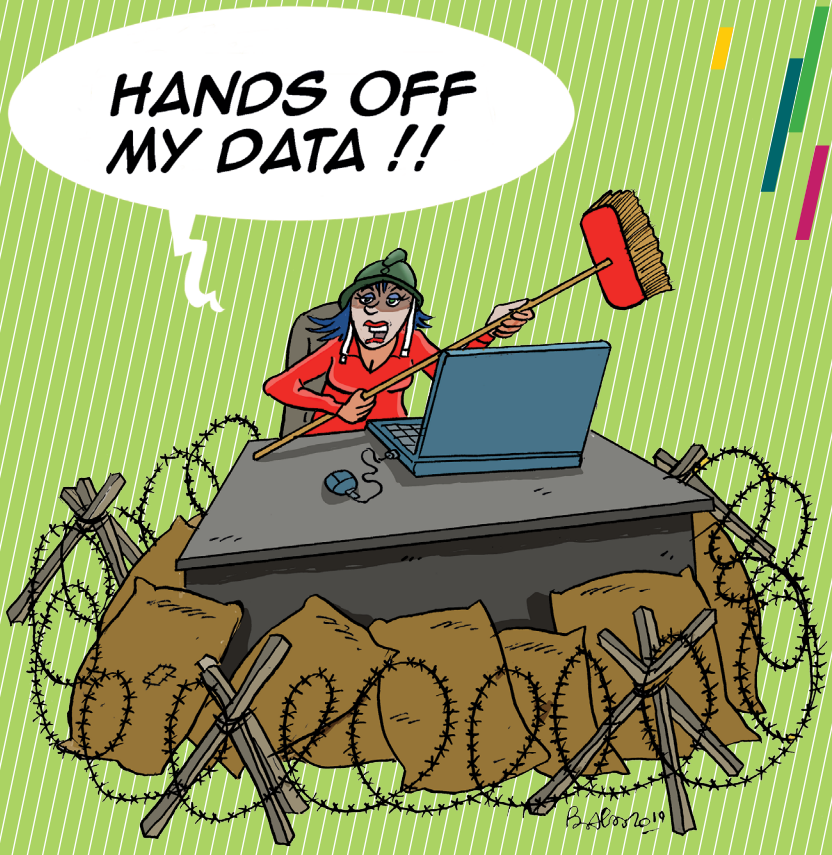
# Guide on the proper use of the General Data Protection Regulation (GDPR)




CRef
CONSEIL DES RECTEURS

fnrs
FREEDOM TO RESEARCH

# Table of contents

# EDITORIAL

As early as December of 1992, Belgium voted a privacy law whose purpose was to protect citizens from unlawful use of their personal data. In 1995, the European Parliament and the Council adopted a directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Since then, personal data have become increasingly valuable, eventually becoming the 21st century's black gold, while technological progress has created new opportunities to exploit these data. One can clearly see how much interest big tech companies (Google, Apple, Facebook, Amazon, Microsoft), to name just those, have in collecting and using personal data.

In response to these concerns, the General Data Protection Regulation (GDPR) was adopted, coming into effect on 25 May 2018.

This guide on the proper use of the GDPR presents an overview of this regulation in accessible and practical terms, based on the experience of its implementation in universities represented within the Conseil des Recteurs (CRef).

# What is it about ?

*The GDPR applies to all processing of personal data. What data ?*

## The data

*'Personal data'* means any information related to an individual who can be identified directly or indirectly. This is a broad definition, as it covers identifiers (e.g. name and surname) as well as any information related to a person who is identified (e.g. a student's exam marks) or a person whose identity is unknown but could reasonably be determined (e.g. CCTV images, voice recording, or coded data). In addition, a combination of non-identifying data can sometimes be used to identify a person, making amalgamated data into personal data.

