Disclosure Control (see below under **Safe Outputs**). Research Data Centres using the 5 Safes model will typically provide different methods of access to data, including remote-only or controlled, on-site connection.

The ambition of the 5 Safes Model is to achieve the 'Safe Use' of research data by accounting for five potential areas of risk to data subject confidentiality.

Safe People - Who is going to be accessing the data?

1. Safe People (authorized) should have the right motivations for accessing research data.
2. Safe People should also have sufficient experience to work with the data safely.
3. Researchers may need to undergo specific training before using sensitive or confidential research data to become Safe People.

Safe Projects - What is the purpose of accessing the data?

1. Safe Projects are those that have a valid research purpose with a defined 'public benefit'.
2. It must not be possible to realise this benefit without access to the data.

Safe Settings - Where will the data be accessed?

1. Access controls should be proportionate to the level of risk contained with the data.
2. Sensitive or confidential data should only be accessed via a suitable Safe Setting.
3. Safe Settings should have safeguards in place to minimise the risk that unauthorised people could access the data.

Safe Data - What does the data contain?

1. Safe Data will present minimal risk possible to the confidentiality of the data subjects.
2. The minimisation of risk could be achieved by removing direct identifiers, aggregating values, banding variables, or other statistical techniques that make re-identification more

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

difficult. However, the loss of detail may limit the usefulness of the dataset.

3. Sensitive or confidential data should not be considered to be safe because of the residual risk to data subject confidentiality. However, it is often the most useful for research but encryption can be a layer of safeguard.

Safe Outputs – What will be produced from the data?

1. Research that is generated from data may form derived outputs; these could include statistics, graphs/charts, or reports.
2. Outputs generated from the use of sensitive or confidential data should only be released if they report statistical findings and cannot be used to reveal the identity of a data subject nor enable the association of confidential information to a data subject.
3. Statistical Disclosure Control (SDC) is often used to minimise the risk of releasing confidential information.
4. Researchers and/or the institution managing the use of the data should check outputs (apply SDC) before publication to ensure they do not present undue risk. The intended outputs should have formed part of any application for ethical approval.

4.4 Vulnerable Groups

The overall motivation in producing these guidelines and recommendations has emphasised the open and timely sharing of research data. There is an important consideration, however, when dealing with groups and not just individual participants. Vulnerable groups may include ethnic minorities like Roma or Sinti, or others such as children, migrants or refugees or those with mental or physical disabilities. They often are disproportionately affected by unequal access to health and preventative services. As well as the Indigenous populations should be given additional consideration.

First of all, these vulnerable groups should be considered for inclusion in research, clinical trials, testing and epidemiology surveys with the same opportunities as others; individuals in such groups also have the same rights as others to information, access to results where pertinent, and protection of privacy. Specific measures to be inclusive of such groups should be put in place.

This is also true in terms of licensing as well as the collecting, processing and sharing of data. Although a general recommendation would be to use a permissive licence (such as CC 0), it is important to remember that licences are not aimed at protecting the rights and expectations of individuals or groups represented in the data. For instance, advanced data analytic techniques may identify previously de-identified individuals themselves, or groupings among individual parties in the dataset which they were unaware of. This could lead to stigmatisation and marginalisation. Therefore, when choosing a licence or when reviewing the ethical implications of sharing data, it is important to consider vulnerable groups and ensure their interests are respected. This of necessity includes data which are not typically thought of as personal data. For example, identifying rare vegetation or animals associated with an Indigenous group may help pinpoint their location and therefore expose them to risk.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

5. SELECTED FAQs

When does the General Data Protection Regulation (GDPR) apply?

The GDPR applies if:

- your company processes personal data and is based in the EU, regardless of where the actual data processing takes place
- your company is established outside the EU but processes personal data in relation to the offering of goods or services to individuals in the EU, or monitors the behaviour of individuals within the EU

Non-EU based businesses processing EU citizen's data have to appoint a **representative in the EU**.

When does the General Data Protection Regulation (GDPR) not apply?

The GDPR does not apply if:

- the data subject is dead
- the data subject is a legal person
- the processing is done by a person acting for purposes which are outside his trade, business, or profession

What is personal data?

