



PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Code of Conduct on Data Protection for Responsible Research and Innovation



This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. It reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Project Information

Project title	Participatory Approaches to a New Ethical and Legal Framework for ICT
Project acronym	PANELFIT
Grant agreement number	788039
Project coordinator	UPV/EHU

Document Information

Deliverable number	D5.4
Document title	Code of Conduct on Data Protection for Responsible Research and Innovation
Document version	Version 4.0
Document date	2021-08-04
Document lead	ICM-CSIC <soacha@icm.csic.es>
Copyright licence	 (Creative Commons Attribution 4.0 International)
Dissemination level	PU (Public)

Project Partners Involved in the Document

N°	Participant organization name	Acronym
1	Institut de Ciències del Mar (Consejo Superior de Investigaciones Científicas)	ICM-CSIC
2	Universidad del País Vasco/Euskal Herriko Unibertsitatea	UPV/EHU
3	European Network of Research Ethics Committees	EUREC
4	Unabhängiges Landeszentrum für Datenschutz AöR	ULD
5	Oesterreichische Akademie der Wissenschaften	OEAW
6	Fonden Teknologiradet	DBT

Document History

Status	Version	Date	Author(s)	Reviewed by
Draft	v0.5	2020-10-30	Pranesh Prakash (ICM-CSIC)	Karen Soacha (ICM-CSIC), Jaume Piera (ICM-CSIC)
Draft	v1.0	2020-11-03	Pranesh Prakash	Julia Maria Mönig (EUREC), Johann Cas (OEAW), Bud Bruegger (ULD), Harald Zwingelberg (ULD), Bjørn Bested (DBT)
Draft	v2.0	2020-12-06	Pranesh Prakash	Iñigo de Miguel Beriain (UPV/EHU), Karen Soacha
Draft	v3.0	2021-01-23	Pranesh Prakash	Karen Soacha
Final	v4.0	2021-08-02	Pranesh Prakash	Karen Soacha, MLEs (Stakeholders, Researchers), Iñigo de Miguel Beriain

Disclaimer: The contents of this publication are the sole responsibility of the PANELFIT consortium and do not necessarily reflect the opinion of the European Union.

Table of content

1	Preamble.....	3
1.1.	RRI and data protection.....	3
2	Data protection principles.....	5
2.1.	Lawfulness, fairness, and transparency.....	5
2.2.	Purpose limitation.....	8
2.3.	Data minimization.....	9
2.4.	Accuracy.....	9
2.5.	Storage limitation.....	10
2.6.	Integrity and confidentiality.....	10
2.7.	Accountability.....	11
3	Good practices relating to data protection principles.....	11
3.1.	Anonymization, pseudonymization and encryption.....	11
3.2.	Aggregate and coarse data.....	11
3.3.	Transparency.....	11
3.4.	Multiple grounds for processing.....	12
3.5.	Consent in data protection and in ethics.....	12
3.6.	Legitimacy, fairness, and ethics approvals.....	12
3.7.	Data protection authorities and ethics boards.....	12
3.8.	Data protection guidelines and DPOs.....	13
3.9.	Data protection impact assessment.....	13
4	Annexures.....	14
4.1.	Annexure 1: Key resources.....	14
4.2.	Annexure 2: Bibliography.....	15
4.3.	Annexure 3: Process for Creating the Code of Conduct on Data Protection for Responsible Research and Innovation.....	15

1 Preamble

This Code of Conduct on Data Protection for Responsible Research and Innovation (CCDP) is a contribution from the PANELFIT project to the research community.

PANELFIT (Participatory Approaches to a New Ethical and Legal Framework for ICT) is an Horizon 2020-funded project that produced operational standards and practical guidelines to address some of the ethical and legal issues posed by ICT technologies. The PANELFIT project thus seeks to provide clarity and guidance with respect to the issues at the intersection between responsible research and innovation,¹ ethics, and data protection.

The CCDP aims to provide an easy-to-understand set of conduct rules that cover the main principles provided in the EU's General Data Protection Regulations (GDPR), as well as a set of desirable practices, specifically tailored to the research community.² There are multiple codes of conduct relating to responsible research and innovation. However, these existing codes of conduct do not seek to provide guidance on data protection principles, which is a gap this CCDP seeks to fill. The CCDP seeks to be an introductory text to data protection principles, and does not seek to cover all aspects of the GDPR that may be of concern to researchers. Thus, for instance, the CCDP does not seek to cover all of the obligations that a researcher may have under data protection laws, nor all the rights of individuals whose personal data are used by researchers, or the legal requirements around sharing of personal data with research colleagues outside the EU, national-level laws on data protection, and so on. The PANELFIT project has also created 'Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation', which aims to be much more comprehensive in this regard.