## Sensitive data

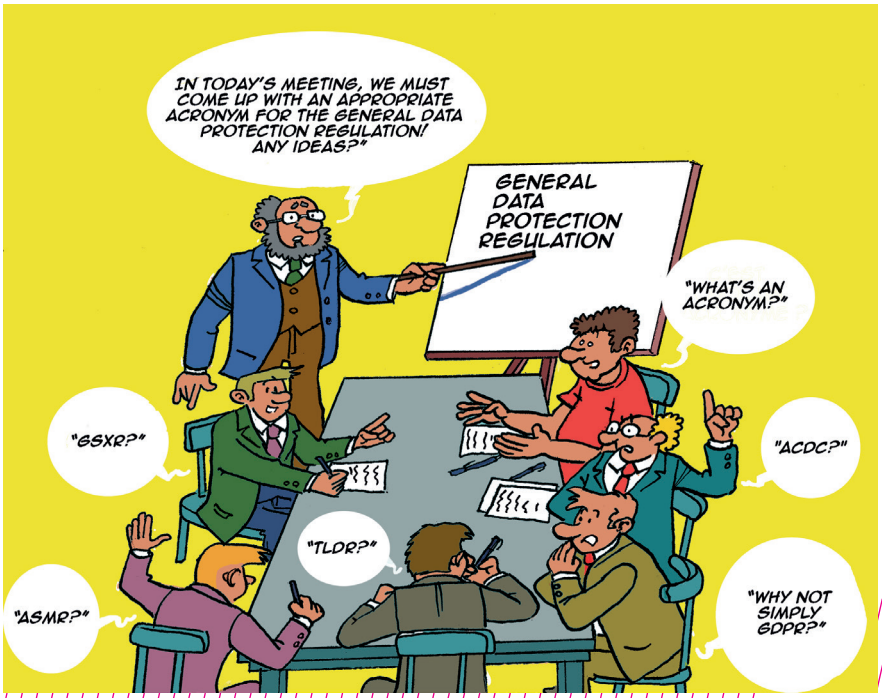
Certain data are called *'particular'* or *'sensitive'*. These are information about ethnic origin, sexual orientation, religious or philosophical beliefs, political opinions, trade union affiliation and physical or mental health, as well as genetic and biometric data when they are used to identify a person. The processing of these data is forbidden except in specific cases, which are subject to stricter rules.

## The processing

The use of these data—whether normal or sensitive—is called *'processing'*. This term is also very broad in scope, covering a series of processes, automated or otherwise, carried out on the data (from collection to destruction, including recording, modifying and use) for one or several established purposes.

## Data transfers

When data are sent to persons who are not part of the University, rules with varying degrees of strictness apply. In particular, the GDPR restricts the transfer of data outside of the European Union. Exceptions exist, but data must be kept inside the European Union to the largest extent possible.



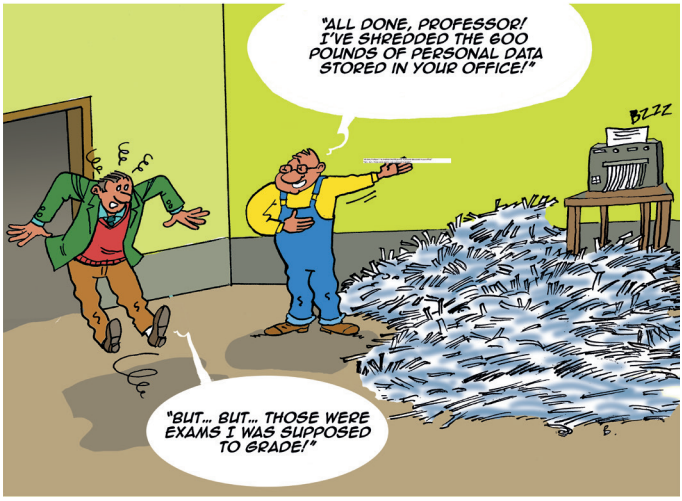
# Who does it apply to ?

*The GDPR involves multiple actors.*

## The controller

This is the natural or legal person who, alone or with others, determines the purposes of the data processing (the 'why') and the means used to carry it out (the 'how'). They are responsible for enforcing the rules defined in the GDPR, including by supervising their staff members.

Universities act as the controller of the data they process.




