ekelmans meijer advocaten

5 things you can do now to ensure GDPR compliance

The General Data Protection Regulation is taking direct effect as from 25 May 2018 in the European Union

(1) Security measures

Proper security of the processing of personal data – and that involves the storage (location) of that data – entails appropriate technical and organizational measures. To provide an adequate level of protection the controller needs to implement modern techniques to ensure digital and physical safety of the stored data. Make sure you have an access policy when it comes to who within your organisation has access to personal data.

(2) Beware of Data Leaks

In the Netherlands there is a law called the Data Leaks Reporting Obligations Act. When a data leak occurs (for instance when a laptop is lost by an employee or when a system is hacked), the organisation has the duty to report the leak to the Dutch Data Protection Authority, but only if it leads to serious adverse consequences for the protection of the personal data. If an organisation fails to report a data leak, it could lead to fines up to € 820.000.

(3) Storage of data: retention periods and location

The GDPR gives a general norm for data retention periods: no longer than necessary for the purposes of processing. Be careful when formulating those purposes: you need to indicate a concrete period of time until (i) the data will be deleted or (ii) that will be reviewed whether or not the purpose for processing has been fulfilled. Furthermore, Dutch law can indicate specific retention periods for specific data.
Regarding storage locations: as long as the server park is in the EU, you don't have to worry. It gets more complicated if that server park is in the US or Africa. When it comes to cross-border data transfers, it is only allowed when the third country has an adequate level of protection equivalent to that of the EU.

(4) Consent of the data subject

When you are processing personal data, you need a legitimate basis that provides the lawfulness of the processing. The first and foremost basis for processing is freely given consent of the data subject. Your organisation, as controller of the data, needs to make sure the consent is truly given freely. The request of your organisation for that consent should be transparent, specified, explicit and in a clear and plain language. If you rely on consent, review your consent forms and other documentation to ensure you uphold the standards of the GDPR.
Next to consent, there are other grounds for lawful processing, such as the legitimate interest of the company itself that outweighs the interest of the data subject, or when processing is absolutely necessary for the performance of a contract.

(5) Privacy statement: rights of data subjects

Every company should have a privacy statement (or privacy policy). The controller of the personal data is obliged to provide certain information to the data subject in a transparent manner, using clear and plain language. This includes for instance the purposes for processing, the right to lodge a complaint with a supervisory authority, the period for which the data will be stored, etc. However, it is of the utmost importance to inform the data subject of their 'new' rights under the GDPR. The privacy statement should therefore include, amongst others: the right to be forgotten, the right to rectification and the right to data portability of a data subject.
As a controller, you must be vigilant when drafting or adjusting your company's privacy statement and any additional documents concerning privacy, bearing in mind the obligation of your company to fully inform the data subject (think about the obligation of the controller to disclose the processing to all natural persons whose data could possibly be involved in the data processing). All of these obligations not only play a big role in contractual engagements, but also in the field of (in)direct marketing.

The Privacy Desk can assist you with questions about the GDPR and offers practical solutions. Just click: https://www.ekelmansenmeijer.nl/en/expertise/practice-groups/privacy