Personal data is any information about an identified or identifiable person, also known as the **data subject**. Personal data includes information such as their:

- name
- address
- ID card/passport number
- income
- cultural profile
- Internet Protocol (IP) address
- data held by a hospital or doctor (which uniquely identifies a person for health purposes).

Who processes the personal data?

During processing, personal data can pass through various different companies or organisations. Within this cycle there are two main profiles that deal with processing personal data:

- **The data controller** - decides the purpose and way in which personal data is processed.
- **The data processor** - holds and processes data on behalf of a data controller.

Who monitors how personal data is processed within a company?

The Data Protection Officer (DPO), who may have been designated by the company, is responsible for monitoring how personal data is processed and to inform and advise employees who process personal data about their obligations. The DPO also cooperates with the Data Protection Authority (DPA), serving as a contact point towards the DPA and individuals.

6. EUROPEAN DATA PROTECTION BOARD (EDPB) GUIDANCE ON DATA PROCESSING

The EDPB is an independent European body responsible for ensuring the consistent application of data protection rules throughout the EU. The EDPB has been established by the GDPR. The tasks of this

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

body consists of providing general guidance on key concepts of the GDPR and the Law Enforcement Directive, advising the EC on issues related to the protection of personal data and new proposed legislation in the EU, and adopting binding decisions in disputes between national supervisory authorities.

On 21 April 2020, the EDPB adopted guidelines on the processing of health data for research purposes and on geolocation and other tracing tools in the context of the COVID-19 outbreak. The guidelines on the processing of health data aim to shed light on the most urgent legal questions concerning the use of health data, such as the legal basis of processing, further processing of health data for the purpose of scientific research, the implementation of adequate safeguards and the exercise of data subject rights.

Full story: EDPB adopts further COVID-19 guidance

7. CYBER-SECURITY/TECHNOLOGY SECURITY

a) Evaluating risks

Examples of some of the questions raised in a cybersecurity risk assessment:

- What type of IT services (email, websites, backups, hardware etc.) does our partner use (with a particular eye to organizations covering data recognition ? How damaging would lost control/inaccessibility data be for each one?
- How much effort is an attacker likely to put into getting the data?
- What level of ownership do organisations have? Do they own the hardware? The content?

b) Determining Appropriate Controls

The Cyber-security/Technology security would include an assessment of any controls that are currently in place such as not only anonymization or recognition but also common technological procedures such as encryption, firewalls, identity and access controls and other technical measures by an organization, including their fitness for purpose.

8. NATIONAL DATA PROTECTION AND HEALTH RESEARCH REGULATIONS

The unCoVer has 29 partners across 19 countries within the EU and outside of EU. In addition to GDPR, and other related regulations outside of EU in compliance with GDPR- each data processor within each Partner county needs to ascertain local/national legal and ethical requirements. These local/national data protection rules and regulations are outlined below.

1. Belgium | DataGuidance
2. Italy | DataGuidance
3. Spain | DataGuidance
4. Romania | DataGuidance
5. Luxembourg | DataGuidance
6. Slovakia | DataGuidance
7. Portugal | DataGuidance
8. Norway | DataGuidance
9. Croatia | DataGuidance
10. Ireland | DataGuidance
11. Turkey | DataGuidance

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

12. UK | DataGuidance
13. Brazil | DataGuidance
14. South Korea | DataGuidance
15. USA Federal | DataGuidance
16. Lebanon | DataGuidance

9. PRACTICAL STEPS FOR THE DATA PROCESSORS ACROSS THE UNCOVER PARTNER COUNTRIES

Some practical steps and activities are necessary to adhere to legal, ethical and data protection guidelines and to seek information for each Data Processor within each Partner countries. These are outlined in Table 1 (Annex 1) of this document, which provides a detailed check-list for each partner country to comply with in advance of data processing activities within the unCoVer project.

Step 1: To read and familiarize with this document.

Step 2: To be informed of local/national data protection regulations (as outlined in Section 8 of this document).

Step 3: To review Table 1 for the level of data necessary in advance of data processing.

Step 4: Identify your local Data Protection Officer (if not done yet).

