# GDPR crash course

In May 2018, the General Data Protection Regulation ([GDPR](https://cdh.uu.nl/glossary/gdpr/)), came in force in the European Economic Space.

The GDPR is the legal framework in the EU for the protection of personal data of natural persons (living individuals). Each member state has a national implementation of this framework. In the Netherlands this is called the *Algemene Verordening Gegevensbescherming* (AVG).

In many research projects personal data is processed.

The GDPR defines what is to be considered personal data and prescribes under what conditions these can be processed. It also requires you to describe how you manage these data, e.g. in a Data Management Plan and/or DPIA and prescribes you to do so before you start your research and at all times be able to show this documentation and, most important, act accordingly.

The essence of this law is to give persons full control over their own digital data. Any researcher using the data which can (in)directly be traced to a living natural person must have a legal ground to do so and warrant this person a number of unalienable rights and protections.

It is the responsibility of the researcher, supported by his employer, to organize this compliancy and to be able to show in a documented fashion at any time starting from the moment of processing, how these rights and protections are guaranteed.

Non-compliancy to the GDPR means that the processing of these data is ‘illegal’. This could result in liability for the researcher (or his employer) to a fine.

Please be aware of the following:

* The rights are unalienable. Whether personal data are found in the public domain or handed over knowingly and willingly, does not change the rights of the data subjects. Being a public figure or signing an Informed Consent Form with specific conditions cannot take away these rights. Also living persons can change their minds during the period that their data is being processed.
* The GDPR distinguishes between personal data, (as defined in art. 4) and special categories of personal data, (as defined in art. 9.)
* Data subjects located outside the EU have the same rights as those located within the EU.
* If you are processing personal data, this processing should in principle take place within the European Economic Space.
* If you or your institute does not control the processing, e.g. because you use a cloud service, you must have an explicit agreement with the controlling party on how GDPR compliancy is warranted. This is done through a [Data Processing – or a Data Transfer Agreement](https://cdh.uu.nl/glossary/data-processing-or-data-transfer-agreement/).
* The personal data you process involve more than the data you analyze for research purposes. You might need to manage Informed Consent Forms or mail addresses of participants. These are your responsibility as well, even though irrelevant from a scholarly point of view.
* Clearance of research by an Institutional Ethical Committee is not the same as being GDPR compliant. The former has solely to do with research integrity and ethics, the latter also with legal compliancy.

The GDPR in short:

* Data processing is both a noun and a verb; compliancy to the GDPR means both having the right documents (ticking boxes of necessary documents) as well as constantly being aware that you deal with personal data and act accordingly.
* Is about personal data of living persons. In general processing of personal data of deceased is [allowed](https://gdpr-info.eu/recitals/no-27/) but there start to emerge differences over this depending on member states. Also in the Netherlands a discussion is relation to this subject
* It is about data which can be (in)directly traced to a person. However, given modern technologies, guaranteeing that data is truly anonymized is hard. [Anonymized data](https://cdh.uu.nl/glossary/anonymized-data/) is not subject to the GDPR.
* There are exceptions for research: a) where special categories of personal data are involved; whereas these are not allowed to be processed, they can be for scholarly reasons and b) once data has been analyzed and has been published about, the right to withdraw or be forgotten, means in practice: no longer being used for future analysis.
* Distinguishes between personal data and special categories of personal data; in case of the latter a Data Protection Impact Assessment might be needed.
* The GDPR requires you to explicitly document (security by design) at least the following points before you start processing the personal data:
  + On what legal grounds you base your processing of personal data. It offers 5 possible categories, of which Informed Consent will probably be the most relevant for you.
  + what specific personal data, e.g. *name*, *age* and *gender*, you will be processing and how this processing occurs. E.g. *during research names and* *age of individuals will be stored in an excel, one row per person on institutional server A to which only researcher X has access. After research, the data rows will be aggregated in age clusters of five years, allowing for the removal of names and ages, thus anonymizing the data, and allowing it to be stored in an institutional repository as an Open Access data package.*
  + What to do in case your data processing is compromised, e.g. in case of a data breach.
  + How you warrant the rights of the data subjects, i.e. a) the right to information about how and for how long their data will be processed, b) right to access their data (note, that does not need to be ‘directly’), c) to rectify and d) withdraw their consent as well as e) their data (note the exception under the third bullet). There are three more rights, sc. to object, to object to automated processing and to transport, but these are of less relevance in a research setting.
  + To register your data processing a [Processing Registry](https://cdh.uu.nl/glossary/processing-registry/) (Verwerkingsregister), which your institute will have in place.

You do so by writing it down in a document, e.g. your data management plan, or, when the data is such that you need one, the Data Protection Impact Assessment document. Some of the issues need to be communicated to the participants. How is up to you, but a normal way to do so is in an Information Form you draw up and hand out to each participant.