



Data Protection and Ethics Review Process

Ethics compliance under the GDPR

Albena Kuyumdzhieva
Programme Manager Ethics/Research Review
Ethics and Research Integrity Sector, SAM

Ethics and Data: Why Should We Care?

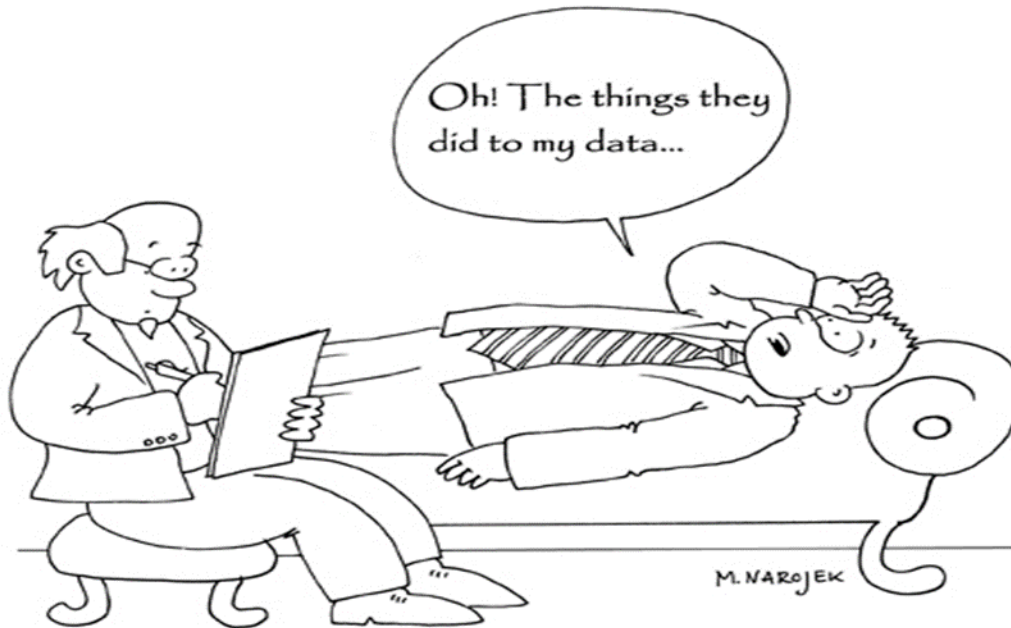


700,000

....270, 000

70 000

...87 000 000?



4 000 000

**7.5 million under 13 and more
than 5 million under 10**

Main Ethics Concerns



Free, voluntary and informed consent

Q Search 

Heads up! On May 1, 2018, we'll update our **Privacy Policy** and **Terms of Service** to make them clearer and to address some new privacy laws in Europe. Tap Accept to let us know you're okay with the updates.

Learn more

Accept

- *Big Data analytics;*
- *Use of data from wearables and social media platforms, collected by third parties;*
- *Use of data collected by commercial organisations for research purposes and vice versa;*

