MLI

AUSTRIA

Data protection reloaded - The GDPR chances and risks

Written by Markus Dörfler, Hohne, In der Maur & Partner

For a moment you could assume that 24 months is a long period of time to implement new rules in a company. But this is wrong. Changing business processes within 24 months is a very challenging task. What happened? The highest political level within the European Union discussed for several years to compromise a new General Data Protection Regulation (GDPR) till 2016.

Markus Dörfler

Largely unnoticed, it came into force on May 24 2016. The reason why the majority did not take notice about the regulation is the transitional period which exists until April 25 2018. The new regulations must be applied from that date. A large number of companies let the first year go by without any action. Only in the beginning of 2017 they realised the need of adapting many business processes to the new situation.

Who is affected by the new General Data Protection Regulation? Basically the General Data Protection Regulations hall be respected by all natural or legal persons, authorities, institutions or other bodies who process personal data.

What is the definition of “personal data”? If a natural person is identified or identifiable we are talking about personal data. A natural person is identifiable if it can be identified due to a personal identifier, ID, location data or other characteristics.This means in summary that every company has to respect the General Data Protection Regulation since every company processes personal data.

In the now repealed regulation (Directive 95/46/EC – General Data Protection Regulation) from 1995 data processors were obliged to comply with several principles (especially a precise and legitimate purpose for the data processing must be defined). In the GDPR even more principles must be fulfilled. Until now it was sufficient that the processing happens in good faith, for a specific purpose, in a small extent, accurate, for a limited period of time and secured.

From now on the processing must also be transparent. This means that the controller (the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data) must disclose to the data subject (the natural person which can be identified or is identifiable within the data processing) how the data is processed. Even the changes in the legitimate basis lead to the fact that companies have to adapt their business processes to the new situation.

But there is more. As before, is it necessary that the data subject has given consent to the processing of his or her personal data for one or more specific purposes.This very strict criteria are now even more aggravated by the General Data Protection Regulation. From now on it is essential that the he controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

In addition, from now on the processing of special categories of personal data (formerly: sensitive data) will be stricter. Specific categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and data concerning health or data concerning a natural person's sex life or sexual orientation.

The GDPR extends this definition so the processing of genetic data, biometric data for the purpose of uniquely identifying a natural personis included. By now the processing of these categories of personal data is prohibited except the processing is explicit allowed.

Even in the old regulation there was a right of access by the data subject. The data subject has the right to ask the controller (once a year: for free!) which personal data relating to the data subject is processed by the controller. The controller is obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests. But there is more. The data subject has the right to rectification.

The controller is now obliged to communicate any rectification (even the erasure) of personal data to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. Due to the fact, that there is an automatic data processing the information will not be impossible nor involves disproportionate effort. On to the controller is obliged to inform the data subject about those recipients if the data subject requests it.

The next big thing is the technical part of the GDPR. The data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller. This norm has a deep impact in the way how companies a processing personal data.

Furthermore the controller is obliged to, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles in an effective manner. These “technical an organizational measures” include – for example – data minimisation and pseudonymisation. Pseudonymisation means the processing of personal data without the direct connection to a natural person, so no data subject is identified or identifiable.

In a next step the controller is obliged to implement measures that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Additionally such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. The controller must implement appropriate “technical and organisational measures” to ensure a level of security appropriate to the risk. This level of security depends on the nature, scope, context, amount, context and purposes of processing.

The organizational part of the GDPR is also fierce. Just to name one thing: Each controller must maintain a record of processing activities under its responsibility. That record has a high detail grade about why, how and where the personal data is processed.

This is just a short (not complete) list of things regarding companies. But: What happens if the companies don’t comply with the GDPR? There will be administrative fines – up to 20.000.000,00 Euro or up to 4 per cent of the total worldwide annual turnover of the preceding financial year – whichever is higher.

All of these changes mean that data protection costs are increasing in the company, but it is also an opportunity. With the new rules, companies have the unique opportunity to streamline work flows within the company and define them in a comprehensible manner.

Whether the company uses this opportunity, the future will tell.

Biography

Mag. **Markus Dörfler** LL.M., born in 1979, worked for several years as an it-technictian while he studied law in Graz and Linz. Afterwards he graduated as Master of Laws in Vienna. After several years as a self-employed attorney he became partner of Höhne, In der Maur & Partner. He is specialized in IT-Law, copyright law and data protection law. Markus Dörfler is lecturer on IT-law at the University of Applied Sciences of BFI Vienna and author of several publications about IT-Law and data protection law.