

4. Personal data

This section concerns projects with activities that involve processing of personal data, regardless of the method used (*e.g. interviews, questionnaires, direct online retrieval etc.*).

Personal data — Information relating to an identified or identifiable natural person.


An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 2(a) EU General Data Protection Regulation [2016/679](#) (GDPR)).

Examples: name, address, identification number, pseudonym, occupation, e-mail, CV, location data, Internet Protocol (IP) address, cookie ID, phone number, data provided by smart meters, data held by a hospital or doctor.

Individuals are not considered 'identifiable' if identifying them requires excessive effort.

Completely anonymised data do not fall under the data protection rules (as from the moment it has been completely anonymised, the GDPR is not applicable).

Special categories of personal data (formerly known as 'sensitive data') — Include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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 (Article 9(1) GDPR).

 The processing of such data is subject to more stringent data-protection safeguards. Member states may introduce special derogations/limitations with regard to the processing of genetic, data, biometric data and data concerning health.

Personal data related to criminal convictions and offences — Can be only processed under the control of official authorities or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects (Article 10 GDPR).

The processing of personal data by state authorities for law enforcement purposes is governed by EU Directive 2016/680. **Processing of personal data** — Any operation (or set of operations) performed on personal data, either manually or by automatic means. This includes:

- collection (digital audio recording, digital video caption, etc.)
- recording
- organisation, structuring and storage (cloud, LAN or WAN servers)
- adaptation or alteration (merging sets, appification, etc.)
- retrieval and consultation
- use
- disclosure by transmission, dissemination or otherwise making available (share, exchange, transfer)
- alignment or combination

- restriction, erasure or destruction.

Examples: access to/consultation of a database containing personal data; managing of the database; posting/putting a photo of a person on a website; storing IP addresses or MAC addresses; video recording (CCTV); creating a mailing list or a list of participants.

Data processing in research projects — Processing normally covers **any** project that uses data for research purposes (even if interviewees, human volunteers, patients, etc. are *not* actively included in the research).

Personal data may come from any type of research activity (*ICT research, genetic sample collection, tissue storage, personal records (financial, criminal, education, etc.), lifestyle and health information, family histories, physical characteristics, gender and ethnic background, location tracking and domicile information, etc.*).

4.1 Ethics issues checklist

Section 4: PROTECTION OF PERSONAL DATA	YES/NO		Information to be provided in the proposal	Documents to be provided on request
Does your activity involve processing of personal data?	<input type="checkbox"/>	<input type="checkbox"/>	<p>1) Details of the technical and organisational measures to safeguard the rights and freedoms of the participants/data subjects. These may include:</p> <ul style="list-style-type: none"> - Project specific data protection policy and/or the contact details of the data protection officer (these must be provided to the participants) <p>The security measures to prevent unauthorised access to personal data</p> <ul style="list-style-type: none"> - Anonymisation /pseudonymisation techniques. <p>2) Details of the informed consent procedures with regard to the data processing (if relevant).</p> <p>3) Explanation as to how all of the processed data is</p>	<p>1) Informed consent forms and information Sheets (if relevant).</p> <p>2) Data management plan (if relevant).</p> <p>3) Data protection impact assessment (if relevant).</p>

			relevant and limited to the purposes of the project ('data minimisation' principle) 4) Justification of why personal data will not be anonymised/pseudonymised (if relevant). 5) Details of the data transfers (type of data transferred and country to which data are transferred).		
If YES:	Does it involve the processing of special categories of personal data (e.g. sexual lifestyle, ethnicity, genetic, biometric and health data, political opinion, religious or philosophical beliefs)?	<input type="checkbox"/>	<input type="checkbox"/>	1) Justification for the processing of special categories of personal data (if relevant). 2) Justification to why the project objectives cannot be reached by processing anonymised/pseudonymised data (if applicable).	
If YES:	Does it involve processing of genetic, biometric or health data?	<input type="checkbox"/>	<input type="checkbox"/>		1) Declaration confirming compliance with the laws of the country where the data were collected.
	Does it involve profiling, systematic monitoring of individuals, or processing of large scale of special categories of data or intrusive methods of data processing (such as, surveillance, geolocation tracking etc.)?	<input type="checkbox"/>	<input type="checkbox"/>	1) Details of the methods used for tracking, surveillance or observation of participants. 2) Details of the methods used for profiling. 3) Assessment of the ethics risks related to the data processing operations. 4) Explanation as to how the rights	1) Opinion of the data controller on the need for conducting data protection impact assessment under art. 35 GDPR. (if relevant).