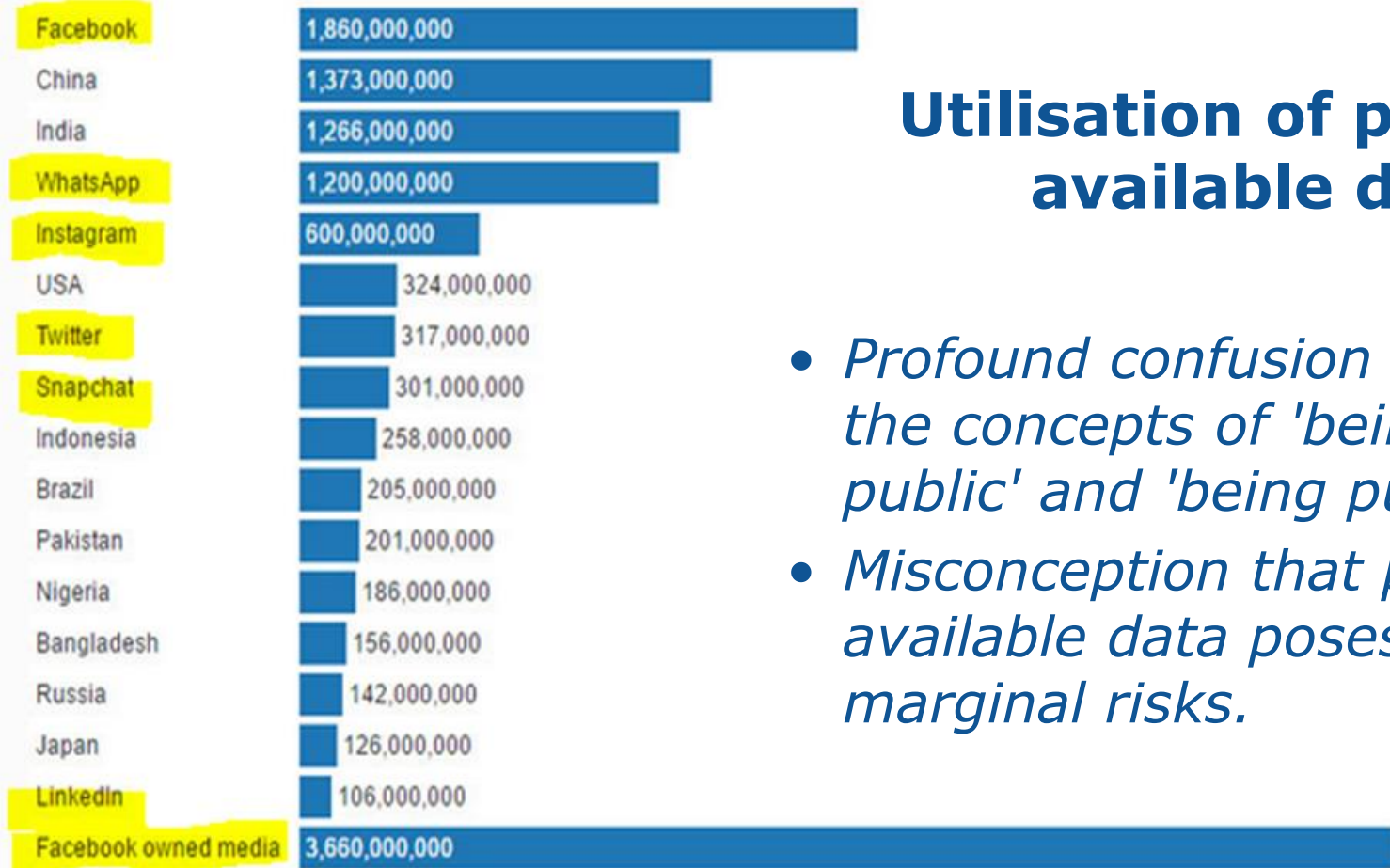


Welcome to the Oath Privacy Center

- Analyze your content and other information (including emails, instant messages, posts [photos](#), [attachments](#), and other [communications](#)). You can review and control certain types of information tied to your Oath account by using [Privacy Controls](#).

Main Ethics Concerns

If social networks were countries



Utilisation of publicly available data

- *Profound confusion between the concepts of 'being in public' and 'being public';*
- *Misconception that publicly available data poses only marginal risks.*