1.1. RRI and data protection

Research activity, whether it is engaging in research or dissemination of research, often involves other people's personal data.³ Thus, data ethics is a necessary component of responsible research and innovation, and that includes the protection of personal data. In the EU, the protection of personal data is a fundamental right under the Charter of Fundamental Rights of the European Union, and the General Data Protection Regulation provides concrete regulatory guidance on that right.

Whenever researchers process personal data, they are required to abide by data protection law and should endeavour to follow data protection best practices.

The CCDP seeks to help researchers understand the basic principles that underlie the data protection

¹ Responsible Research and Innovation (RRI) is a important component of the "Science with and for Society" programme of EU's Horizon 2020 (H2020). "RRI is the on-going process of aligning research and innovation to the values, needs and expectations of society" ('Rome Declaration on Responsible Research and Innovation in Europe'). The European Commission notes that "RRI is an inclusive approach to research and innovation (R&I), to ensure that societal actors work together during the whole research and innovation process... In general terms, RRI implies anticipating and assessing potential implications and societal expectations with regard to research and innovation." (European Commission, 'Science with and for Society')

² While there is no single, universally accepted definition of research, it is useful to keep in mind the words of the European Data Protection Supervisor in a recent report: "Reputable definitions of research tend to emphasis systematic activity, including the gathering and analysis of data, which increases the stock of understanding and knowledge and their application. The European Commission has defined the objectives of the EU's research and policies to be 'opening up the innovation process to people with experience in fields other than academia and science', 'spreading knowledge as soon as it is available using digital and collaborative technology' and 'promoting international cooperation in the research community'" (European Data Protection Supervisor, 'A Preliminary Opinion on Data Protection and Scientific Research', 9–10)

³ Personal data is any information relating to an identified or identifiable natural person. The term is a very broad category, and includes a person's name, identification number, location data, an online identifier, or factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity.

law in Europe and to equip them with the knowledge on how to practically apply those principles as part of responsible research and innovation. The understanding of research under the GDPR is expansive, covering activities to provide knowledge that can ‘improve the quality of life for a number of people and improve the efficiency of social services’, and includes “technological development, fundamental and applied research and privately funded research and studies conducted in the public interest in the area of public health”⁴

⁴ General Data Protection Regulation, EU Regulation 2016/679, Recital 159.

2 Data protection principles

The protection of personal data under the GDPR is built around a number of principles:

- Lawfulness, fairness, transparency¹
- Purpose limitation²
- Data minimization³
- Accuracy⁴
- Storage limitation⁵
- Integrity and confidentiality⁶
- Accountability⁷

2.1. Lawfulness, fairness, and transparency

In order to comply with the requirements of the principle of lawfulness, transparency, and fairness, researchers need to:

- Determine the purposes for collecting and using personal data.
- Ensure that they identify a valid ground (at least one of the six grounds (“legal bases”) provided in the GDPR) for collecting and using the data.
- Ensure that everything they do with the data is legitimate and in compliance with all applicable laws and ethical guidelines, including those relating to clinical trials, intellectual property, human rights, contract, etc.
- Determine the expectations of individuals as to how the researchers might use their data and what they would consider reasonable.
- Determine the potential harms to the individuals whose data are used.
- Collect and use the data in a manner that is open and transparent.
- Inform individuals in clear language as to who is collecting or obtaining the data, under which legal ground it is being collected/obtained, why it is being collected/obtained, for how long it will be kept, how it will be used and by whom, and what rights they have.
- Use the data in a manner that is fair, in line with the expectations of individuals, and in a manner that does not result in any unjustified or unfair harm to them.
- Check if the data that need to be collected relate to “special categories of personal data” (sensitive data, defined in the GDPR), in which case one of the specific legitimate bases listed in Art. 9(2) of the GDPR must be satisfied. such as having the data subject’s explicit consent, or being on the basis of a law that permits such collection for “archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.”
- Check if the data that need to be collected relate to “criminal convictions and offences”, in which case special laws will apply.

¹ General Data Protection Regulation, EU Regulation 2016/679, Art. 5(1)(a).

² General Data Protection Regulation, EU Regulation 2016/679, Art. 5(1)(b).

³ General Data Protection Regulation, EU Regulation 2016/679, Art. 5(1)(c).

⁴ General Data Protection Regulation, EU Regulation 2016/679, Art. 5(1)(d).

⁵ General Data Protection Regulation, EU Regulation 2016/679, Art. 5(1)(e).

⁶ General Data Protection Regulation, EU Regulation 2016/679, Art. 5(1)(f).

⁷ General Data Protection Regulation, EU Regulation 2016/679, Art. 5(2).

