General Data Protection Regulation (GDPR) in brief

When does the GDPR apply?

Well, this depends on where your YO is registered and operational, and what kind of activities it conducts.

- If your organization is registered in the European Union,

Then the GDPR applies to your YO.

Any data processing activity that you undertake falls in the scope of the GDPR and you need to comply with the GDPR anytime you collect and further use personal data. It doesn't matter if you collect data of EU citizens, residents, or residents of non-EU countries. What matters is the fact that you operate in the EU.

- If your organization is registered outside of the EU,

Then the GDPR may apply to your YO in some cases.

If your organization offers goods or services to residents of the European Union, irrespective of whether a payment is required, then the answer is YES. That typically applies to tourist agencies of airline companies. But you should check if you provide any service or goods to EU residents before you conclude that you have no GDPR responsibilities. For example, if you offer and facilitate exchange opportunities to students residing in the EU, you would need to apply GDPR rules in such operations.

You should also comply with the GDPR if you conduct monitoring of behaviour of residents of the EU, provided that their behaviour takes place within the European Union. This applies typically to internet giants, social networks and other online services. It does not apply to you if you just use social networks for targeted marketing, for example. So, your organization probably does not fall under this category. Nevertheless, you should have this requirement in mind and consider it within your process of making your organization digitally safer.

Also, bear in mind that even if you do conduct any of such data processing practices, the GDPR applies to your organization only within the boundaries of such data processing practices. So, as an organization registered outside of the EU, you may be required to comply with the GDPR when offering some services to residents of the EU. But on the other hand, your data processing activities in terms of labour relations or organization of conferences remain within the scope of your national data protection legal framework only.

Penalties under the GDPR

Penalties under the GDPR may be huge. They could significantly endanger business operation of a data controller that fails to use citizens' data adequately. So far, the highest penalty issued under the GDPR is 50 million Euros (against Google).

However, even non-monetary penalties may significantly shake up data controllers. Their reputation may be destroyed even if there is just a gossip on inadequate handling of users' data. For YOs that is an additional argument for improving their data processing activities – your beneficiaries have trust that you would use the data adequately. Don't spoil that trust.

GDPR Principles

The GDPR sets a list of data processing principles. If you apply these principles, your data processing practices will be much safer. Let us briefly explore them.

- **Lawfulness, fairness and transparency.** Make sure that you always have a legal ground to process personal data, which you should define case-by-case. Do not use personal data you obtain against best interests of the data subject. Whatever you do with personal data – keep data subjects timely informed about your practices.
- **Purpose limitation**. Make sure you use personal data within the boundaries of the purpose you want to achieve. For example, if you have obtained CVs from individuals responding to your job vacancy (including contact details), do not spam them with invitations for your seminars. They wanted to interact with you because they needed a job. Data collected for purpose A should not be used for purpose B.
- **Data minimization**. Collect the amount of data that fits the purpose of data collection. For example, if you are organizing a conference, you probably do not need information on participants' blood type.

- **Accuracy**. Make sure that personal data you store are not incorrect or misleading. Don't be afraid – that doesn't mean you need to check if participants at your prior events have changed their last names due to a new marital status. This is not a purpose of this principle. Rather than that, it aims to prevent unwanted consequences for data subjects resulting from decisions or acts based on incorrect or misleading information about them.
- **Storage Limitation**. Sometimes there are explicit rules for how long you should keep the data. Adhere to such rules. When such rules are not put in place, make sure you store data no longer than necessary. For example, you probably don't need job candidates' CVs for an unlimited or unspecified period of time.
- **Integrity and confidentiality (security)**. YOs should ensure security of personal data, by creating a work process that prevents unauthorized or unlawful access and use of personal data. A necessary prerequisite for this is to understand your data infrastructure, which we will address in the following chapter of the Guide.
- **Accountability**. This principle combines the previous ones and adds a new value – **you** are responsible for the state of implementation of data protection rules in your organization. This is not a one-time-task, but a never ending, evolving process. Develop, implement, evaluate and review your data protection internal mechanisms. Act proactively. Be ready to bear consequences in cases of incidents.

Data subject's rights

Data subjects have a variety of rights per the GPDPR. You may have heard about some of the rights, including the right to:

- Withdrawal of consent,
- Be informed about data processing practices,
- Rectification,
- Data portability,
- Be forgotten, etc.

However, we will not further elaborate these rights, as the purpose of the Guide is to support YOs to improve their practices of collection and further use of personal data and to make their operation safer. For advises on how to address legal requirements arising from specific GDPR provisions establishing data subjects' rights, assuming such provisions are applicable for operations of your YO, we advise you to further explore relevant legislation and seek for available compliance support.

In the following chapter, we will help you to map your data infrastructure. This should further enable you to:

a) recognise weaknesses and blind spots inside your existing data processing practices, and
b) develop and implement measures to improve safety of your operations.