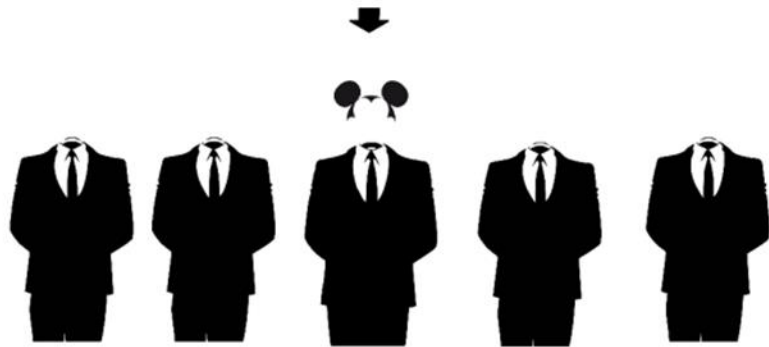
Source: Data from Statista (2016) and CIA World Factbook [Get the data](#)



Main Ethics Concerns

Online recruitment

- *Uncertainty as to the real age of the participants;*
- *Possible harm for the individuals;*



I can't identify you... But I can single you out!
Does the difference really matter?

Anonymisation, Pseudonymisation, Data Minimisation

- *Lack of clear understanding of the process and the difference between anonymisation and pseudonymisation;*
- *Excessive collection of data and unjustified storage periods.*