Background

Under European law, all processing of personal data must be done for a lawful purpose, and with a legitimate aim. While the other principles provide limitations on how personal data may be processed, this principle places restrictions on the purposes for which personal data may be processed.

Lawful basis

The GDPR lays down six legal bases⁸ for which personal data may be lawfully processed. Thus, the purpose of processing of personal data must fall within at least one of the six categories:

- Consent of the individual
- Performance of a contract
- Compliance with a legal obligation, as authorized by law
- Necessary to protect vital interests of a person
- Necessary for legally authorized official or public interest task, as authorized by law
- Legitimate interests

It should be noted that unlike private institutions, public authorities are not permitted to use 'legitimate interest' as a purpose, unless the processing falls outside the scope of the tasks of public authority. Further, 'necessity' and 'public interest' imply a 'pressing social need', as opposed to largely private or commercial advantages.⁹

If 'consent' is used as a basis, then it is important that the purpose is specified clearly and explicitly, and reveals, explains or expresses in an easily understood form why the data is being collected and processed. The consent itself must be freely-given, specific, informed, and unambiguous, and the individual has the right to withdraw the consent at any time.

The GDPR acknowledges that, "it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."¹⁰

The European Data Protection Supervisor (EDPS) notes that, "Specific consent normally required under the GDPR may therefore become less appropriate in the case of collected and inferred data and especially in the case of special categories of data on which much scientific research relies," and thus, "when research purposes cannot be fully specified, a controller would be expected to do more to ensure the essence of the data subject rights to valid consent are served, including through as much transparency as possible and other safeguards."¹¹

Fairness

Further, the way the processing is done must be fair and transparent. Even if the processing that is undertaken has a lawful basis, it may still be unfair, and thus in violation of this principle. Fairness is a broad concept: it requires that researchers only handle personal data in ways that people would reasonably expect, and that they not do anything that may harm the data subjects.

Transparency

Transparency requires that individuals be informed about the intended purposes for collecting and using the personal data; the legal grounds for the processing, etc. This is necessary whether there is direct

⁸ General Data Protection Regulation, EU Regulation 2016/679, Art. 6.

⁹ European Data Protection Supervisor, 'A Preliminary Opinion on Data Protection and Scientific Research', 23.

¹⁰ General Data Protection Regulation, EU Regulation 2016/679, Recital 33.

¹¹ European Data Protection Supervisor, 'A Preliminary Opinion on Data Protection and Scientific Research', 19.

collection of personal data from the individuals concerned (whether consciously provided by the individual, or collected through observation of the individual), or obtaining of personal data from some other source (such as a third-party to whom data has been entrusted, public sources, data brokers, or from other individuals).¹² The information that should be provided, at a minimum includes:¹³

- who your company/organisation is (your contact details, and those of your DPO if any);
- why your company/organisation will be using their personal data (purposes);
- the categories of personal data concerned;
- the legal justification for processing their data;
- for how long the data will be kept;
- who else might receive it;
- whether their personal data will be transferred to a recipient outside the EU;
- that they have a right to a copy of the data (right to access personal data) and other basic rights in the field of data protection (see complete list of rights);
- their right to lodge a complaint with a Data Protection Authority (DPA);
- their right to withdraw consent at any time;
- where applicable, the existence of automated decision-making and the logic involved, including the consequences thereof.

In case you have obtained personal data from a source other than the individuals concerned, you need to inform them within a reasonable period, and at most within a month from your gaining access to their personal data.

Transparency obligations do not apply where and insofar as, the data subject already has the information.¹⁴ For personal data collected from a third-party source, there are three additional situations where transparency obligations do not apply:¹⁵

- Where it proves impossible (in particular for archiving, scientific/ historical research or statistical purposes);
- Where it would involve a disproportionate effort (in particular for archiving, scientific/historical research or statistical purposes); or
- Where providing the information required under Article 14.1 would make the achievement of the objectives of the processing impossible or seriously impair them.

Special categories of personal data / Sensitive data

Special categories of personal data, or sensitive data,¹⁶ are data that reveal a person's:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,

or are:

- genetic data,
- biometric data for the purpose of uniquely identifying a natural person,
- data concerning health, or
- data concerning a natural person's sex life or sexual orientation.

Such sensitive data may not be collected unless the collection falls under one of the ten legitimate grounds provided in the GDPR,¹⁷ which includes explicit consent, as well as when necessary for archival,

¹² General Data Protection Regulation, EU Regulation 2016/679, Art. 12(1), (5), (7), Art. 13, Art. 14, Recitals 39, 58–62.

¹³ European Commission, 'What Information Must Be Given to Individuals Whose Data Is Collected?'

¹⁴ General Data Protection Regulation, EU Regulation 2016/679, Art. 13(4), Art. 14(5)(a).

