Deloitte.
Legal

Natalia Aleksejeva

Attorney (LL.M Eur)
Law Firm Deloitte Legal

Tel: +372 5171890
naleksejeva@deloittece.com

Are you ready for the new General Data Protection Regulation?

The new EU General Data Protection Regulation (GDPR) is coming into effect next year in May, bringing along a number of new obligations for data processors. It is important to bear in mind that GDPR affects absolutely every company, which is dealing with processing of personal data in its every day business – be it the clients' data or even the data of its own employees. It is also crucial to note that GDPR does not merely concern the companies established in the EU, but also those that process data in the EU – for example, offer their products or services on the EU market.

GDPR brings along the following changes:

1. **Stricter consent requirements** - the person's consent for processing of his or her personal data is valid only if it has been given in a voluntary, specific, conscious and unequivocal way, in a form of a statement, confirmation or other consent-expressing deed.
2. **Right to the erasure of data („the right to be forgotten") –** the new Regulation gives person a clear basis to request the data processors to erase all the data concerning said person that they have collected.
3. **Special rules with regard to personal data of minors –** if a person is younger than 16 years old, then in addition to his or her consent, the consent of the parent or trustee is required. In Estonia, the lowest age limit of 13 years will most likely be applied.
4. **Obligation to nominate a Data Protection Officer, if a company is one of the following:**
    - public sector company;
    - processing large amounts of data (i.e. the data of at least 5000 persons per year);
    - processing special categories of data;
    - employing 250 or more workers.
5. **Right to data portability from one service provider to another -** a service provider must be able to provide a person with his data in a structured, commonly used and machine-readable format, in order for this data to be transferred to another service provider.
6. **Obligation to maintain a record of processing activities** - each company shall maintain a record of all categories of personal data processing activities and preserve such records.
7. **Obligation to notify about the data breaches** – the Data Protection Inspectorate must be notified of incidents within 72 hours. In certain cases, the data subjects must also be notified.
8. **Obligation to conduct data protection impact assessments** - Where a type of processing (e.g. using new technologies) is likely to result in a high risk, the company shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
9. **Sanctions up to 20 000 000 EUR or 4% of the total worldwide annual company's turnover of the preceding financial year** - whichever is higher.

Deloitte has a comprehensive international experience in the field of data protection and is able to help bring the internal processes of your company in compliance with GDPR requirements. We are pleased to offer you the following services:

1. **GDPR maturity assessment** – whilst conducting the compliance assessment we provide you with an evaluation of whether the internal processes in your company are in compliance with GDPR requirements, including whether the data protection measures that have been implemented so far ensure the appropriate level of security and identify the security gaps.
2. **Drafting and reviewing data protection policies** – we will help you review and amend

the existing data protection policies or draft the new ones. The documentation in scope could range from the design of data protection policies as such, to the review of in-house implementing procedures, guidelines, contracts, checklists and more.

3. **Privacy *Help Desk* service** – if your company does not have the in-house experience in the field of data protection, then Deloitte is able to offer you a "help desk" that, in principle, will efficiently answer any legal or practical questions you may have about data protection, ranging from issues around notification requirements through reviews of contractual clauses with your service providers or the identification of special requirements on a specific subject in a country.
4. **Data protection impact assessments** - if you are planning a new activity which involves the processing of personal data or want to change an existing one, then we can help you assess whether such initiative could entail a data protection risk and if yes, which would be the best way to address this right from the start of the project.
5. **Assistance with communication with Data Protection Inspectorate** – we identify relevant registration and/or notification requirements applicable to your company, designing the notification approach, drawing up and submitting the relevant notifications and if your company desires to do so, building a notifications maintenance program to ensure that notifications' work is appropriately monitored and managed over time.
6. **Data protection training** – we organize a data protection training course for the management and/or employees of your company, during which we explain the GDPR requirements and how they affect your company, bearing in mind the specifics of your business.