Technically, Moses

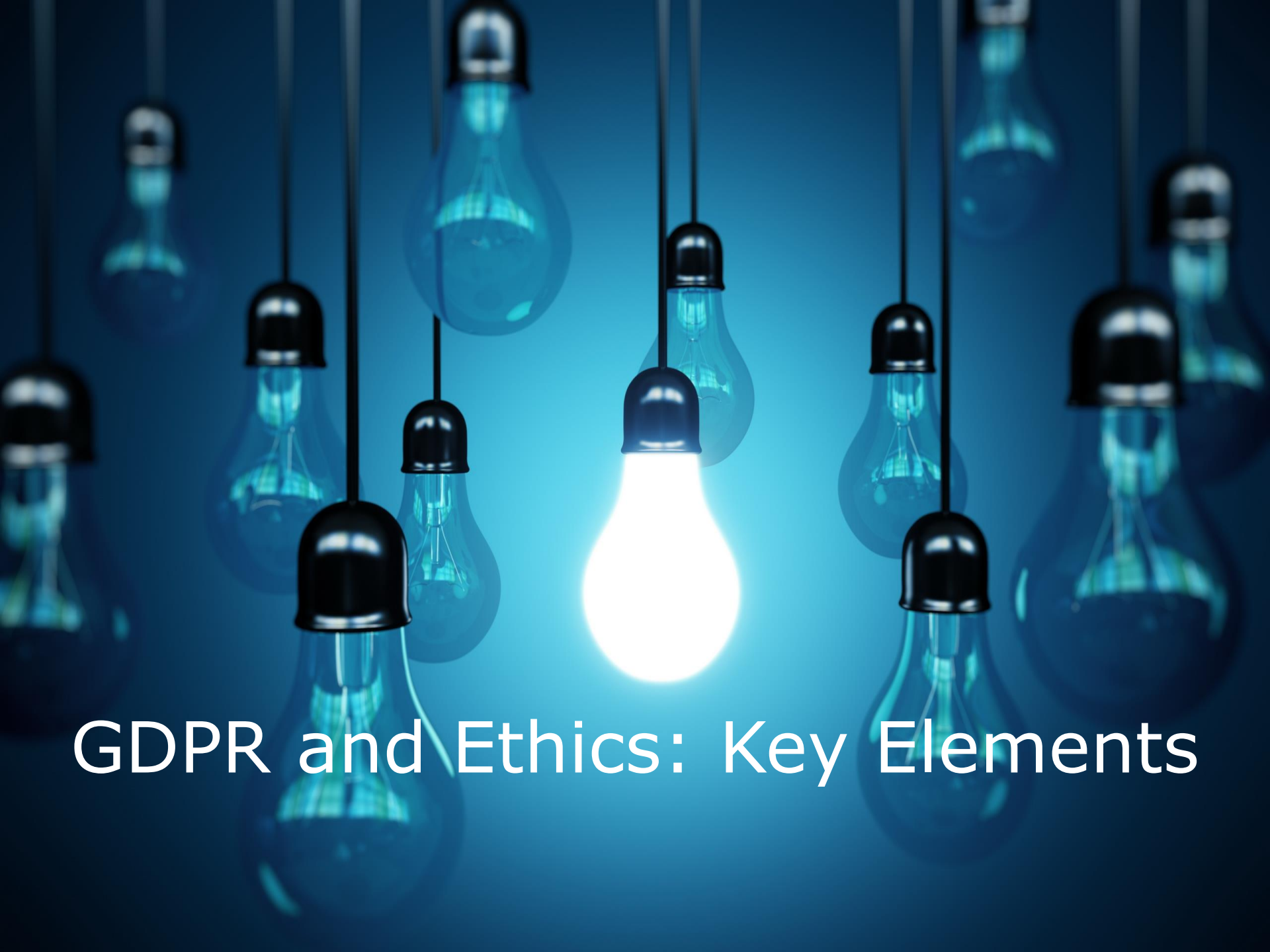


was the first person
with a tablet
downloading data
from the cloud

Main Ethics Concerns

Non-adequate Security Arrangements and Data Transfer Outside/To EU

- *Non-secure data processing arrangements;*
- *Use of non-adequate software and storage providers and changing terms of use;*
- *Restrictions for processing of data in third countries.*



GDPR and Ethics: Key Elements



EU Data Protection Reform: Main Principles

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

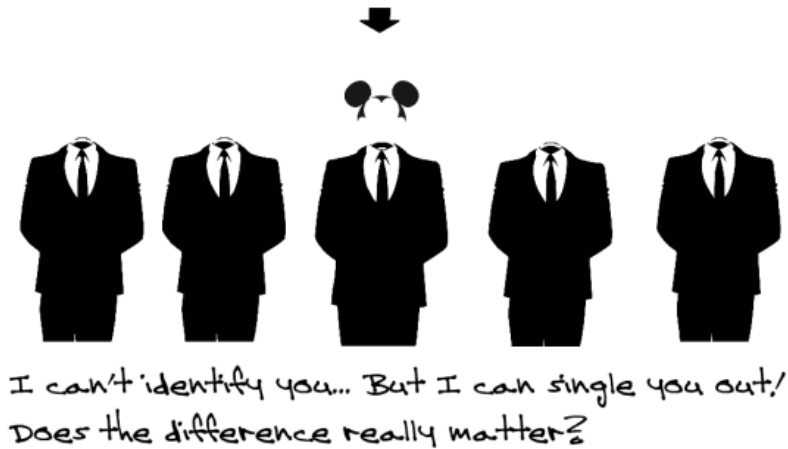
Personal data *is any information relating to an identified or identifiable (directly or indirectly) natural person.*



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.

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!**



Data Minimisation

Personal data should be **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed (*art.5.1c GDPR*)



Data Protection by Design and by Default:

...**by default**, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the **amount of personal data collected, the extent of their processing, the period of their storage and their accessibility**. In particular, such measures shall ensure that by **default personal data are not made accessible without the individual's intervention** to an indefinite number of natural persons (art.25).



Profiling

Any form of automated processing of personal data **evaluating the personal aspects** relating to a natural person, in particular to **analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements**, where it produces legal effects concerning him or her or similarly significantly affects him or her.

