WHITEPAPER

This is how the new General Data Protection Regulation, GDPR works!

This is how the new General Data Protection Regulation, GDPR works!

Does your company have a registration page where you collect personal information? All organizations that process personal data in any way are affected by the new General Data Protection Regulation, GDPR. But, what does the regulation really mean in practice? And, how does it affect your business? In this paper, we will try to combine our knowledge and expertise in IT security and law, to interpret the regulation so that everyone will be able to understand what is required to comply with the new regulation.

The main purpose of the GDPR is to ensure that people have the ownership of their personal data and that their privacy is respected. Personal data encompasses all information that can be linked directly or indirectly to an identifiable physical person. For example, a person can be directly identified with information such as a name, social security number, phone number or e-mail address. Data that can be indirectly linked to a person is for example eye color, age, occupation, shopping habits and interests.

GDPR gives people much stronger rights pertaining to their personal data than what most countries offer today. Individuals have the right to be informed about what personal data is being processed, to be able to make corrections and have personal data deleted. Any time personal data is processed, it must have a clear and specific purpose. Organizations can't collect personal data just because it may "be good to have." And, companies will be required to gain control over their unstructured data, such as e-mails and Word documents.

Built-in data protection on multiple levels

The new legislation places high demands on built-in data protection. In practice this means two things - Privacy by design and Privacy by default.

Privacy by design means that privacy protection should permeate the entire system's life cycle, from the gathering of requirements to the maintenance of the system. Today, it is common for security and privacy protection to be added afterwards as an add-on in system development, which will no longer be acceptable.

Privacy by default means that the strictest privacy settings should be active by default and should not be required to be manually configured by the user. For example, web sites like Facebook should not make public accounts public per default.

New liability

The new regulation places new demands on controllers and processors. A controller is the legal entity (public authority, company, etc.) that controls what and why personal data is being processed. A processor is an organization that processes personal data on behalf of a controller, i.e., a supplier. Controllers and processors can receive sanctions that amount to a maximum of 4% of global sales or 20,000,000 euros!

New documentation requirements

With GDPR, you must prove when, why, what and how you process personal data from the beginning. The regulation simply imposes very hard documentation requirements. A privacy policy and a data protection policy must be written.

With the new risk exposure and the new requirements in Article 28, all contracts between controllers and processors will need to be rewritten. It is also essential that log management be introduced to provide proof when a breach has occurred and who/what is responsible.

More stringent requirements in case of a breach

When GDPR comes into effect on May 25, 2018, the rules around breaches are tightened. A breach may, for example, involve personal data that has been stolen, hacked, misrepresented on the Internet, improperly destroyed or altered.

When should incidents be reported?

As soon as the controller becomes aware that a personal data breach has occurred, the controller must notify the personal data breach to the supervisory authority without undue delay, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Data Protection Officer

There will be a requirement for many organizations to hire a Data Protection Officer (DPO). The role of DPO involves, among other things, helping and controlling compliance with GDPR in the organization. It is also the role of the DPO to report to the supervisory authority, so it is important that there is no conflict of interest. For example, a CEO, CIO or CTO can't be a Data Protection Officer.

What organizations will require a DPO?

- A must for all public authorities.
- Companies that handle sensitive personal data to a large extent.
- When regular and systematic monitoring of personal data is done on a large scale.

This is how the new General Data Protection Regulation, GDPR works!

Impact assessment

Before your business can start using information systems and new technologies that process personal data, Article 35 of the GDPR must be met. In short, it states that a Privacy Impact Assessment (PIA) has to be conducted where the processing of personal data can pose a high risk to the rights and freedom of data subjects. A privacy impact assessment includes a risk analysis, mapping of the flow of personal data in systems, and checks compliance with GDPR.

GDPR involves major changes that will require an early start

In conclusion, the General Data Protection Regulation will require many organizations to rethink when it comes to personal data. It is time to understand that personal data can only be owned by the person that the information relates to. An organization can only borrow this information for legitimate purposes. In accordance to the principle of transparency, organizations must become more transparent and tell you what, how and why they process your personal data.

Here's what you need to do for your business to live up to the new data protection regulation – step by step

Start by asking the following questions:

- What personal data does the organization process today?
- Why and how is it processed?
- Are the processes within the organization documented?
- Identify the organization's personal data flows.
- What security mechanisms does the company have, internally and externally?

Start this as soon as possible:

- Discuss the issue at board level and allocate responsibility and appropriate resources throughout the organization.
- Discuss GDPR with a lawyer.
- Inform all relevant entities within the organization, such as IT, Customer Support, Communications Department that changes are under way.
- Start looking for a good data protection officer.

Before December 2017, your company should ensure that the privacy policy is in place and that the processing of personal data is documented, updated and communicated with employees.

In order to achieve this, the company must:

- Train its employees.
- Update the organization's IT infrastructure, security, and develop privacy by design.
- Review and adapt all vendor contracts regarding personal data processing.