Step 5: Populate Table 1 and provide all additional information in support of each of the indicators. For instance, if explicit consent was sought- a copy of this should be provided to the Consortium by each data processor.

Step 6: The WP2 team and the independent DP-EAB (Data Protection and Ethics Advisory Board) will review this master check-list for additional information and/or the risks involved in data processing on a case-by-case basis. The team may come up with a Risk Evidence Score and will act accordingly. For instance, informed consent was not sought and no data anonymization was possible- then these set of data are considered to be high risk. However, the risk can be mitigated if a DPIA and an Ethical approval were available. An informed decision has to be made in collaboration with other members of the Consortium if a prospective data set can be processed within a data provider of a specific partner country. Such a decision is primarily drawn on local/national data protection regulations (Step 2).

Step 7: Once all safeguards are in place and the DP-EAB are satisfied with the compliance - a green signal to proceed with data processing for a specific partner country will be given.

Step 8: A copy of data workflow has to be submitted to DP-EAB before the data processing activity commences (a template is provided in Annex 5).

9.1 Data workflow details for a Data Processor (in accordance with Article 30 of the GDPR)- a generic guideline

If you are a processor for the ***personal data*** you process, you need to document the following:

- Your organisation's name and contact details.
- If applicable, the name and contact details of your data protection officer – a person designated to assist with GDPR compliance under Article 37.
- The name and contact details of each controller on whose behalf you are acting – the organisation that decides why and how the personal data is processed.
- If applicable, the name and contact details of your representative – another organisation that represents you if you offer services to people in the EU.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

- If applicable, the name and contact details of each controller's representative – another organisation that represents the controller if they monitor or offer services to people in the EU.
- The categories of processing you carry out on behalf of each controller – the types of things you do with the personal data, e.g. marketing, payroll processing, IT services.
- If applicable, the name of any third countries or international organisations that you transfer personal data to – any country or organisation outside the EU.
- If applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations. An exceptional transfer is a non-repetitive transfer of a small number of people's personal data, which is based on a compelling business need.
- If possible, a general description of your technical and organisational security measures – your safeguards for protecting personal data, e.g. encryption, access controls, training.