## The processor

This is a natural or legal person who processes personal data on behalf of the controller. Processors are typically technical service providers who carry out technical operations on data upon request from the controller (see p. 9).

## The data subjects and their rights

These are the natural persons whose personal data are processed.

As the GDPR's purpose is to give individuals more control over their personal data, they are granted a number of rights (see p. 10).

## The data protection officer (DPO)

One of the GDPR's major innovations was the establishment of a new role : the data protection officer, or DPO. In some cases, this role is mandatory within the organisation.Belgium's French-speaking universities have all designated a DPO.

The DPO plays an important part in implementing the GDPR. They act as an intermediary between the players involved : the supervisory authority, the members of the university community, and the data subjects. They may be consulted regarding questions or projects involving the processing of personal data (preferably as early as possible).

## The data protection Authority

Since 25 May 2018, the privacy protection Commission (*'Commission de protection de la vie privée'*) has been replaced by the data protection Authority (DPA), which is the supervisory authority that can verify on its own initiative the the correct application of the GDPR or receive complaints from data subjects regarding the processing of their data.

# How is it implemented ?

*Principles to follow when designing a processing activity.*

**The GDPR is based on six fundamental principles.**

**1.** Each processing activity must be built on one of the legal bases defined in the GDPR and conducted in a transparent manner in relation to the data subjects. At the University, the legal bases most often used are a legal or contractual obligation, the performance of a task carried out in the public interest, or the data subject's consent (which must be explicit).
**2.** The data may be processed only for one or several purposes that are specified and clearly communicated.
**3.** Only the data strictly necessary in relation to these purposes may be processed.
**4.** The data must be accurate and, where necessary, kept up to date.
**5.** The data must not be kept longer than strictly necessary for the purposes of the processing (see p. 9).
**6.** Data security must be ensured by using appropriate technical or organisational measures. Data security is threefold : confidentiality, integrity and availability (see pp. 14 and 15).

The University must, at any time, be able to demonstrate to the DPA and to the data subjects that these principles are respected, for instance by documenting the measures or decisions taken to ensure compliance.

## Length of data retention

Defining the storage period of data is a basic requirement for data protection. This period must not be longer than required by the purposes for which the data are processed.
The period is often prescribed by law.

## Contractual aspects

If the University calls upon an outside service provider (including a provider of software applications) to process personal data on its behalf and on its instructions, it must ensure that this provider—who will act as the data processor (see p. 6)—complies with the requirements set by the GDPR, in particular in relation to data security and confidentiality. The GDPR also requires the conclusion of a written contract, which must cover certain aspects of the processing carried out by the processor.

Similarly, if the University processes data for a third party (for instance in the context of a research project), this processing must also be covered by a contract.

A contract between *'joint controllers'* may also be necessary for collaborative research.

# What are the University's duties?

## Processing records and prior information

The University is required to keep records of all processing activities carried out under its responsibility. The DPA may request an access to these records at any time. The staff's collaboration is essential to the creation and maintenance of this tool that can also help identify issues that may arise.

In addition, the University must specify to the data subjects, among other things, who the data controller is, what the purposes and legal bases of the processing are, who can access the data, whether the data are transferred outside the EU, and the DPO's contact information. This must be done when the data is obtained, whether they are collected directly from the data subjects or by other means.

## Respecting the rights of data subjects

The right to information does not stop at a one-time notification. Data subjects may request, at any time, additional information on the processing and on the data used; they may request, among other things, their rectification or erasure (right to be forgotten), or they may object to their processing.

A procedure must therefore be put into place in order to enable the effective exercise of these rights and ensure a response to all requests within one month as provided in the GDPR.

# When should an impact assessment be conducted ?

## Risk management

Where the processing of personal data is likely to present a high risk to the rights of the data subjects, an in-depth risk analysis called an impact assessment must be conducted.

If, at the conclusion of this impact assessment, the risk is deemed to be severe, the controller may be required to consult the DPA.