¹⁵ General Data Protection Regulation, EU Regulation 2016/679, Art. 14(5)(b).

¹⁶ General Data Protection Regulation, EU Regulation 2016/679, Art. 9(1), Recitals 51–56.

¹⁷ General Data Protection Regulation, EU Regulation 2016/679, Art. 9(2)(a).

scientific or historical research, and statistics with the appropriate safeguards that are legally required under the GDPR and are provided under an appropriate law.¹⁸ Given national differences in the laws regulating sensitive data, and especially genetic, biometric, or health data,¹⁹ researchers should consult their institution's data protection officer, or their local data protection authority to know more about what's permissible and what's not.

Further, while data relating to criminal convictions and offences aren't categorized as "sensitive" under the GDPR, the regulation requires that all usage of such data by researchers need to additionally be authorized under an EU or national law, and follow the safeguards provided under such law.²⁰

2.2. Purpose limitation

To comply with the purpose limitation principle, researchers should:

- Document in clear and specific terms the purposes behind the collection and use of personal data.
- Provide individuals information on the purposes behind their data collection and use.
- Restrict processing of personal data to the specified purposes or to purposes that are compatible with the specified purposes.
- Ensure they notify the individual in those situations where the original ground for use of the personal data was something other than consent or a legal requirement, and now those data are being put to a new compatible use. This should be done reasonably prior to the new use of the personal data taking place, so as to enable the individual to object to the processing.
- Ensure they request fresh consent in those situations where the original ground for use of the personal data was consent, and now those data are being put to any other use (regardless of whether the new use is a 'compatible' use).
- Ensure they have either consent or a clear obligation/function provided in the public interest in a law if they wish to use the personal data for purposes other than those specified or compatible.
- Ensure that the new use is fair, lawful, and transparent.

Background

The purpose should be "specified, explicit, and legitimate".²¹ The Article 29 Working Party notes that, "a purpose that is vague or general, such as for instance ... 'future research' will — without more detail — usually not meet the criteria of being 'specific'. That said, the degree of detail in which a purpose should be specified depends on the particular context in which the data are collected and the personal data involved. In some clear cases, simple language will be sufficient to provide appropriate specification, while in other cases more detail may be required."²²

The permission to process are limited to:

- the legitimate purposes which were explicitly specified when the data were collected, or to
- other purposes that are compatible with the initial purposes

Compatibility may be judged using the following criteria:

- a) the link between the initial purposes and the additional purposes under consideration;
- b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- c) the nature of the personal data, in particular whether they include special categories of (i.e., sensitive) personal data or personal data related to criminal convictions and offences are processed
- d) the possible consequences of the intended further processing for data subjects;

¹⁸ General Data Protection Regulation, EU Regulation 2016/679, Art. 89.

¹⁹ General Data Protection Regulation, EU Regulation 2016/679, Art. 9(4).

²⁰ General Data Protection Regulation, EU Regulation 2016/679, Art. 10.

²¹ General Data Protection Regulation, EU Regulation 2016/679, Art. 5(1)(b).

²² Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation', 15–16.

e) the existence of appropriate safeguards, which may include pseudonymization.

Some purposes that are *presumed* to be compatible, if appropriate, legally-prescribed safeguards are followed, are:

- archiving in the public interest,
- scientific or historical research, and
- statistics

However, as the EDPS notes, “The presumption is not a general authorisation to further process data in all cases for historical, statistical or scientific purposes. Each case must be considered on its own merits and circumstances. But in principle personal data collected in the commercial or healthcare context, for example, may be further used for scientific research purposes, by the original or a new controller, if appropriate safeguards are in place... in order to ensure respect for the rights of the data subject, the compatibility test under Article 6(4) should still be considered prior to the reuse of data for the purposes of scientific research, particularly where the data was originally collected for very different purposes or outside the area of scientific research.”²³

2.3. Data minimization

To be in line with the data minimization principle, researchers need to:

- Ensure they only collect personal data if they are adequate, relevant, and necessary for the purpose they have specified.
- Refrain from collecting larger amounts of personal data than needed.
- Refrain from collecting more detailed or granular kinds of personal data than needed.
- Ensure that they do not store personal data for longer than is necessary.
- Review the personal data that they store periodically to check if they continue to be in compliance with the above, and remove any personal data that do not qualify.

Background

Adequacy, relevance, and necessity are three requirements for personal data processing under the GDPR. Thus, data that are inadequate, i.e., unfit for the purpose specified, cannot be collected or processed; the data must also be relevant, i.e., they must serve the purpose specified. And the limitation on necessity has three aspects:

- quantity of data;
- granularity of data, and
- duration of storage (covered more fully in the “storage limitation” principle below)

Thus, in simple terms, researchers should seek to collect, store, and process as little personal data as necessary, for as short a time period as possible for achieving the specified purpose. This, as with other principles, is achieved through both technical and organizational measures.