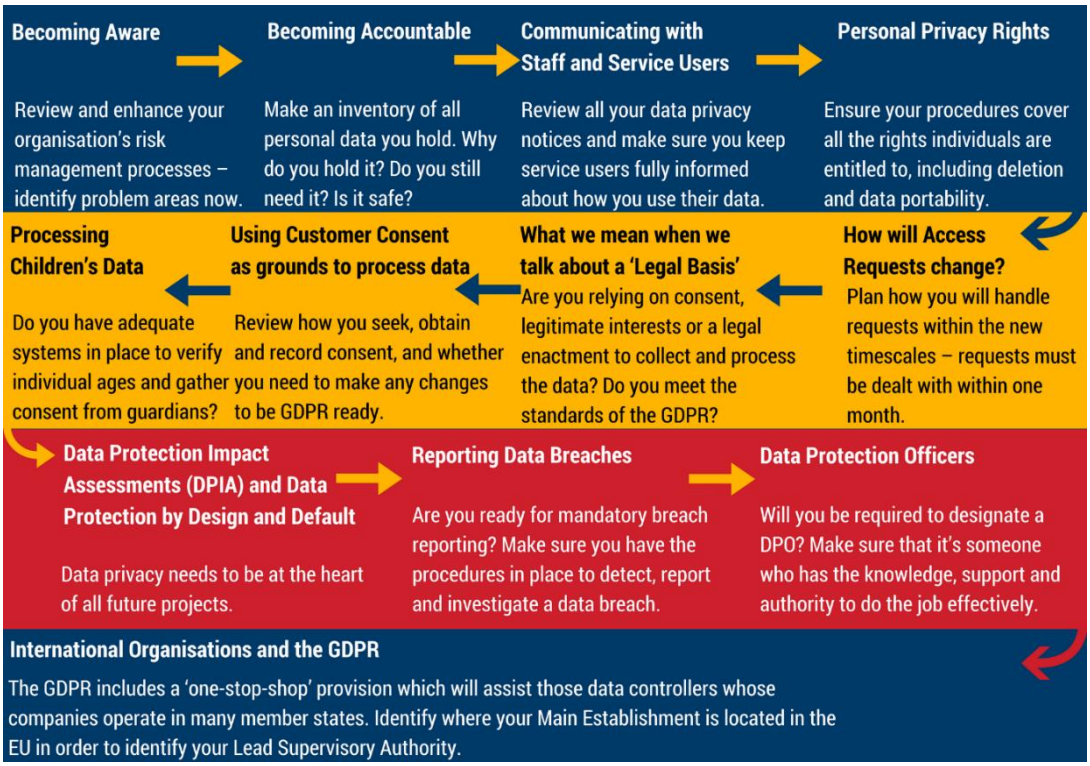

Figure 4: The GDPR workflow

10. CONCLUSIONS

This document summarises the guidelines addressing the legal and ethical aspects of unCoVer.

At this stage of the project, the platform design and development is still subject to discussion. The main goal of this document is to influence any decisions taken early during the project lifetime to ensure a high level of compatibility with legal obligations and ethical values.

Additional challenges are expected to be derived from the need for a high level of usability of data with an optimal level of protection for the data subjects and their privacy.

11. REFERENCES

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

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04 (GDPR)

Article 29 Working Party on Data Protection Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 revised 2018 WP251rev.01

Article 29 Working Party on Data Protection Working Document on the processing of personal data relating to health in electronic health records (EHR) 2007 WP131

European Data Protection Supervisor Opinion 7/2015 on Meeting the challenges of big data - A call for transparency, user control, data protection by design and accountability

Article 29 Working Party on Data Protection Opinion 1/2010 on the concepts of "controller" and "processor" WP169

ISO/IEC 27701:2019 "Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines"

Pocs, M., "Will the European Commission be able to standardise legal technology design without a legal method?" Computer Law & Security Review 28/2012, pages 641-650

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

ANNEX 1: Table 1 - MASTER CHECK-LIST OF DATA PROCESSING ACTIVITIES IN THE UNCOVER NETWORK PARTNERS

No	Acronym	Clinical Data (Y/N)	Hospital Records (Y/N)	Publicly available data (Y/N)	Personal Data (Y/N)	Special Personal Data (Y/N)	Vulnerable Groups (Y/N)	Explicit Consent (Y/N)	Assent (Y/N)	Follow-up data (Y/N)	DPO Identified (Y/N)	DPIA (Y/N)	Ethical Approval (Y/N)	Ethical Approval Pending (Y/N)	Anonymisation (Y/N)	Pseudonymisation (Y/N)	Data Minimisation (Y/N)	Data Transfer Agreement (Y/N)	Data Controller (Name)	Data Processor (Name)	Joint Data Controller (Y/N)	International Transfer outside EU (Y/N)
1	UZA																					
2	FIHM																					
3	UPM																					
4	UNAV																					
5	UPORTO																					

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

6	TU Dublin																				
7	UCC																				
8	UMF Cluj																				
9	UMF IASI																				
10	LIH																				
11	UCP																				
12	TU																				
13	IPC																				
14	SERMAS																				
15	IIS-FJD																				

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

16	UTH																				
17	USN																				
18	IRCCS SCDCH																				
19	Sciensano																				
20	CIPH																				
21	INANTRO																				
22	BU																				
23	SMUC																				
24	ULSS																				

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

	6																				
25	KU																				
26	USF																				
27	UDEA																				
28	ASPEUR																				
29	UNSA																				

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

ANNEX 2: A TEMPLATE OF INFORMED CONSENT

PARTICIPANT CONSENT FORM

This template is designed primarily for those doing qualitative interviews with adults from non-vulnerable populations and dealing with non–sensitive topics.

The form would be different in the case of focus groups or quantitative research. If conducting research with vulnerable populations and / or sensitive topics please see Research Ethics Committee website for further details.

The points listed on the template below are for illustration only. You may alter the wording to suit your project as you see fit.

A consent form is not simply about a person giving you permission to involve them in research, it is an agreement between the researcher and the research participant outlining the roles and responsibilities they are taking towards one another throughout the whole of the research process.