This only concerns processing activities that may present a high risk to the rights and freedoms of the data subjects, such as:

- The right to privacy
- The right to free movement
- Freedom of speech and information
- Freedom of assembly and association
- Freedom of thought, conscience and religion
- The respect for medical privilege
- The prohibition on discrimination
- The right to integrity and dignity

The GDPR provides examples, including profiling, the processing on a large scale of sensitive data or the use of a new technology.

The DPA has published a list with more examples, such as the processing of biometric data for the purpose of identifying persons or the large-scale processing of data generated by devices equipped with sensors.

In practice, the DPO can help the controller determine whether an impact analysis is necessary and how to conduct it.

# Research

*The GDPR applies to the research sector. Research-related data processing activities must therefore be included in the processing records (see p. 10).*

*The drafters of the GDPR and the Belgian legislator have designed specific rules to reconcile privacy and freedom of research.*

These allow some flexibility with regard to the general rules in relation to research, including mainly:

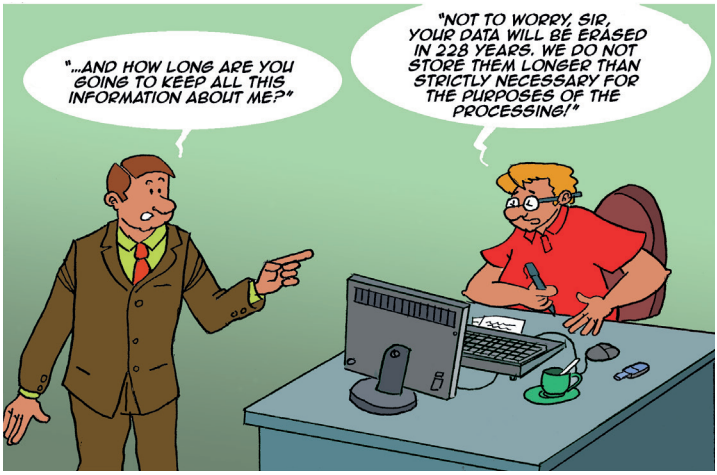
- the reuse ('further processing') of data is deemed to be compatible with the initial purpose of processing;
- the data may be stored for longer periods than the regular rules provide;
- the researcher may process sensitive data;
- the duty to respect the right to erasure and the right to be forgotten may be waived. Other requirements may be waived only by invoking Belgian law of 30 July 2018 on the protection of natural persons in relation to the processing of personal data.

Appropriate safeguards must, however, be implemented, such as:

- data minimisation (process only data that are strictly necessary);
- data anonymisation, if possible;
- data pseudonymisation (encoding);
- data encryption;
- the consultation of an ethics committee;
- the consent of the data subject to take part in the research project.

# How to conduct questionnaire-based surveys ?

Regarding surveys, the use of anonymisation techniques should be favoured, especially for questionnaire-based surveys. This is because if no personal data is processed, rules on the protection of personal data do not apply. However, care must be taken to ensure the data is truly anonymous, meaning that it must be impossible to establish a relationship between the answers to the questionnaire and the person who provided them.




If this cannot be done and personal data must be collected, then participants must be provided clear information on the purpose of the study as well as all information required by the principle of transparency. This information must be provided before the data is processed. The person responsible for the survey shall retain proof that this information was provided.

# How to guarantee data security ?

*The controller may use technical measures to ensure that personal data is processed in accordance with the GDPR.*

## Transferring and publishing information and data

The confidentiality of personal data must be ensured, which means—among other requirements—that they must not be transferred to anyone who does not need to access it.

## Workstations

The workstations used to process the data must be made secure using state-of-the-art technologies. They must run anti-virus software and be automatically kept up to date. Work sessions must be protected using a personal identifier and a password.

## A proper password

Access to personal data should only be possible after the user has entered their credentials, which is most often done using a personal login and password. The password must be sufficiently complex, and strictly personal.


"I'M TOO FORGETFUL, SO I JUST POSTED MY PASSWORD ON FACEBOOK AND NOW I ALWAYS HAVE IT HANDY!"
"REALLY? DID YOUR 2,759 FACEBOOK FRIENDS LIKE YOUR POST?"

