5-Minute Insight

The General Data Protection Regulation: key changes and risk assessment in the context of non-compliance

The General Data Protection Regulation (GDPR) seeks to harmonise national legislation regarding data protection across the EU. It includes important new rules on governing, using, collecting, retaining and sharing data. The key changes relate to privacy legislation (especially in the field of customer relations), internal privacy mechanisms and enforcement rights of the supervisory authorities. The impact of non-compliance can be high given the significant fines and the possible reputational damage following a data breach notification.

Key changes

Customer relations

Consent

One of the legal requirements for the processing of personal data (including customer data) is the data subject's consent to the processing of his or her personal data. The GDPR imposes requirements for the request to consent. The request must be in simple, understandable wording and form. The connection between the personal data and the purpose for which it is processed must be clear and the request must be clearly distinguishable from other matters or requests. As a result of these requirements, a request for consent can no longer be part of a company's general terms and conditions. The data subject has the right to revoke his or her consent at all times. The data processor will then have to stop the processing if no other legal ground for continued processing exists. Revoking consent must be as easy as giving consent.

Right to be forgotten

The GDPR gives customers the right to be forgotten. Customers are entitled to ask the processor to delete their personal data, where continued processing is no longer required for its original purpose, or where they have withdrawn their consent. The data processing systems must be designed so that compliance with this new right is possible.

Portability

Customers will become entitled to request that their personal data is transferred from one company to another, for instance when switching providers. Companies are obliged to facilitate this data portability in a structured and commonly used machine-readable format.

Internal privacy mechanisms

Privacy Impact Assessment

A new tool on the road to compliance is the privacy impact assessment (PIA). A PIA must be carried out when new technologies are being used and where data processing is likely to result in a high risk to the rights or the freedom of the data subjects. Please note that the PIA is seen as part of the general duty of care of a company. Conducting PIAs on a regular basis reduces the chances of violating this duty of care.

Personal data: any information relating to an identified or identifiable natural person ('data subject')
Data subject: a natural person whose personal data is being processed
Supervisory authorities: an independent public authority which is established by a Member State pursuant to the GDPR
Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed

pwc

Data Protection Officers
The GDPR requires the appointment of a data protection officer (DPO) by companies whose core activities consist of (i) data processing operations that require regular and systematic monitoring of data subjects on a large scale; or (ii) processing on a large scale of special categories of data (including sensitive data relating to health, religion, race, sexual orientation, etc.). The DPO consults on privacy matters, develops internal privacy regulations and monitors compliance with the GDPR. The DPO does not have the power to impose sanctions, but will have supervisory powers. The DPO must be allowed to perform his tasks independently and must not be dismissed or penalised for performing his tasks. In order to ensure this, a DPO must be bound by professional confidentiality. The DPO reports directly to the highest management level of the company.

Privacy by design/Privacy by default
The GDPR obliges companies to implement the principles of data protection in their new and existing ICT systems and procedures. This is called privacy by design. Examples of these principles are data minimisation and data processing for specified, explicit and legitimate purposes. To further ensure the protection of data subjects, maximum privacy must be the default option when using standard settings. For example, if a customer needs to register to receive a service, only the minimum of personal data necessary to provide the service should be processed. Any excess data processing will require the data subject's active and explicit prior consent.

Enforcement rights of the supervisory authorities

Substantial fines
A large part of the regulation is dedicated to the supervisory authorities. Their new powers include the ability to impose higher fines, to limit or ban data processing by a company and to impose rectification or erasure of personal data. The fines were significantly increased: the maximum fine is set at € 20 million or 4% of the global annual turnover of the respective company, whichever is higher.

Data breach notification
Any breach of personal data falling within the scope of the GDPR must be reported to the supervisory authorities within 72 hours after discovery of the breach. When the data breach is likely to result in a high risk to their individual rights and freedoms, the data subjects should also be informed about the breach. This may result in public disclosure of the data breach. Failure to comply with this rule may lead to substantial fines.

The risk of non-compliance

In view of the above, we have identified risks for companies in several areas:

- *Regulatory risk*: Substantial fines may be imposed on companies for non-compliance with GDPR provisions, which may also lead to increased personal liabilities for board members.
- *Reputational risk*: Now that companies are required to notify the supervisory authority of a data breach and, in some cases, the data subjects as well, data breaches can become publicly known. This can lead to brand damage, loss of consumer trust, loss of employee trust and consumer attrition.
- *Financial risk*: Apart from the obvious financial loss caused by a substantial fine or the decline of earnings due to brand damage, there is also the risk of litigation costs. The fact that data subjects have gained more rights may cause customers to sue the company in the case of infringements. In addition, if IT systems or data protection procedures are inadequate or out of date, the costs of remediation must also be paid (i.e. due to the privacy by design and default principles).
- *Operational risk*: There are several risks in conjunction with the operation of enterprises. One of these is the possible temporary or permanent limitation on processing personal data imposed by the supervisory authorities. Other risks include invalidated data transfers to third parties or non-European countries.

Scope and entry into force

The GDPR applies to (i) the processing of data within the EU; (ii) the processing of data of EU citizens; and (iii) the processing of data by a company established outside the EU if such processing is related to the offering of goods or services to EU citizens or the monitoring of their behaviour.

The GDPR can be enforced as of 25 May 2018, when all companies in the EU must be compliant.

For a more in-depth discussion about the key changes described above, non-compliance risks and any other questions you may have about the GDPR, please contact:

Yvette van Gemerden
Partner | Privacy Law
+31 (0)88 792 5442
yvette.van.gemerden@nl.pwc.com

Sander Geurts
Senior Consultant | Privacy Law
+31 (0)88 792 19 41
sander.geurts@nl.pwc.com