The researcher should retain one copy of the consent form signed by both themselves and the participant. The participant should also be given a copy of the consent form as a record of what they have signed up to.

Even if a person has signed a consent form consent should still be re-established at the point of doing the interview.

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

TEMPLATE

[Title of project]

CONSENT TO TAKE PART IN RESEARCH

- I……voluntarily agree to participate in this research study.
- I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind.
- I understand that I can withdraw permission to use data from my interview within two weeks after the interview, in which case the material will be deleted.
- I have had the purpose and nature of the study explained to me in writing and I have had the opportunity to ask questions about the study.
- I understand that participation involves…[outline briefly in simple terms what participation in your research will involve].
- I understand that I will not benefit directly from participating in this research.
- I agree to my interview being audio-recorded.
- I understand that all information I provide for this study will be treated confidentially.
- I understand that in any report on the results of this research my identity will remain anonymous. This will be done by changing my name and disguising any details of my interview which may reveal my identity or the identity of people I speak about.
- I understand that disguised extracts from my interview may be quoted in…[list all forum in which you plan to use the data from the interview: dissertation, conference presentation, published papers etc.
- I understand that if I inform the researcher that myself or someone else is at risk of harm they may have to report this to the relevant authorities - they will discuss this with me first but may be required to report with or without my permission.
- I understand that signed consent forms and original audio recordings will be retained in [specify location, security arrangements and who has access to data] until [specific relevant period – for students this will be until the exam board confirms the results of their dissertation].
- I understand that a transcript of my interview in which all identifying information has been removed will be retained for [specific relevant period – for students this will be two years from the date of the exam board].

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

- I understand that under freedom of information legalisation I am entitled to access the information I have provided at any time while it is in storage as specified above.
- I understand that I am free to contact any of the people involved in the research to seek further clarification and information.

Names, degrees, affiliations and contact details of researchers (and academic supervisors when relevant).

Signature of research participant

Signature of participant Date

Signature of researcher

I believe the participant is giving informed consent to participate in this study.

Signature of researcher Date

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

ANNEX 3: A TEMPLATE OF DPIA

Step 1a: DPIA Screening Checklist

Does your project involve:	Yes	No
Evaluation or scoring of personal data (including profiling and predicting)		
Automated decision-making with legal or similar significant effects		
Systematic monitoring including through a publicly accessible place on a large scale		
Sensitive data or data of a highly personal nature (including special categories of data and criminal data)		
Data processed on a large scale		
Matching or combining data sets		
Data concerning vulnerable people (including children)		
Innovative use or applying technological or organisational solutions		
Processing preventing data subjects from exercising a right or using a service or contract		

If you have answered yes to any of the above questions, you must carry out a DPIA. Please see the DPIA Procedure for further information.

Step 1b: Identify the Need for a DPIA

Explain broadly what the project aims to achieve and what type of processing of personal data it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA (this can draw on your answers to step 1/ the screening questions).

Step 2: Describe the Processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Step 3: Assessment of Necessity and Proportionality of Processing

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? Prior consultation?

Step 4: Consult with Stakeholders

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

Steps 5 & 6: Risk Assessment - Identifying Privacy Risks and Evaluating Privacy Solutions										
		Name of College/School/Service/Project:_XXXX								**Risk Register Owner: XXXX**
Risk ID		**Risk Description**	**Consequence**	**Risk Owner**		**Current internal <u>CONTROLS</u> (provide details of how you currently manage the risk)**	**Assessment of Risk**			**Describe what further <u>ACTIONS</u> you will take to <u>reduce the Impact/Likelihood</u> and <u>mitigate</u> the risk. State who is the risk owner for each action**
							Impact (1,2,3,4,5)	**Likelihood** (1,2,3,4,5)	**Score**	

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

Step 7: Document DPIA Outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Residual risks approved by:		If accepting any residual high risk, consult the Data Commissioner before going ahead
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

ANNEX 4: A TEMPLATE OF DATA WORKFLOW FOR A DATA CONTROLLER

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.

ANNEX 5: A TEMPLATE OF DATA WORKFLOW FOR A DATA PROCESSOR

This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101016216.