Data minimization is listed as an especial concern in the GDPR for those who process personal data for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, since these are operate under a slightly relaxed regime when it comes to the principle of purpose limitation. Measures that can be taken for data minimization include pseudonymisation, if that’s feasible.

2.4. Accuracy

To comply with the principle of accuracy, researchers should:

- Ensure that the personal data they hold are factually correct.
- Ensure that the personal data they hold are up-to-date.

²³ European Data Protection Supervisor, ‘A Preliminary Opinion on Data Protection and Scientific Research’, 22–23.

- Put in place processes to check for the accuracy of the data, with timelines for checking currency.
- Correct any factually incorrect or misleading data as soon as they are discovered.
- Record any mistakes that are needed to be preserved as mistakes, along with the reason for preservation.
- Comply with any requests for rectification from individuals.

Background

There are two aspects to the principle of accuracy: factual correctness and being up-to-date. It is prohibited to use inaccurate personal data, since that could be unfit for the purpose the data are sought for. Further, inaccurate data could harm the data subjects, and may thus violate the principle of fairness. Thus, researchers are under an obligation to erase or correct inaccurate personal data.

In order to ensure that their personal data are accurate, data subjects have been granted a right to seek rectification of data.

2.5. Storage limitation

To ensure compliance with the principle of storage limitation, researchers need to:

- Ensure they do not store personal data for longer than necessary for the purpose citing which they were collected.
- Ensure they either delete or anonymize personal data that are no longer necessary.
- Document the purpose for which personal data were collected, and how long the data needs to be retained for achieving that purpose.
- Document the justification for the period of retention.
- Review the necessity of retention when the pre-determined retention period ends.
- Identify and document the public interest archiving, scientific or historical research, or statistical purpose for which data are being stored for longer than strictly necessary, in case the data are being stored under the exception for such research, along with compliance with adequate safeguards, as legally prescribed under Art. 89.

Background

Researchers should not keep personal data for longer than is necessary for the specified purposes for which the data were collected. The data should be destroyed as soon as they are no longer necessary for the specified purposes.

One way to effectuate this is by engaging in anonymization of data wherever possible, thus converting personal data into data that no longer permits direct or indirect identification of the data subjects to which they pertain.

Researchers are allowed to keep personal data for longer than strictly necessary if the personal data are to be used solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and if they further meet the conditions laid down in Article 89 of the GDPR of having adequate safeguards in the form of appropriate technical and organisational measures to safeguard individual's rights. Further, researchers should ensure they do not use such personal data as the basis for any measure or decision regarding any particular individual.²⁴

2.6. Integrity and confidentiality

To comply with the principle of integrity and confidentiality, researchers must:

²⁴ Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation', 28.

- Ensure that personal data are kept securely, protecting against unauthorized or unlawful processing, and against accidental loss, destruction or damage, using both technical and organizational measures.
- Document the technical and organizational measures that are put in place to ensure security.

Background

Researchers are obligated to ensure that personal data are kept securely, meaning that they ensure confidentiality, integrity, and availability of the data, and thus protect against unauthorized or unlawful processing and against accidental loss, destruction or damage, using both technical and organizational means.

Thus, data security is a core part of the protection of personal data. In addressing whether confidentiality and integrity have been met, it is important to look at it from the perspective of the data subjects, and not from the perspective of the researchers. In other words, even if the researchers haven't suffered any damage because of unauthorized processing, that can't be said to mean that the unauthorized processing caused no harm.

This means that researchers need to have come up with clearly designated roles and responsibilities so that it is clear who all have authorized access to personal data for any particular research undertaking.

2.7. Accountability

For compliance with the principle of accountability, researchers must:

- Ensure that they are proactively and organized in their compliance with data protection law.
- Learn about the obligations placed on them and the rights that individuals have under the law.
- Put in place clear policies, processes, and technical measures that ensure compliance with the above principles and the law.
- Ensure that the 'privacy by design and by default' approach is followed.
- Ensure that their organization has a data protection officer in case they are a public authority or body; if they engage in regular and systematic monitoring of individuals on a large scale; or if they process a large scale of special categories of data, such as sensitive data.
- Conduct a data protection impact assessment if the type of data processing they wish to undertake is likely to result in a high risk, and in particular if they plan to use systematic and extensive profiling with significant effects; process special category or criminal offence data on a large scale; or systematically monitor publicly accessible places on a large scale.
- Notify individuals, usually through your institution's data protection officer, of a data breach no later than 72 hours if the breach is likely to pose a risk to the rights and freedoms of the individuals whose personal data were breached.
- Respond immediately to any exercise by individuals of their rights over their data.
- Document their compliance with all the above principles and the law.

