Data protection in EU projects – Implications of the GDPR

Louiza KALOKAIRINOU, PhD
Policy Officer
Ethics and Research Integrity Sector
DG Research Innovation
European Commission

1. The Ethics Appraisal Process

1. The Ethics Appraisal Process

What is Horizon 2020?

- The biggest EU Research and Innovation programme
- Almost €80 billion of funding available over 7 years (2014-2020)
- It is implemented mainly through open calls for proposals; proposals are evaluated by independent experts
- Emphasis on excellent science, industrial leadership and tackling societal challenges.

- For all activities funded by the EU, ethics is an integral part of research from beginning to end, and ethical compliance is seen as pivotal to achieve real research excellence.

1. The Ethics Appraisal Process

Regulation of establishment (EU No 1291/2013)

Article 19 "Ethical Principles"

All the research and innovation activities carried under Horizon 2020 shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols

1. The Ethics Appraisal Process

ETHICS APPRAISAL STEPS

Activity	Who?	When?	How?
Ethics Self-assessment	Applicant	Application phase	Consideration of ethical issues of the proposal
Ethics Pre-screening/Screening	Ethics experts and/or qualified staff	Evaluation phase	Review of application material
Ethics Assessment (for proposals involving hESC or raising serious ethical issues: severe intervention on humans)	Ethics experts	Evaluation/ Grant preparation phase	Review of application material
Ethics Check/Audit	Ethics experts	Implementation phase	Review of project deliverables/interview with applicants

1. The Ethics Appraisal Process

The Ethics Issues Table:

1. Human embryo/foetuses
2. Human beings
3. Human cells/tissues
4. Personal data
5. Animals
6. Non-EU countries
7. Environment, health & safety
8. Dual-use
9. Exclusive focus on civil applications
10. Misuse
11. Other ethics issues

2. Data Protection Requirements in Horizon 2020 Ethics Review

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.

European Commission

2. Data protection

Key principles fairly consistent for 35 years;

1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data;

1981 CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Directive EC/95/64;

GDPR 2016/679.

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.

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.

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.

2. Data Protection: Key Approaches for the Ethics Review

Risk Based Approach

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

2. Data Protection
Higher Ethics Risk Indicators

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").

Guidance Note on Ethics and Data Protection (2018)

2. Data Protection
Higher Ethics Risk Indicators

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.

Guidance Note on Ethics and Data Protection (2018)

2. Data Protection
Higher Ethics Risk Indicators

In case of higher-risk data processing, researchers must provide a detail analysis of the ethics issues raised by the project methodology including:

- An overview of all planned data collection and processing operations
- Identification and analysis of the ethics issues raised
- An explanation of how these ethics issues will be mitigated in practice

2. Data Protection: Key Approaches for the Ethics Review

Lawfulness, FAIRNESS and transparency of data processing

2. Data Protection Requirements in Horizon 2020 Ethics Review

Consent

Consent is a main pillar ensuring fairness of data processing

Consent needs to be given by a **clear affirmative act establishing a freely given, specific, informed and unambiguous** indication of the data subject's agreement to the processing of their personal data.

2. Data Protection Requirements in Horizon 2020 Ethics Review

Broad consent: Where it is difficult, if not impossible to envision all purposes of personal data processing at the moment of data collection, data subjects may give their consent to certain areas of scientific research (recital 33 GDPR).

Conditions:

- Only if the rights of the data subjects are safeguarded by adherence to the recognised ethical standards of scientific research;
- Data subjects should be allowed to give consent only to certain areas of research or parts of research projects

2. Data Protection Requirements in Horizon 2020 Ethics Review

Technical and organisational measures: Anonymisation/pseudonymisation

Anonymisation: A process of ensuring that all identifying elements are eliminated from a dataset so that the data subject is no longer identifiable;

Pseudonymisation: 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');

2. Data Protection Requirements in Horizon 2020 Ethics Review

Technical and organisational measures: Security

[Box 7] Data security: 10 do's and don'ts

Do

- ✓ use GDPR-compliant tools to collect, process and store research subjects' personal data;
- ✓ take communications security seriously, and devise and implement dedicated protocols for your project as necessary;
- ✓ check the terms and conditions of all of the service providers you use (software, applications, storage, etc.) to process personal data within your project, in order to identify and mitigate risks to the data subjects;
- ✓ encrypt your research data and/or the devices on which they are stored, and ensure that keys/passwords are appropriately protected; and
- ✓ consult your DPO or a suitably qualified expert for advice on how to achieve a level of data security that is commensurate to the risks to your data subjects.

Don't

- ✗ collect data on a personal device such as a smartphone without ensuring that they are properly protected (e.g. consider the implications of automatic back-ups to the cloud, and the device's security features);
- ✗ use free services that may use your participants' data for their own purposes in lieu of payment, or collect data or communicate with research participants via social media platforms without first assessing the data protection implications;
- ✗ use unencrypted email, SMS or insecure 'voice over IP' platforms to communicate with vulnerable participants or those who may be subject to state surveillance;
- ✗ expose personal data to unauthorised access or use when accessing them remotely (e.g. by using insecure wifi connections) or travelling to countries where your devices may be inspected or seized; and
- ✗ assume that your research partners, collaborators or service providers have appropriate information security and data protection policies without checking that this is the case.

2. Data Protection Requirements in Horizon 2020 Ethics Review

Data minimization

Data processing should involve only data that are necessary and proportionate to achieve the specific task or purpose for which they were collected.

Only data needed to meet the research objectives should be collected.

Data minimization applies not only to the amount of personal data collected, but also to the extent to which they may be accessed, further processed and/or shared, the purposes for which they are used, and the period for which they are kept.

2. Data Protection Requirements in Horizon 2020 Ethics Review

- Specific derogation reminder (for health, genetic and biometric data);
- DPO plays a key role in ensuring compliance and safeguarding the rights of the research participants.

2. Data Protection: What is at stake?

Ethics risks may include:

- Discrimination
- Stigmatisation
- Exposing identity and sensitive data (privacy breach)
- Security/safety risks
- 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

Thank you for your attention!

Special thanks to Dr. Albena Kuyumdzhieva

Further help:

Guidance 'How to complete your ethics self-assessment' (2019):
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 helpdesk: RTD-ETHICS-REVIEW-HELPDESK@ec.europa.eu