Horizon 2020 Projects: Ethics Compliance under GDPR

Albena Kuyumdzhieva, PhD
Programme Manager Ethics/Research Review
Ethics and Research Integrity Sector, SAM
DG Research and Innovation, European Commission

European Convention on Human Rights

ARTICLE 8

Right to respect for private and family life

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

2. 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.

Data protection: ~~R~~evolution

- *Key principles fairly constant for 35 years;*
- *1980 OECD Guidelines;*
- *1981 CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;*
- *1995 Directive EC/95/64;*
- *100 countries;*
- *GDPR 2016/679.*

Charter of Fundamental Rights of the European Union

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.

Treaty on the Functioning of the European Union

Article 16
(ex Article 286 TEC)

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

European Commission

EU Data Protection Reform: Main Principles

- *Builds on the principles of the previous Data Protection Directive 95/46/EC;*
- *Increases transparency and accountability of the data processing;*
- *Enhances the data protection rights of the individuals.*

EU General Data Protection Regulation: Scope and Application

- *Processing of personal data of living individuals;*
- *Data controllers/processors established in EU;*
- *Non-EU data controllers/processors, processing personal data of data subjects who are in the EU while:*
  - **offering them goods or services;**
  - **monitoring their behaviour.**

Some useful terms

Personal data *is any information relating to an identified or identifiable (directly or indirectly) natural person.*

Identifiers:

- Name;
- Identification number;
- Location data;
- Online identifier (e.g. IP, cookie ID);
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Processing of data is any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special Categories of Personal Data

- ***Genetic data****;*
- ***Biometric data;***
- *Data concerning* ***health*** *or data concerning a natural person's* ***sex life or sexual orientation****;*
- *Personal data revealing* ***racial*** *or* ***ethnic origin****,* ***political opinions, religious*** *or* ***philosophical beliefs,*** *or* ***trade union membership.***

European Commission

Anonymisation

A process of ensuring that the risk of somebody being identified in the data is negligible.

Some useful terms

Pseudonymised data: where obvious identifiers (e.g. names and addresses) have been **replaced with indirect identifiers** (e.g. numbers) in the main data set and the indirect identifiers are then held with the obvious identifiers in a separate data set (known as the 'key');

NB!

Pseudonymised personal data, which could be attributed to a natural person by the use of additional information is considered to be information related to an identifiable natural person and thus falls within the scope of GDPR!

Some useful terms

European Commission

Consent

FREELY FIVEN

Is there imbalance between the data controller and the data subject?

Can the consent be withdrawn as easy as it is given?

SPECIFIC

What is the scope of the given consent?

Possibility to consent only to certain areas of research or parts of research.

INFORMED

In plain language;

Intelligible;

Clearly distinguishable from other issues;

UNAMBIGIOUS

Absolutely clear

European Commission

Data Minimisation

Personal data should be **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed.

Risk Based Approach

Data protection must be proportionate to the risks to data subjects.

Indicators of data processing operations that may entail higher ethics risk (some examples)

Types of personal data used in the research	* racial or ethnic origin; * political opinions, religious or philosophical beliefs; * genetic, biometric or health data; * sex life or sexual orientation; * trade union membership.
Data subjects involved in the research	* children; * vulnerable persons ; * persons who have not given their explicit consent to participate in the research project.
Scale or complexity of data processing	* large-scale processing of personal data; * systematic monitoring of publicly assessable area on a large scale * involvement of multiple datasets and/or service providers, or the combination and analysis of different datasets (i.e. “big data”).

Indicators of data processing operations that may entail higher ethics risk: some examples

Data collection or processing techniques involved in the research	* privacy-invasive methods or technologies (e.g. the covert observation, surveillance, tracking or deception of individuals); * the use of camera systems to monitor behaviour or record sensitive information; * “data-mining” (including data collected from social media networks), “web-crawling” or “social network analysis”; * the profiling of individuals or groups (particularly behavioural or psychological profiling); * the use of “artificial intelligence” to analyse personal data; * the use of automated decision-making which has a significant impact on the data subject(s).
Involvement of non-EU countries	* Transfer of personal data to non-EU countries; * Collection of personal data outside the EU.

