Whitepaper

The new privacy regulation or GDPR. How to comply?

GDPR Management
By Data Privacy Partners

General Data Protection Regulation

The existing rules around the protection of personal data are being strengthened with the introduction of the General Data Protection Regulation. Every organization has to deal with the GDPR, because almost every organization processes personal data of customers, suppliers or employees. On May 25, 2018, the processing of personal data has to comply to the GDPR. In this whitepaper are the main consequences for the organization summarized with a guideline.

What happens if the GDPR is not respected?

The consequences of not complying with the GDPR are far greater than under current law. The new height for fines is far more than before. The privacy authority can now give fines from either up to €20 million euro's or 4% of the global turnover for the organization, whichever is higher.

Which data qualifies as personal data?

Every piece of data that can be traced back to a living person is personal data, some examples of this are: name, email address and birth date. There are some pieces of data that have extra protection under the GDPR law, for example: race, religion or health status.

What is careful processing?

Starting point of the GDPR is the obligation to process personal data carefully and in accordance with the law. The GDPR creates a number of obligations on main features and are discussed further in this document. When your organization wants to know where they currently stand they can do a Privacy Impact assessment (PIA). This is an instrument of proposed regulations for projects, in which personal data are processed, to study the effects for those involved and to assess on the impact in the event of a data breach.

Data Privacy Partners
Tel. +31 (0) 888 SECURE (732873) https://data.privacy.partners

Registration- and documentation duty

All organizations will be required to show that they are "privacy law (GDPR) compliant" to the supervisor. An organization has to be able to demonstrate with documents that appropriate measures have been taken. Important here are company wide information security policies where attention is paid to the technical aspects (e.g. backup & restore plan, identity and access management) but also the organizational side (people side) of the risk management. This includes for example: security awareness, Incident response procedure, and Bring Your Own Device policy.

This registration and documentation duty also applies to your HR administration and customer administration!

Finally, your organization has to implement ' privacy by design ' and ' privacy by default '. This means that for example (web-) forms and fill menus etc. privacy enhancement settings are set and that no unnecessary information is required (data minimization).

Processing agreement

When your organization uses another party for the processing of personal data (processor), such as a payroll processor, administration office or a hosting provider that stores data, then closing a processors agreement with this party is required. A processors agreement drawn up between the responsible (client) and the processor describes the way in which a processor deals with the personal data.

Also, both the client and the processor must keep a processing register. It contains, among other things, the contact details of the client and processor, responsible persons for data, the name of the data protection officer (DPO) if required, purposes of data collection and categorization of personal data. Also it contains a general description of the security measures taken.

Right to inspection by, among others, employees and customers:

- Personnel and customer file;
- A copy of their personnel or customer file in a standard format (such as a PDF-file);
- Easy-to-understand information about the how and why of the processing, his/her rights and the privacy policies of the Organization;
- Free at all times to access the Information concerning them, and, if necessary, to correct it or removal (for example because of the right to be forgotten).

The Organization will be, on penalty of a fine, required to provide all of the requested information.

Preventing technical data breaches

The law calls for your organization to take technical appropriate measures in order to guard the private sensitive data. Handy tools for example are a so-called GDPR-Gap analysis and a penetration test on your digital organization by examining security gaps.

When discussing technical measures think of the following:

Secure network and access	Secure Data	Secure Identity and Access Management	Secure Devices	Secure Email
Unified Threat Management (UTM)	Secure Data Sharing	VPN	Mobile Device Management	Email encryption, decryption and signing
Security Operation Center	Collaborate and store	Strong Authentication	Endpoint Protection	Automatic secure archiving
(Wireless) Access Control		Authorization Management	Vulnerability Scans	

Data Privacy Partners
Tel. +31 (0) 888 SECURE (732873) https://data.privacy.partners

DPO as a service

Some organizations are required to appoint a Data Protection Officer. Hiring a Data Protection Officer (DPO) is advised when implementing the GDPR as a project. The advantage is that a DPO has extensive knowledge about the whole scope of aspects to be handled when implementing the GDPR (juridical, organizational and technical).

Conclusion

Organizations need a listing of all processing of personal data to track and demonstrate that appropriate (organizational and technical) measures have been taken to protect privacy-sensitive personal data.

We live in a time in which we increasingly become more aware of privacy and the problems surrounding the protection of privacy. Almost every day in the newspapers and on the internet there is something to read about a hack, a data leak or privacy violation. Your organization doesn't want to be among these posts right? Apart form all the work and mysery caused by dataleaks your organization might also suffer of image damage resulting in financial losses. By taking privacy and data protection seriously you can prevent this and even gain a head start while outpacing your competitors!

Data Privacy Partners
Tel. +31 (0) 888 SECURE (732873) https://data.privacy.partners