

GDPR begins to apply on 25 May 2018 (1/20/18)

Enforcement of the General Data Protection Regulation (GDPR)¹ is starting in nine days, and that's exactly how many days are left before each company that processes personal data must implement any necessary changes to be able to perform such processing according to GDPR requirements and avoid penalties for non-compliance. As you may know, all EU regulations are directly applicable, meaning a member state is not required to pass their provisions into its national law. This article offers an overall stress test to help you assess whether your company is ready to comply with GDPR requirements.

Again – what is personal data and personal data processing?

Personal data is any information that relates to an identified or identifiable individual (including a customer or a customer's representative, beneficial owner or guarantor).

Personal data processing is any activity that involves personal data, such as gathering, registering, organising, structuring, storing, accessing, altering, deleting, disclosing, transferring, and restricting.

How to achieve GDPR compliance?

You should carefully examine the circumstances of personal data processing done within your company and preferably prepare documents detailing the following aspects:

- Personal data held by your company and the purposes for personal data processing in your company;
- Locations where the personal data held by your company is processed (stored) (in paper form and on information systems);
- Recipients of personal data within and outside your company (data flows);
- Legal grounds for data processing, such as legitimate interests, statutory requirements, and the data subject's consent to data processing, explaining how such consent is requested, obtained, and documented. The data subject should give their consent freely. In certain cases you should explain to the data subject that your company will be unable to provide a particular service without receiving such consent and it is the data subject's choice;
- Time limits for storing personal data and procedures for deleting/destroying personal data when a time limit expires;
- The data subject's rights (to access, delete, adjust their data etc), how those rights will be secured and how relevant information will be provided to the data subject;
- Protecting the confidentiality and safety of personal data (whether access is monitored, what technical means are used in personal data processing etc);
- Whether your company has all the necessary equipment for detecting, investigating, preventing and reporting personal data protection breaches;
- Procedures for reporting breaches to the National Data Office and in certain cases also to the data subject whose data is affected by a breach;
- Assessing the need to appoint a data protection officer;
- Evaluating your data processor's compliance, and amending your agreement with them if necessary.

This analysis is designed to help your company prepare a register of personal data processing activities, which the GDPR requires your company to maintain in certain cases and submit to the regulator's

inspection on request.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)