				<p>and freedoms of the participants/data subjects will be safeguarded and harm will be prevented.</p> <p>5) Explanation as to how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded.</p>	
<p>Does your activity involve further processing of previously collected personal data <i>(including use of pre-existing data sets or sources, merging existing data sets)?</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	<p>1) Details of the database used or of the source of the data.</p> <p>2) Details of the data processing operations.</p> <p>3) Explanation as to how the rights of the participants/data subjects will be safeguarded.</p> <p>4) Explanation as to how all of the processed data is relevant and limited to the purposes of the project ('data minimisation' principle)</p> <p>5) Justification of why the data will not be anonymised/pseudonymised (if relevant).</p>	<p>1) Confirmation that the data controller has a lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects 2) Permission by the owner/manager of the data sets (<i>e.g. social media databases</i>) (if applicable). 3) Informed Consent Forms + Information Sheets + other consent documents (if applicable).</p>	
<p>Is it planned to export personal data (data transfer) from the EU to non-EU countries?</p> <p><i>Specify the type of personal data and countries involved</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	<p>1) Details of the types of personal data and countries involved.</p> <p>2) Explanation as to how the rights and freedoms of the participants/data</p>	<p>1) Confirmation that data transfers will be made in accordance with Chapter V of the General Data Protection Regulation 2016/679</p>	

			subjects will be safeguarded	
Is it planned to import personal data (data transfer) from non-EU countries into the EU or from a non-EU country to another non-EU country? <i>Specify the type of personal data and countries involved</i>	<input type="checkbox"/>	<input type="checkbox"/>	1) Details of the types of personal data and countries involved.	1) Confirmation of compliance with the laws of the country in which the data was collected.
Does this activity involve the processing of personal data related to criminal convictions or offences?	<input type="checkbox"/>	<input type="checkbox"/>	1) Details on the personal data to be processed and the legal basis for the processing; 2) Risk assessment for the data processing operations. 3) Explanation as to how harm will be prevented and the rights of the participants/data subjects will be safeguarded.	1) Opinion of the data controller on the need for conducting data protection impact assessment under art.35 GDPR.(if relevant).

4.2 How do I deal with the issues?

Your activities must comply with the ethics provisions set out in the Grant Agreement, and notably:

- highest ethical standards
- applicable international, EU and national law (in particular, the GDPR, national data protection laws and other relevant legislation).

Under these rules, personal data must be processed in accordance with certain principles and conditions that aim to **limit** the negative **impact** on the persons concerned and ensure **fairness, transparency** and **accountability** of the data processing, **data quality** and **confidentiality**.

This implies the following main obligations:

- data processing should be subject to appropriate safeguards (*see table above*)
- data should wherever possible be processed in anonymised or pseudonymised form
- data processing is subject to free and fully informed consent of the persons concerned (unless already covered by another legal basis, *e.g. legitimate or public interest*)
- data processing must NOT be performed in secret and participants/data subjects must be made aware that they take part in the project and be

informed of their rights and the potential risks that the data processing may bring

⚠ Information about the data processing operations and the contact details of the data protection officer (project DPO or partner DPO, whichever relevant) must be provided to the participants (art.13/art.14 GDPR).

- data may be processed ONLY if it is really adequate, relevant and limited to what is necessary for the project ('data minimisation principle')

⚠ Collecting personal data (*e.g. on religion, sexual orientation, race, ethnicity, etc.*) that is not essential to your project may expose you to allegations of hidden objectives or mission creep (*i.e. collecting information with permission for one purpose and using it/making it available – online or otherwise – for another reason, without additional permission*).

- data processing operations which are more intrusive and likely to raise higher ethics risks must be subject to higher safeguards
- for complex, sensitive or large-scale data processing or data transfers outside of the EU, you should consult your data protection officer (DPO), if you have one, or a suitably qualified expert
- the level of data security must be appropriate to the risks for the participants/data subjects in case of unauthorized access or disclosure, accidental deletion or destruction of the data
- you are responsible for all your partners, contractors or service providers that process data at your request or on your behalf.

Generally, one of the best ways how to avoid/limit data protection issues for your project is to use **anonymised** or **pseudonymised** data.

⚠ Pseudonymisation and anonymisation are not the same thing.

'Anonymised' means that the data has been rendered anonymous in such a way that the data subject can no longer be identified (and therefore is no longer personal data and thus outside the scope of data protection law).

'Pseudonymised' means to divide the data from its direct identifiers so that linkage to a person is only possible with additional information that is held separately. The additional information must be kept separately and securely from processed data to ensure non-attribution.

Moreover, if you have a **data protection officer** (DPO), it is generally recommended to involve them in all stages of your project, whenever it comes to privacy and data protection issues, since this will help your proposal and grant implementation (EU grants are subject to full compliance with privacy and data protection rules).

⚠ Be aware that even if you solve all privacy-related issues, data may still raise other ethics issues, such as potential misuse of methodology/findings or ethics harms to specific groups.

For further advice on how to ensure that your data processing operations are compliant, please consult the [Guidance on ethics and data protection in research projects](#).

4.3 What do you need to provide?

If your proposal raises one of the issues listed in the ethics issue checklist above, you must complete the **ethics self-assessment** in **Part A** of your proposal.

Your grant proposal must include the **information** referred to in the ethics issues checklist and any of the **documents** already available. Documents that are not submitted together with the proposal should be kept on file and may have to be provided later on, if requested by the granting authority.

Background documents & further reading

General

EU Regulation [2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1)

EU Directive [2016/680](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89)

[Note on ethics and data protection](#)

[Guidelines, Recommendations and Best Practices, European Data Protection Board](#)

[Handbook on European data protection law](#) (2018 edition), European Union Agency for Fundamental Rights and Council of Europe, European Court of Human Rights, European Data Protection supervisor

Data transfers outside the EU: [International data transfers using model contracts](#)

Electronic communications

EU Directive [2002/58/EC](#) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

EU Directive [2006/24/EC](#) of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks