PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

PANELFIT Project is funded by the EU Commission, H2020 SWAFS Programme, research grant number 788039

GDPR and its implication for research

IÑIGO DE MIGUEL BERIAIN
Ikerbasque Research Professor. Ikerbasque Bilbao
University of the Basque Country

Introduction

The General Data Protection Regulation (GDPR) was adopted on 14 April 2016 and became enforceable beginning 25 May 2018.

The GDPR is a regulation. Thus, it is directly binding and applicable.

However, it does provide flexibility for certain aspects of the regulation to be adjusted by individual member states (similar to a Directive in several key issues, such as the regulation of the processing of genetic data, biometric data or data concerning health

The GDPR is applicable to research concerning personal data (any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly)

This presentation follows an excellent paper by Rossana Ducato: Data protection, scientific research, and the role of information, Computer Law & Security Review, Volume 37, 2020, 105412,

Non-personal data

Non- personal data: Regulation on the free flow of non-personal data (FFD Regulation)

"Mixed dataset". Mixed datasets represent the majority of datasets used in the data economy and commonly gathered thanks to technological developments such as the Internet of Things (i.e. digitally connecting objects), artificial intelligence and technologies enabling big data analytics.

If both type of data are inextricably linked", the data protection rights and obligations stemming from the GDPR fully apply to the entire mixed dataset, including in cases where personal data represents only a small part of the dataset.

Some basic ideas

The GDPR establishes a framework particularly favorable for research.
The concept of research must be understood in a wide way.
Processing for research purposes can benefit from some exceptions to data protection principles and derogations to data subjects' rights (specially if we talk about public research).
However, this special regime comes with obligations. Data controllers, in particular, will have to set up appropriate measures and safeguards to protect the rights and freedoms of individuals.
How these safeguards look is not entirely clear in either the adaptations of the GDPR or at the national level.

Research: the legal basis

Different legal framework depending on whether we are processing special categories of data or not.

If NOT: The controller shall rely on one of the legal conditions listed in Article 6 GDPR.
If YES: Also requirements provided at Article 9(2) GDPR.

Article 6 offers three main roads:

(Article 6(1)(a) GDPR), the consent of the data subject

(Article 6(1)(e) GDPR), the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or

(Article 6(1)(f) GDPR), the legitimate interests of the controller or a third party

The special regime for research purposes: exceptions to principles and rights.

Exceptions to some data protection principles (Article 5(1)(b); Article 5(1)(e); Article 9(2)(j) GDPR),

Derogations to the exercising of a set of data subjects' rights (articles 14, 15, 16, 18, 21 GDPR).

Exceptions to the purpose limitation principle

Presumption of compatibility between (secondary) processing for research purposes and the original purpose of collection

No new legal basis for data processing is needed.

In some concrete types of data, this presumption might be limited by MS (biometric, genetic data…)

Storage limitation principle

The data processed for research purposes may be kept in a form which allows the identification of data subjects even beyond the period strictly necessary for the achievement of the purpose for which they were originally collected.

This exception is particularly relevant in the context of scientific research, since the storage is fundamental to allow the verification of research results (so, even after the research project has officially ended).

However, the EDPS has warned against the abuse of such provision: "the intention of the lawmaker appears to have been to dissuade *unlimited* storage even in this special regime, and guards against scientific research as a pretext for longer storage for other, private, purposes"

The special regime for research purposes: derogations to the exercising of a set of data subjects' rights

One needs to distinguish between derogations that are 1) laid down in the GDPR and 2) can be introduced by Union or Member States law.

Derogations in the GDPR:

Limitations to the right to be erasure
Limitations to the right to object

Limitations that can be introduced by Union or MS law: art. 89(2): Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21

GDPR: Derogations of rights

- Limitations are permitted insofar as they are necessary and proportionate in a democratic society.
- "Three-step-test" for research derogations, centred on necessity and proportionality. Elements that must be present (cumulative)
  - First, exercising the rights is likely to render impossible or seriously impair the achievement of scientific purposes.
  - Second, the derogations must be necessary for the fulfilment of those purposes.
  - Finally, appropriate safeguards for the rights and freedoms of the data subject must be adopted.

Limitations to the right to erasure

Right to erasure: The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay

It does not apply it the exercise of the right by the data subject would render impossible or impair achievement of research purposes

However, this limitation only applies when the research is finished or the data are necessary for its success. If they can be replaced, the right rules

Safeguards according article 89(1) must be implemented

Limitations to Right to object

Right to object. This can be invoked by the data subject for reasons connected to his or her particular situation **only when processing is based on the legitimate interest of the controller.**

It **cannot be exercised in the context of research when the processing is necessary for the performance of a task carried out for reasons of public interest.**

Therefore, before the superior interest of the public, the particular situation of an individual leading to an objection to processing can be limited by law.

Possible discrimination between public and private research?

Rights to data portability and ADM

Rights corresponding to articles 20 (data portability) and 22 (automated decision-making process) remain even in the scientific research domain However, data portability does not apply to inferred data. These are considered intellectual property of the researcher/developer.

Limitations to the right to be informed

Articles 13 and 14, mandates the provision of a series of information duties to the data controller, who has to inform the data subject about the relevant aspects of processing
However, the GDPR states that when the provision of information proves **impossible**, requires a **disproportionate** effort or risks seriously compromising the achievement of the research the data controller is relieved of the information obligations provided for in Article 14 (data non obtained from the data subject)
Balancing assessment.

First, “impossibility” and “disproportionate effort” must be confronted with “the number of data subjects, the age of the data and any appropriate safeguards”
Second, the EDPB has further stressed the need for the controller to evaluate “the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information”. This will consist at least of **making the information publicly available** (e.g. publication on website, newspapers, etc.)

What if the data was obtained from article 13?

GDPR makes no exceptions to the rigth to information included in article 13.
This means that the effort to inform from the beginning or to contact again later (in case of further processing for a different purpose) is presumed to be reasonable when the data controller has a direct relationship with the data subject. However, there might be cases where informing the data subject in a transparent way might compromise the achievement of the research. This issue is yet to be solved.

Safeguards

Article 89(1) of the GDPR states that safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization. These measures may include pseudonymization, but offer no further insight into what they may also be.

Candidates:

Data Protection Impact Assessment (often compulsory)
Intervention of ethics committees
Creation of specific agencies, such as Finndata
The Article 29 WP (now the European Data Protection Board) states that safeguards could include 'Information Security Management Systems (e.g., ISO/IEC standards) based on the analysis of information resources and underlying threats, measures for cryptographic protection during storage and transfer of sensitive data, requirements for authentication and authorization, physical and logical access to data, access logging and others'

PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

PANELFIT Project is funded by the EU Commission, H2020 SWAFS Programme, research grant number 788039

GDPR and its implication for research

IÑIGO DE MIGUEL BERIAIN
Ikerbasque Research Professor. Ikerbasque Bilbao
University of the Basque Country