Background

Those who are collecting and using personal data, such as researchers, are responsible for compliance with the principles listed above. Importantly, they need to be able to demonstrate that they are compliant.

Thus compliance with these principles needs to be planned and documented. For instance, researchers should be able to justify why they need certain personal data at the granularity at which they are collecting them and the duration for which the data are being stored. Many aspects of accountability would benefit from having automated technical measures in place.

3 Good practices relating to data protection principles

Good practices for data protection principles covers practices that go beyond the minimum that is legally mandated under the GDPR and national laws. Though they are not legally required, they will help researchers comply with the data protection principles already discussed in this document.

3.1. Anonymization, pseudonymization and encryption

The varied requirements of the GDPR do not apply if researchers are not handling *personal data*. Hence, whenever possible, check if the data that needed for the research requires to being able to identify a person. But do note that the GDPR distinguishes between pseudonymized data and anonymized data. Just removing all personal identifiers does not automatically make data “anonymized”.

Pseudonymous personal data refers to personal data that can no longer be attributed to a specific data subject without the use of additional information; but with additional information, the data subject can be uncovered.

For anonymized data, not only must one not be able to identify any particular individual based on the data one has collected and processed, but one also need to consider all the means that others may find “reasonably likely to be used, such as singling out ... to identify the natural person directly or indirectly.” To see what means are “reasonably likely to be used to identify the natural person”, the GDPR informs us that “account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”¹ Thus, if it is practically possible to de-anonymize the data, then that can’t be seen as anonymized data — it would then be pseudonymized data, which still counts as personal data.

The GDPR suggests pseudonymization and encryption as two means of ensuring better security of personal data. Both techniques would help in fulfilling the requirements of the principle of integrity and confidentiality. Pseudonymization would also help in complying with the principle of data minimization. In case of some kinds of data processing for scientific research, for which the principle of purpose limitation are slightly relaxed, the GDPR requires that researchers seek to minimize data, and to do so using pseudonymization wherever possible or to anonymize the data if that’s feasible.²

3.2. Aggregate and coarse data

Whenever possible, prefer aggregate data over individual-level data, and prefer coarse data over granular data. For instance, if age data is required, choose to collect it in the form of a number rather than a date of birth. Better yet, if an age range would suffice, opt to collect that instead of a precise age. Lastly, if the date of multiple persons can be aggregated and the individual-level data destroyed, then opt to do so.

3.3. Transparency

If personal data is collected in an online context, provide a prominent link to the privacy statement or notice, or ensure that the information is available on the same page on which the personal data is

¹ General Data Protection Regulation, EU Regulation 2016/679, Recital 26.

² General Data Protection Regulation, EU Regulation 2016/679, Art. 89(1).

collected.³ If there are changes in how you are processing personal data, all the information should be provided again to the data subject, while making it easy to tell what information amongst it is new.⁴

3.4. Multiple grounds for processing

The GDPR seems to allow the possibility of multiple lawful grounds being used for processing of the same personal data. However, this could lead to a situation where two grounds (such as consent and legitimate interest) are used, but one of the grounds is removed (such as an individual revoking consent). In such a case, it is unclear what the law requires, and there is no clear unanimous view amongst legal authorities. It is preferable to resolve this uncertainty through a conservative understanding of the law, and ceasing to process any data when any of the grounds disappears. To avoid this situation, it may be preferable not to combine consent with any other grounds. In such cases, it may be preferable to choose to only process data under the most appropriate ground.

3.5. Consent in data protection and in ethics

Consent as a lawful ground for processing data under data protection law is different from “informed consent” as a principle of ethics for research on human subjects.⁵ Thus it is always preferable to provide separate consent forms and obtain each type of consent separately. Even if the institution obtains both using a single consent form, a clear record should be maintained of what each participant has consented to with regard to the research.

Even in cases where consent is not used as the ground under the GDPR, “*informed consent* as a human research participant could still serve as an ‘appropriate safeguard’ of the rights of the data subject.”⁶

3.6. Legitimacy, fairness, and ethics approvals

Legitimacy of data collection will sometimes be determined by laws that prescribe ethical requirements (such as for clinical trials). But even when specific research isn’t covered by legal requirements of ethics clearance, it is best to work on the presumption that unethical data collection or use will also be seen as an illegitimate purpose for the basis of the GDPR, as well as not complying with the principle of fairness. Thus, for instance, researchers should refrain from engaging in any data processing that an ethics review board disapproves of.