European Commission

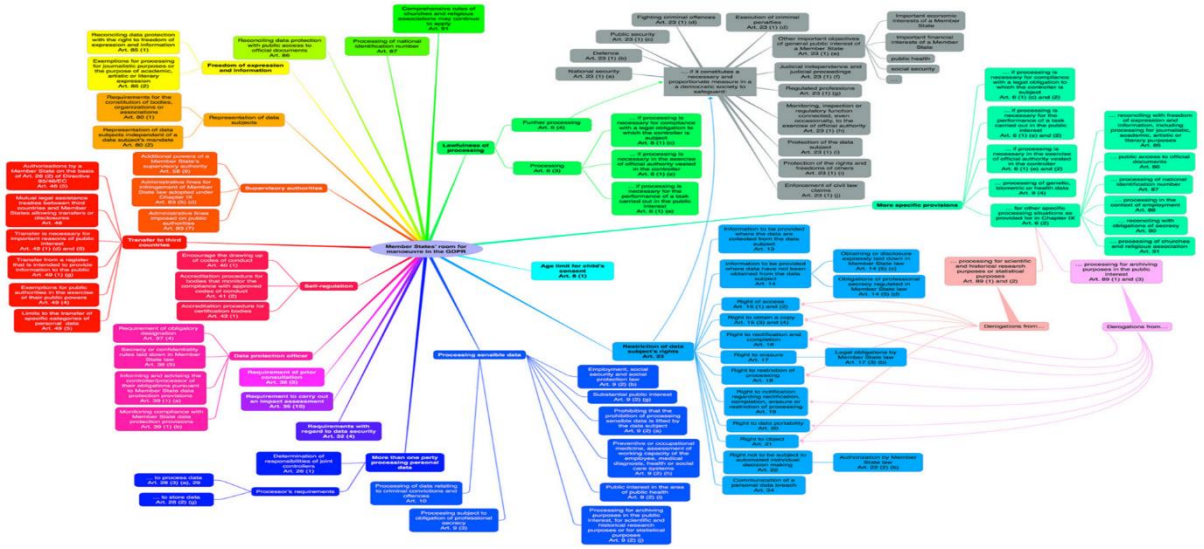
Data Protection Impact Assessments

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a **high risk to the rights and freedoms of natural persons,** the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data(art.35.1. GDPR).

GDPR and Research

- Processing of data for research purposes shall be subject to appropriate safeguards;
- Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation.

GDPR and Research

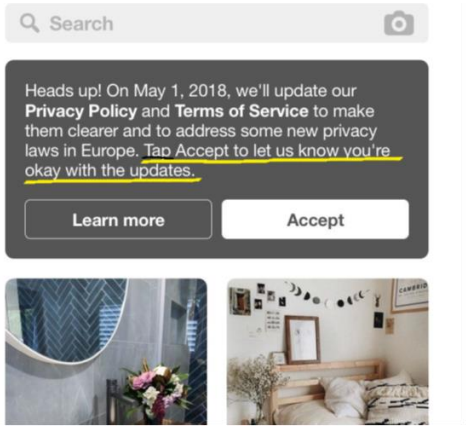


- ✓ Processing of sensitive data is allowed for research purposes;
- ✓ Member states may introduce further conditions or limitations with regard to the processing of **genetic, biometric and health data** and adopt derogations for some of the data subjects' rights.

Ethics and Data Protection under GDPR:

Lawfulness, FAIRNESS and transparency of data processing.

