GDPR: definitions

Data controller and data processor

Most obligations under the GDPR fall on the data controller, who determines the purposes and means of the processing of personal data. The controller can act alone or jointly with others.

The GDPR also imposes specific and separate duties and obligations on data processors. A processor is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller" .

Personal data and data subjects

The GDPR defines personal data as "any information relating to a data subject". A data subject is the identified or identifiable person to whom the personal data relates.

Identifiability

A person is identifiable if he or she can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Types of personal data

Personal data includes:

- Personal details.
- Family and lifestyle details.
- Education and training.
- Medical details.
- Employment details.
- Financial details.
- Contractual details (for example, goods and services provided to a data subject).

And should relate specifically to an individual.

Online identifiers

The GDPR addresses the question of online identifiers by specifically including online identifiers in the definition of "personal data" and this includes a wide range of online identifiers, including IP addresses, cookie identifiers and other identifiers like RFID tags.

Processing of data

The GDPR applies to the processing of data is very broadly defined as carrying out "any operation or set of operations" on the data, including:

- Collection.
- Recording.

- Organisation.
- Structuring.
- Storage.
- Adaptation or alteration.
- Retrieval.
- Consultation.
- Use.
- Disclosure by transmission.
- Dissemination or otherwise making available.
- Alignment or combination.
- Restriction (that is, the marking of stored data with the aim of limiting its processing in the future).
- Erasure.
- Destruction.

In effect, any activity involving personal data falls within the scope of the GDPR.

Data protection principles

The GDPR sets out a number of principles with which data controllers and processors must comply when processing personal data. These principles form the core of the obligations of each data controller and will usually form the basis of any claim that a data controller has not complied with its statutory duties.

- **Lawfulness, fairness and transparency.** Personal data must be processed lawfully, fairly and in a transparent manner. For example make sure you understand the legal basis on which you can process (*see lawfulness of processing below*) the information, make sure you are open with Dojos about how you will process their information and what you will use it for.
- **Purpose limitation.** Personal data must be collected only for specified, explicit and legitimate purposes. Make sure you clearly say why you are collecting the data what the purpose is when you are communicating with your Dojos.
- **Data minimisation.** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Make sure you are only collecting the data that you need to contact Dojos about the CoderDojo you are running and for the benefit of your Dojo. For example, there may be good reasons to ask the age of participants or to as if they identify as female in making sure our Dojos are as good as they can be.
- **Accuracy.** Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data that you process is accurate and is then erased or rectified without delay.
- **Storage limitation.** Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed. You also need to make sure you have appropriate data security measures designed to safeguard the rights and freedoms of data subjects. Make sure that you securely delete information about Dojos who no longer come to your club or where you have not heard from the for some time.
- **Integrity and confidentiality.** Personal data must be processed in a manner that ensures its appropriate security this includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Both data controllers and data processors must use appropriate technical or organisational security measures.

- **Accountability.** If you are a data controller then you are responsible for, and must be able to demonstrate, compliance with the other data protection principles.

Transparency

Specific transparency requirements include the data subjects' right to receive information on the identity of the data controller and the nature of the processing; about whether or not their personal data is being processed and if so the nature and purposes of that processing and about any personal data breach when that breach is likely to result in a high risk to their rights and freedoms.

Fair and lawful processing information

Certain information must be provided to ensure that the transparency requirement is met with regard to the fair and lawful processing principle. The information that must be supplied depends on whether the data controller collects the data directly from the data subject or obtains the data from a third party:

Data collected from the data subject

If the personal data is collected directly from the data subject and you are the data controller you must provide the data subject with the following information:

- The identity and contact details of the data controller and its representative, if any.
- The contact details of the data protection officer where you have one.
- The intended purposes of, and the legal basis for, the processing.
- Where the processing is based on legitimate interest, the specific legitimate interest pursued by the data controller or by a third party.
- The recipients or categories of recipients of personal data, if any.
- Where applicable, the fact that the controller intends to transfer the personal data to a recipient in a country outside the EEA.

It is important that this information is provided at the time the personal data is collected either through a privacy policy, a consent form or just and information form.

At the same time the controller must also provide the data subject with the following information to ensure fair and transparent processing:

- The period for which the data is stored.
- The existence of the data subject's:
    - right of access;
    - right to rectification;
    - right to erasure;
    - restriction of processing;
    - right to object to processing; and
    - right to data portability.
- If you are relying on the consent of the data subject, the right to withdraw that consent at any time.
- The right to lodge a complaint with the supervisory authority.
- The existence of any automated decision-making or profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Lawfulness of processing

If you are a data controller you must only process personal data on the basis of one or more of the following legal grounds. We have highlighted the two that are most likely to apply to you as a CoderDojo volunteer where you are a data processor:

- **The data subject has given their express and clear consent.**
- It is necessary for entering or performing a contract with the data subject.
- It is necessary for compliance with a legal obligation to which the data controller is subject.
- It is necessary to protect the vital interests of the data subject like natural or man made disasters.
- It is in the public interest.
- **It is necessary for the purposes of legitimate interests pursued by the data controller or by a third party, except where these interests are overridden by the interests or the fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child. When determining whether the data subject's interests or fundamental rights and freedoms override the data controller's legitimate interest, the data subject's reasonable expectations based on the relationship with the controller must be taken into account. The interests and fundamental rights of the data subject could, in particular, override the interest of the data controller where personal data is processed in circumstances where data subjects do not reasonably expect further processing. Further, in relation to using legitimate interests for children, this involves a judgement as to the nature and purpose of the processing and the potential risks it poses to children. It also requires data controllers to take appropriate measures to safeguard against those risks.**
- Where it is strictly necessary for the purposes of preventing fraud and for direct marketing purposes is deemed to constitute a legitimate interest of the data controller concerned.