Key privacy-related definitions and terminology

What is personal data?

Personal data is any information that directly or indirectly may lead to identification of an individual.

Typically, the most common type of personal data used by YOs are:

- Name
- ID numbers
- Address
- Bank account number
- Emails and phone numbers
- Level of education, etc.

However, YOs may collect and further use much more personal data. For example, you probably take photos at the events you organize. A photo may also be considered as personal data if its quality enables identification of a person.

It applies to one's IP address also, if it may help someone to identify that person.

If you provide legal support to young people, any information that relates to that individual (for example, medical data, criminal record, sexual orientation, etc) is also considered as personal data.

So, consider the definition of personal data as broad as possible.

Data processing

Data processing is basically any activity you undertake which involves personal data. So, it typically refers to collection, use, disclosure, multiplication, etc.

A common mistake is that this term applies only to physical handling of personal data. No. Even storing a file comprising of a list of participants at a meeting means that you process personal data. As with the definition of personal data, consider applying definition of data processing as generous as possible. Anything you do with personal data means that you should apply data protection rules.

Should all personal data be protected in the same way?

Generally, speaking, all personal data should be protected to avoid misuse of unlawful use. We protect data to protect people the data relate(s) to.

Some data are used more frequently. It may mean that they are accessible to more people, which may increase risks for any misuse. However, let us consider damage that may occur if certain categories of data are compromised.

For example, your mobile phone number is probably available to more people than your bank account number or your medical record. However, damage that may result from your medical record being stolen, or your bank account number being compromised, may be higher than if someone shares your mobile phone number without your approval.

There are some categories of personal data that are particularly important to protect. The types of personal data that are considered as **special categories of personal data** per the General Data Protection Regulation (GDPR) are the ones revealing:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data,
- data concerning health of individual's sex life or sexual orientation.

If such data are compromised, significant damage may occur. Therefore, higher standards should be applied both in terms of conditions for the use of such data and for their protection.

When designing data protection measures, YOs should prioritize:

- Processes involving special categories of personal data,
- Processes with higher risk of misuse (accidental or deliberate),
- Personal data that – if compromised - may lead to discrimination of an individual or any other serious consequence.

Data controller

Data controller is.... your organization if it collects and further uses personal data. This is the term that fits you role, per data protection rules you need to apply.

However, there is another term that describes those that use personal data – data processor. It is usually a company that you contract to perform some services for you that involve use of personal data. Typically, data processor is:

- Your Cloud provider,
- A company that you contract to refund travel costs of participants at your events,
- An HR company you hire when recruiting staff members, etc.

Data processor is forbidden to use the data for any other purpose. In case you do have such arrangements with data processors, bear in mind that you are responsible for any misuse of data. To prevent that, make sure that you instruct each data processor what types of activities it needs to perform.

Data subject

Data subject is a person whose personal data you process. In this guide we will sometimes use some other terms and refer to that person simply as *person*, *individual*, *citizen*, etc. Data subject is a natural person; therefore, data protection rules do not apply to legal entities.

Typically, YOs hold information about the following types of data subjects:

- Participants at events,
- Staff members (regardless of the type of engagement per labour law regulations),
- External experts and consultants,
- Volunteers,
- Individuals to whom you provide various support (for example, legal aid, or psychological support),

Consent

For every data processing practice there should be a legal ground. Otherwise, your practices are unlawful and you are at risk of being fined.

Consent is one of such legal basis. Consent is basically a permission you obtain from the data subject, to start using its personal data. Consent needs to be:

- **Freely given**. Data subject has to have options, including to say no. Do not make taking photos mandatory at your events – your participants may oppose and they have a right not to consent to that. It should not affect their attendance at the event.
- **Informed**. All pertinent information should be provided before you start collecting personal data. Including: who are you, what do you intend to do with the data you collect, etc. Avoid complicated legal terminology and use clear and plain language.
- **Specific**. There should be no general consent for any activity you may want to undertake by using personal data. Let's assume you collect contact data of conference participants with the purpose to organize the event (to avoid delays, inform participants about change of venues, etc). Their consent relates to that activity only. If you want to further send them offers for your services, you should obtain consent for that as well, because that's not why they had registered for.
- **Unambiguous**. Avoid opt-out approach. "Silence, pre-ticked boxes or inactivity" are not allowed – says the GDPR! You may obtain consent through a statement, or an activity that clearly demonstrates that the data subject has provided consent.