Main Ethics Concerns



- *Free, voluntary and informed consent;*
- *Utilisation of publicly available data;*
- *Online recruitment;*
- *Anonymisation and Pseudonymisation;*
- *Data Minimisation;*
- *Security Arrangements;*
- *Data Transfers.*

New Data Protection Requirements for H2020 projects

In case personal data are processed, the applicant must:

Confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. If designation of a DPO is not required under the GDPR, a detailed data protection policy for the project must be elaborated.

In case personal data are processed, the applicant must:

Explain how all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation 'principle).

Explain why the research data will not be anonymised/ pseudonymised (if revelavnt).

In case personal data are processed, the applicant must:

Provide detailed information on the informed consent procedures in regard to data processing.

Provide templates of the informed consent forms and information sheets (in language and terms intelligible to the participants).

In case personal data are processed, the applicant must:

Describe the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants. This must also include:

- Description of the respective anonymisation/pseudonymisation techniques;
- Description of the security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing.

European Commission

In cases where special categories of data are processed, the applicant must:

Check if special derogations pertaining to the rights of data subjects or the processing of genetic, biometric and/or health data have been established under the national law and submit declaration of compliance.

Provide justification for the processing of sensitive personal data.

European Commission

In cases of further processing of previously collected data, the applicant must:

Provide details of the data processing operations and database used or of the source of the data.

Confirm the lawful basis for the data processing and describe the appropriate technical and organisational measures that are in place to safeguard the rights of the data subjects.

Provide permission by the owner/manager of the data sets (e.g. social media databases)

In cases the research involves the processing of publicly available data, the applicant must:

Confirm that the data used in the project is publicly available and can be freely used for the project.

Provide permission by the owner/manager of the data sets (e.g. social media databases).

In case personal data are transferred from the EU to a non-EU country, the applicant must:

For countries, not covered by adequacy decision*

Provide details of the types of personal data to be exported.

Confirm that such transfers are in accordance with Chapter V of the GDPR.

*Norway, Liechtenstein, Iceland; Andorra; Argentina; Canada(commercial organisations); Switzerland; Faeroe Islands; Guernsey; Israel; Isle of Man; Japan, Jersey; New Zealand; United States (under Privacy Shield); Eastern Republic of Uruguay

European Commission

In case personal data are transferred from a non-EU country to the EU (or a third country), the applicant must:

Provide details of the types of personal data to be imported.

Confirm that such transfers comply with the laws of the country in which the data was collected.

European Commission

In cases the research involves profiling, the applicant must:

Provide details of the methods used for profiling.

Provide explanation how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded.

In case the research involves **intrusive data processing methods*** **or any other data processing operation that may result in high risk to the rights and freedoms of the research participants,** the applicant must:

Provide details of the methods used for tracking, surveillance or observation of participants.

Explain how will harm be prevented and the rights of the research participants safeguarded.

*Such as, tracking, surveillance, audio and video recording, geo-location tracking etc.

Specific cases

In case the research involves **profiling, systematic monitoring of individuals processing of large scale of special categories of data intrusive methods of data processing or any other data processing operation that may result in high risk to the rights and freedoms of the research participants,** the applicant must:

Evaluate the ethics risks related to the data processing activities of the project. This includes also an opinion if data protection impact assessment should be conducted under art.35 GDPR.

Ethics risk assessment

Assessment of:

- Individual ethics harms (for the research participants);
- Ethics harms to third parties (e.g. family, friends etc.)
- Group level ethics harm (for the community or the group).

Potential ethics risks (non-exclusive list):

- *Discrimination;*
- *Stigmatisation;*
- *Exposing identity and sensitive data (privacy breach);*
- *Security/safety risks for the data*
- *Reputational risk and loss of position within occupational and other settings;*
- *Harms to the interests and wellbeing on the research participants, third parties and the community;*
- *Misuse of data.*

Further help:

Guidance 'How to complete your ethics self-assessment' (2018):
http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

EC Guidance Note on Ethics and Data Protection (2018):
http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

Ethics help desk: RTD-ETHICS-REVIEW-HELPDESK@ec.europa.eu