Further information: Article 29 WP 251/2017



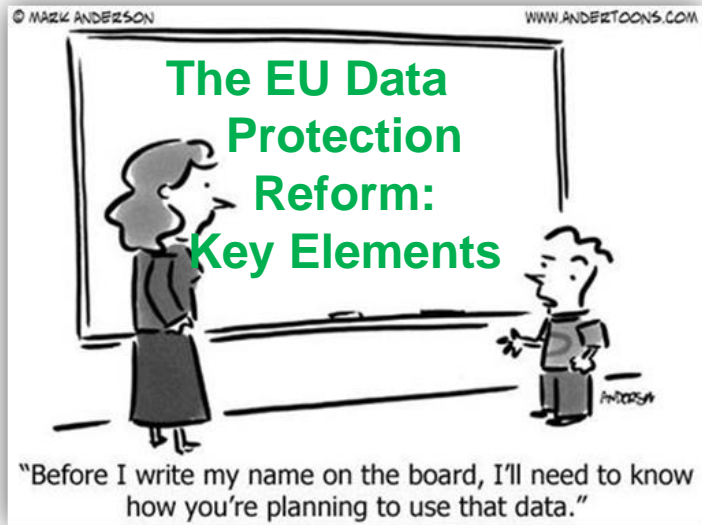
✚ ***Shift from compliance-based to accountability based approach (record keeping);***

✚ ***Mandatory appointment of Data Protection Officer*** (in certain cases).



Appointment of DPO in cases where:

- the processing is carried out by a public authority or body;
- the **core activities** of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring of data subjects on a large scale**;
- the core activities of the controller or the processor consist of **processing on a large scale of special categories of data**. (section IV GDPR)



⊕ ***Data Protection Impact Assessments (DPIA)***

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)



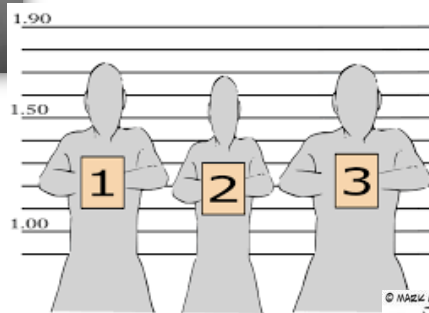
DPIA must be carried out in particular in cases of:

- A **systematic and extensive evaluation** of personal aspects relating to natural persons which is based on automated processing, **including profiling**, and **on which decisions are based that produce legal effects** concerning the natural person or similarly significantly affect the natural person;
- The processing on a **large scale of special categories of data**;
- A **systematic monitoring of a publicly accessible area on a large scale**.

More information: WP 248/2017 Article 29

GDPR and Research: Key principles

- ✓ 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**.



"Before I write my name on the board, I'll need to know how you're planning to use that data."



10 000 000

2%

20 000 000

4%

GDPR and Its Impact on the Ethics Review Process.



***New Data Protection Requirements for
H2020 projects***



The Ethics Appraisal Process

What the researchers should do:

"Start thinking (and discussing) about ethics while designing your research protocols. Do not wait until the last minute to seek advice or check what is required under national and European legislation."