3.7. Data protection authorities and ethics boards

Given the increasing interplay between ethical issues and privacy and data protection issues, it would be profitable for ethics review boards to engage more fully with data protection officers and authorities.⁷ There are many instances (such as genetic data) in which the use of an individual’s personal data in research would affect not only that individual, but also others. The framework of data protection alone may be inadequate to capture those concerns in a way that a combined framework of research ethics and data protection could. This calls for greater collaboration between those working on ethical issues and those working on data protection issues.

³ Article 29 Data Protection Working Party, ‘Guidelines on Transparency Under Regulation 2016/679’, 8.

⁴ Article 29 Data Protection Working Party, 27–28.

⁵ European Data Protection Supervisor, ‘A Preliminary Opinion on Data Protection and Scientific Research’, 19–20.

⁶ European Data Protection Supervisor, 20.

⁷ European Data Protection Supervisor, 25.

3.8. Data protection guidelines and DPOs

Many research institutions have issued data protection guidelines, in addition to ethics guidelines. Researchers should familiarize themselves with their institution's guidelines. Many times, funders have special requirements around data protection as well. All Horizon 2020-funded projects, for instance, require the involvement of a data protection officer (DPO) if one has been appointed, and even in cases where a DPO is not legally required,⁸ a data protection policy needs to be elaborated.

There are some issues on which member-state laws apply, rather than just the GDPR. Importantly for researchers, the special data protection regime for processing for the purposes of archiving in the public interest, scientific or historical research, or statistical purposes, can have relaxations in the rights of the individual and the consequent obligations of the researcher, if national laws allow for it. Appropriate safeguards are required for processing of personal data for any of these such purposes. Researchers need to abide by the principles discussed above, and need to pay especial attention to technical and organizational measures to ensure data minimization.⁹ Given that the specifics of researchers' obligations under the law are thus not uniform, researchers should consult their institution's data protection officer and data protection guidelines if possible, as they would be able to help guide researchers on the applicable legal and extra-legal standards.

3.9. Data protection impact assessment

If a project will deal with a large quantity of personal data, or the personal data or vulnerable people, then discussing such a project with the DPO and instituting a data protection impact assessment (DPIA) would be beneficial, even when it isn't legally mandatory to do so. The EDPS notes that a "DPIA is mandatory for data processing operations presenting high risks to data subjects, such as when two of the following criteria apply":¹⁰ 1. Systematic evaluation/profiling 2. Automated decision making 3. Systematic monitoring 4. Sensitive data processing 5. Large scale processing 6. Match/combine datasets with different purposes 7. Vulnerable data subjects 8. New technologies 9. Preventing people from exercising their rights or entering into a service/contract

⁸ General Data Protection Regulation, EU Regulation 2016/679, Art. 38.

⁹ General Data Protection Regulation, EU Regulation 2016/679, Art. 89.

¹⁰ European Data Protection Supervisor, 'Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA Lists Issued Under Articles 39(4) and (5) of Regulation (EU) 2018/1725', Annex 1.

4 Annexures

4.1. Annexure 1: Key resources

The PANELFIT project has put together a detailed set of guidelines on data protection, ethical, and legal issues in ICT research and innovation, as well as a critical analysis of the ICT data protection regulatory framework. The CCDP is largely based on those two documents. Those who wish to understand more about the issues raised in the CCDP or wish to understand the aspects of data protection that weren't covered in the CCDP are urged to consult the Guidelines, which provide far more detail.

They will both be made available at <https://www.panelfit.eu/deliverables/>.

Here are some other important resources for researchers seeking to learn more about data protection and responsible research and innovation.

- European Data Protection Supervisor. “A Preliminary Opinion on Data Protection and Scientific Research,” January 2020. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
- Article 29 Data Protection Working Party. “Opinion 03/2013 on Purpose Limitation,” April 2, 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
- Article 29 Data Protection Working Party. “Opinion 05/2014 on Anonymisation Techniques,” April 10, 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf*
- Article 29 Data Protection Working Party. “Guidelines on Transparency under Regulation 2016/679,” November 29, 2017. <https://ec.europa.eu/newsroom/article29/items/622227>.
- European Data Protection Board. “Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak.” Guidelines, April 30, 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.
- European Data Protection Board. “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.” Guidelines, November 13, 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.
- European Data Protection Board. “Guidelines 04/2019 on Article 25: Data Protection by Design and by Default.” Guidelines, October 20, 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
- European Data Protection Supervisor. “EDPS Guidelines on Assessing the Proportionality of Measures That Limit the Fundamental Rights to Privacy and to the Protection of Personal Data,” December 19, 2019. https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.
- European Data Protection Supervisor. “Flowcharts and Checklists on Data Protection.” 2020. <https://doi.org/10.2804/823679>.
- European Commission (Directorate-General for Research and Innovation). “Ethics and Data Protection,” November 2018. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf.
- ALLEA. *The European Code of Conduct for Research Integrity*. 2nd ed., 2017. <https://ec.europa.eu/>

[research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf](#).

