Privacy legislation: are you GDPR compliant?

The European privacy regulation (GDPR) foresees a number of new provisions for processing, managing and keeping personal data. As from 25 May 2018 every Belgian company collecting data from EU citizens should comply with this new privacy legislation. Companies are responsible for complying with the privacy legislation and should be able to demonstrate this.

General Data Protection Regulation

Since 1995 a privacy directive exists which has been implemented in national law by all member states. This directive determines how and when companies can collect, process and transfer personal data to third parties. These rules currently do not honor our economic and technological reality (digital revolution, internet, cloud computing, ...).

The General Data Protection Regulation (GDPR) provides an answer to our daily internet world. The regulation already entered into force on 24 May 2016, but companies have the time until 25 May 2018 to adapt to the new rules. These rules now apply throughout the whole European Union without any further implementation legislation (some exceptions apply). This regulation does not apply to processing data of legal persons. The protection provided by this regulation only concerns individuals - irrespective of their nationality or place of residence - and the processing of their personal data.

Rights of civilians

The protection of (private) individuals when processing personal data is a basic right. Research by the European Commission has shown that internet users have questions concerning the way their personal data is used online. The new regulation provides individuals with more control by:

- Simpler access to their own personal data;
- The right to transfer data (data portability). This is an enhanced form of access whereby the concerned has the right to obtain personal data in a structured, common and electronic form;
- The confirmation of the right to data erasure or the right to be forgotten;
- The right to be informed in case of hacking of a database with your data.

Obligations of companies

As from 25 May 2018 some processors (e.g. banks and insurance companies) should appoint a Data Protection Officer (DPO). But also companies not falling under this obligation have an interest in appointing such an officer which can play an important role in the data protection policy of your company.

GDPR also obliges to keep internal documentation on processing activities (risk analysis). The Privacy Commission provides a register template. In order to take into account the specific situation of SME's and micro companies, a derogation on keeping registers applies to organizations with less than 250 employees.

COMPTAFID-Benelux NV SA Brussels
Bld. Edmond Machtensl. 180/100
B-1080 Brussels
Tel: +32 (0)2 410 75 75
www.comptafid.be

COMPTAFID-Benelux NV SA Antwerp
Schijnparklaan 45
B-2900 Antwerp (Schoten)
Tel: +32 (0)3 658 89 02
www.comptafid.be

COMPTAFID (Schweiz) AG Zürich
Seefeldstrasse 19 – Postfach
CH-8032 Zürich
Tel. : +41 44 250 2929
www.comptafid.ch

In order for companies to be prepared for the new rules, the Privacy Commission has drafted a roadmap (www.privacycommission.be). These thirteen steps concern the following:

1. Awareness: inform staff about the upcoming changes.
2. Data register: map which personal data are kept, where it comes from and with who it is shared.
3. Communication: are personal data currently being processed? Then you have to provide certain information to the concerned such as the identity of the processor and the way the data is used. Normally this information is provided through the privacy statement. This privacy statement should be completed with new information types.
4. Rights of the concerned: these are the same as under the current Belgian privacy law with some improvements. GDPR foresees a.o. in information and access to personal data; correction and exchange of data; objection against direct marketing practices; objection against automatic decision-making and profiling and transferability of data. The right to transferability of data is new.
5. Request for access: in most cases, free access should be given to the data within 30 days (currently 45 days).
6. Legal base for processing of personal data: ... is under GDPR almost identical as under the current privacy law. Examine the data processing, determine the legal base and document this in relation with the responsibility requirements.
7. Consent: the GDPR mentions 'consent' and 'explicit consent'. The distinction is not really clear. However consent cannot be deducted from silence, a pre-checked box or not acting.
8. Children: when your company collects data from children younger than 16 year, a parent or guardian should consent to process legally.
9. Data breach: data breaches where it is likely that the concerned will suffer some kind of damage, e.g. as a result of identity theft or breach of confidentiality obligation, should be reported to the Privacy Commission, within 72 hours. Also the concerned should be informed.
10. Privacy by design and privacy impact assessment: GDPR makes this a clear legal obligation. An impact assessment is only necessary in high risk situations, e.g. when new technology is being implemented.
11. Data Protection Officer: see above.
12. International: when active in an international environment, it should be determined which supervising authority is competent.
13. Contracts: criticize existing contracts, especially with processors and subcontractors, and if necessary modify in due time.

Stricter audits

The current privacy legislation remains almost unpunished since the Privacy Commission cannot impose fines. However, those who will not be GDPR compliant may expect severe audits. The Privacy Commission will after all obtain investigative and prosecution powers. Infringements are subject to administrative fines up to 20m€ or, for companies, up to 4% of the total worldwide turnover during the previous accounting year, when this amount is higher!