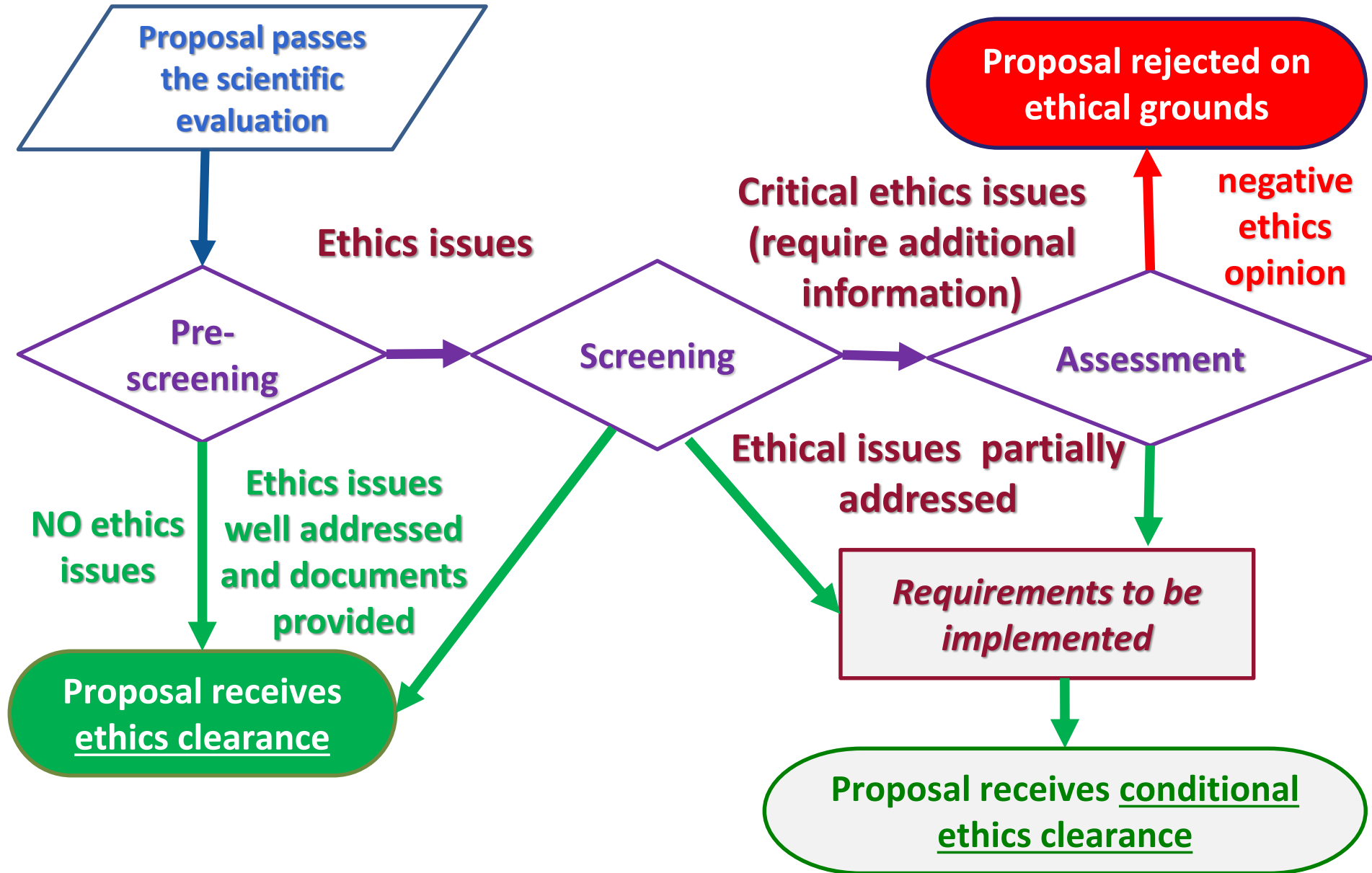


The Ethics Appraisal Process

What the researchers should do:

"Consider that ethics issues arise in many areas of research. Apart from the obvious, the medical field, research protocols in social sciences, ethnography, psychology, environmental studies, security research, etc. might involve the voluntary participation of research subjects and the collection of data that might be considered as personal. You must protect your volunteers and also protect yourself (and your researcher colleagues)."

Ethics Review



Ethics and Data Protection Requirements





The beneficiary may be requested to:

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;

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.



The beneficiary may be requested to:

- ✓ Describe the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants.

- Describe the anonymisation/pseudonymisation techniques that will be implemented

- Describe the security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing.

The beneficiary may be requested to:

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.





The beneficiary may be requested to:

- ✓ The requirements on informed consent remain the same;
- ✓ The requirement on justification of processing sensitive data remains the same;
- ✓ The requirements for further processing are to be changed.



Data Transfers

The beneficiary may be requested to:

For countries, not covered
by adequacy decision

In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the GDPR, must be submitted.

In case personal data are transferred from a non-EU country to the EU (or a third country), confirmation that such transfers comply with the laws of the country in which the data was collected must be submitted.



The beneficiary may be requested to:

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. The risk evaluation and the opinion must be submitted as a deliverable.



Ethics help desk:

RTD-ETHICS-REVIEW-HELPDESK@ec.europa.eu