- RESPECT Project. “RESPECT Code of Practice for Socio-Economic Research.” Institute for Employment Studies, 2004. http://www.respectproject.org/code/respect_code.pdf
- EFAMRO and ESOMAR. “Guidance Note for the Research Sector: Appropriate Use of Different Legal Bases under the GDPR.” June 2017. https://www.esomar.org/uploads/public/government-affairs/position-papers/EFAMRO-ESOMAR_GDPR-Guidance-Note_Legal-Choice.pdf.
- Wilford, Sara, Malcolm Fisk, and Bernd Stahl. “Guidelines for Responsible Research and Innovation.” GREAT Project, 2016. <https://www.great-project.eu/Deliverables10>.
- The European Data Protection Board has stated that it “intends to issue guidance on the ‘horizontal and complex’ conditions for the applicability of the ‘presumption of compatibility’ of further processing for archiving purposes in the public interest, scientific, historical research or statistical purposes, as provided for by the GDPR Article 5(1)(b).”¹ That will be useful for researchers when it is issued.

4.2. Annexure 2: Bibliography

Article 29 Data Protection Working Party. ‘Guidelines on Transparency Under Regulation 2016/679’, 29 November 2017. <https://ec.europa.eu/newsroom/article29/items/622227>.

———. ‘Opinion 03/2013 on Purpose Limitation’, 2 April 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

European Commission. ‘Science with and for Society’. Horizon 2020, 11 November 2013. <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/science-and-society>.

———. ‘What Information Must Be Given to Individuals Whose Data Is Collected?’. Text. Principle of the GDPR - What information must be given to individuals whose data is collected?, 8 January 2018. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-information-must-be-given-individuals-whose-data-collected_en.

European Data Protection Board. ‘Opinion of the Board (Art. 70.I.b)’. Opinion, 23 January 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

European Data Protection Supervisor. ‘A Preliminary Opinion on Data Protection and Scientific Research’, January 2020. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

———. ‘Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA Lists Issued Under Articles 39(4) and (5) of Regulation (EU) 2018/1725’, 16 July 2019. https://edps.europa.eu/sites/default/files/publication/19-07-16_edps_dpia_list_en.pdf.

General Data Protection Regulation, EU Regulation 2016/679 (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504>.

‘Rome Declaration on Responsible Research and Innovation in Europe’, 21 November 2014. https://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf.

4.3. Annexure 3: Process for Creating the Code of Conduct on Data Protection for Responsible Research and Innovation

We sought to involve multiple stakeholders in the review of the CCDP and obtain as much feedback as possible. The consultation process is described below.

The first draft of the CCDP was circulated in October 2020 and the final version was consolidated in August 2021. Five versions were generated at different stages of the process, incorporating feedback at each step. The following sections summarize the CCDP feedback process, capture the most significant comments received, and the steps taken to respond in each case.

The scope of each of the feedback stages is described below:

¹ European Data Protection Board, ‘Opinion of the Board (Art. 70.I.b)’.

- Consultation of internal experts (PANELFIT): the first version of the CCDP generated in October 2020 was reviewed by the PANELFIT Project consortium that includes experts in cybersecurity, governance, privacy, data protection, among others.
- Consultation of external experts (stakeholders): this consultation was carried out through the Mutual Learning Encounter for stakeholders organized by the project. In this online event held on April 20 2021, 13 people from the following organizations met: ALLEA, European Group on Ethics (EGE) to the European Commission, University of Vilnius, NEC Laboratories Europe, Tech Uni Cluj-Napoca, Museum for Naturkunde, COCIR, Babes-Bolyai University, Research Centre for Data Science and Senior Lecturer, School of Computing, Electronics and Mathematics at Coventry University, Uni Babes Bolyai, European Commission, Open Science (DG RTD), Tilburg University, School of Computing, Electronics and Mathematics at Coventry University, University of Copenhagen.
- Consultation of external researchers: researchers from various disciplines participated in the Mutual Learning Encounter for researchers organized by the project. The online event was held on June 24 2021.
- Public consultation: the CCDP was published on the PANELFIT website with a form available to receive feedback from any interested person. Participation in feedback was promoted through social networks and mailing lists. The document was available from March to August 2021 at the following link: <https://www.panelfit.eu/a-code-of-conduct-on-data-protection-for-responsible-research-and-innovation-ccdip/>
- Survey of researchers: the survey was part of the CCDP feedback closing process. It was circulated before, during and after MLE for researchers. The feedback contributed to the improvement of the good practices section.