# How to store data ?

## Data storage

Personal data must be stored securely. Use of an *'institutional'* storage platform offered by the University is recommended. This can be either local storage or an on-premises or external cloud platform.

The storage of personal data on local workstations and the use of free cloud solutions as well as removable media such as USB devices or external hard drives is discouraged, unless specific protection measures are taken such as dataencryption.

Personal data must also be saved on a secure backup storage platform.

The local premises where personal data is stored must be secured using locks or other forms of access control. This requirement also applies to cabinets in which paper documents or removable digital media are stored.

## Data end-of-life

When personal data reach the end of their storage period as defined in the processing records, they must be destroyed (see p. 9). Data stored on paper should be shredded.

# Incident management

## What is an incident ?

An incident related to personal data is any event that results from the loss, theft, destruction, accidental damage or unlawful change of said data, such as the theft of a computer, the hacking of an account or password or the loss of a USB drive. Unauthorised or illicit access also constitutes an incident.

## What to do in the event of an incident ?

Depending on their severity, such incidents must be reported to the DPA within 72 hours of being detected, either by the University as the data controller or, by way of delegation, by its DPO. In order for this requirement to be fulfilled, all members of the university community must develop the habit of immediately notifying any incident they spot, in accordance with the procedure in place within the University.

## Developing good habits

In practice, you should immediately report, following the procedures defined by your university :

- the loss or theft of digital equipment such as USB drives, laptop computers, mobile phones, etc. ;
- the abandonment in a public place of personal data in paper form : binders, folders, etc. ;
- the loss or theft of paper files containing personal data ;
- the breach of a password or login identifier, whether as a result of sharing, hacking, phishing, etc. ;
- any other incident involving personal data.

Should the University neglect its duties related to security incidents, it may face sanctions from the DPA.

# Conclusion

While the GDPR creates new obligations, it essentially reinforces existing legal requirements that were not always widely known.

The University's observance of the GDPR requires its staff to be involved, for instance by maintaining processing records, ensuring data security or report incidents related to personal data.

Your DPO is there to help you. If necessary, they may point you to technical specialists with expertise on data protection.

Lastly, the GDPR has made us realise the value of our personal data and the importance of having a strong legal framework for their protection.

We must not overlook such an important topic!

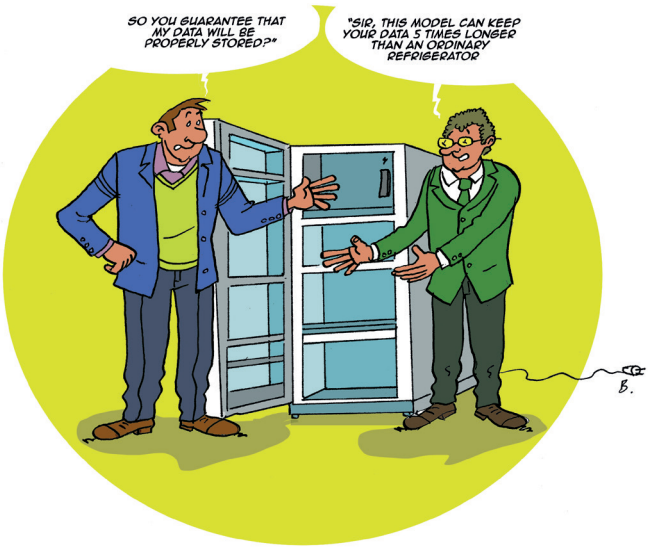
Thank you in advance for your collaboration.

# For more information...

➔ General Data Protection Regulation:
**https://www.dataprotectionauthority.be/european-union**

➔ Data protection authority:
**https://www.dataprotectionauthority.be/**

➔ European Data Protection Board:
**https://edpb.europa.eu/**




ULB – ULiège – UMONS – UCLouvain – UNamur – USL-B

Editor in change: Vincent Blondel, CRef, Rue d'Egmont, 5 - 1000 Brussels, May 2019 • Illustrations: Baloo • Graphic design: by-im.be