

What to Expect from the New Data Protection Legal Framework?

The new General Data Protection Regulation (GDPR) will enter into force for all EU Member states by 25 May 2018. GDPR provides for a considerably changed legal rules for processing of personal data. This should be taken into account by the business as soon as possible in order to opt for the necessary steps and the companies to be prepared for compliance with the new requirements.

The full text of GDPR is [here](#).

Material Changes

Although at first glance it seems GDPR follows a similar approach of regulation with that of the hitherto existing legal framework, it still provides several significant changes:

1. Severe Sanctions

GDPR increases the sanctions that can be imposed for non-compliance with the rules on protection of personal data. Sanctions for more serious offenses (eg, non-compliance with data transfer obligations to countries outside the EU; violating the general principles of data protection, etc) can reach up to EUR 20 mln or **4% of the total annual worldwide turnover of the data controller** (the higher of the two amounts). Accordingly, a sanction of EUR 10 mln or 2% of the total annual worldwide turnover of the data controller (the higher of the two amounts) is provided for minor infringements of GDPR. (See Art. 83 GDPR).

2. Broadened Scope

The whole business of the data controller must comply with GDPR. This applies also to any **businesses located outside the EU** (eg, when goods and/or services are provided to individuals within the EU or when organisations monitor the behaviour of the inhabitants of the EU).

3. Compliance Requirements. Data Processing Registers

GDPR obliges the data controllers and processors to demonstrate in a sufficient manner how the processing, storage and/or data transfer is carried out in compliance with the principles of data protection. This includes the maintenance of **data processing registers**. In addition, **complex measures and internal policies** for data management must be put in motion (if not yet introduced), to reduce the risk of unlawful processing of personal data. The measures include assessment of the impact on the protection of personal data processing with a high degree of risk and guarantees that data protection is carefully planned and organised and is not a secondary priority of the respective organisation (See Art. 32 et seq. GDPR).

4. Additional Rights

The rights of persons providing their data are expanded. GDPR regulates the **right «to be forgotten»** - one person may request deletion of its data under particular circumstances. The right to **limit the processing of data** in certain cases is also regulated, together with another novelty - the right the personal data of the individuals to be provided in a way that allows them **to be easily transferable**.

5. Consent Evidences

Where data processing is based on the consent of the physical person which data is subject to processing, the data controller will have **to be able to prove** that such consent was actually given by the person, the latter having the opportunity **to withdraw consent as easy as given**. Therefore it is required the already provided under the old regulation consents to be reviewed for compatibility with the new requirements of GDPR. If considered too burdensome, another option for the organisations is to go directly to an alternative legal basis for data processing - existence of contract between the respective person and the data controller and/or the existence of a legitimate interest of the data controller.

6. Data processors and DPOs

At present, data processors have no direct obligations (except those given by the data controller) and the data controller is the one responsible for any infringements committed by the processor/s. GDPR imposes **specific obligations on the processor**, including the application of appropriate security standards, ensuring adequate data backup and informing the controller for violations. For this reason, data processors will be now **direct object of sanctions** in case of violation of GDPR. GDPR also provides a number of provisions that should be included in all contracts related to the processing of personal data. This **increases the regulatory burden and risk to the data processors**.

In some circumstances, the data controller or the data processor will determine a **data protection officer (DPO)**. This will apply primarily when processing includes regular and systematic monitoring of data on a large scale or the data processing is associated with the public sector. The DPO should have enough competence to perform its functions. A DPO could be determined for a group of enterprises too.

The 7 P's Rule

If you have not met the new rules yet and have not started preparing for the compliance of your business with GDPR, we strongly advise you to make your own assessment of the interaction of your business with personal data and how GDPR will affect its functioning, and the functioning of the particular sector in which your business operates. Given the level of changes, the required measures and the strict sanctioning regime, the deadline up to May 2018 may prove to be extremely insufficient for some organisations. Do not hesitate to seek expert advice on the new data protection legislation thus to follow the rule of the 7 P's -

Prior Proper Planning Prevents Painfully Poor Performance!