TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

The new EU General Data Protection Regulation - What businesses need to know

G DATA Software AG | September 2017

Introduction

Guaranteeing the privacy of personal data requires more than just a regional or national policy: the updated EU General Data Protection Regulation (GDPR) puts data protection on the agenda of companies across the European Union. Starting 25 May 2018 at the latest, businesses must comply with the new regulation with effective protection for their customer data. Non-compliance fines are higher than before, increasing the pressure. Companies must inform their employees and check workflows and tools in order to make sure that customer data are processed in accordance with the updated regulation. This leads to a number of measures that must be taken, many of which involve changes to IT infrastructure. This whitepaper lists the most important changes of the General Data Protection Regulation and shows the ways in which a comprehensive IT security solution can support GDPR compliance.

1. What is the EU General Data Protection Regulation?

The European Parliament adopted the EU General Data Protection Regulation (GDPR) in April 2016. The GDPR updates and unifies the various data protection regulations of EU member countries. Its goal is to guarantee the protection of personal data regarding the following principles[1]:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality

The regulation replaces the somewhat outdated Data Protection Directive (DPD), which was passed in 1995. Unlike the DPD, the GDPR is not ”just” a policy, but an actual law. It does not need to be separately ratified by the EU member countries. This means it already went into effect on 24 May 2016. To make sure businesses have enough time to comply with the new law, a transitional period was decided upon. This period ends on 25 May 2018. Businesses must implement measures to meet the GDPR requirements before this date. If they do not do so, large fines may apply in the event of a data breach.

2. Which companies are affected by the GDPR?

The General Data Protection Regulation guarantees the protection of personal data. This means it applies to all companies that process personal data of natural persons in the EU. To clarify the type of data to which the law applies, Article 4 contains the following definition:

> „For the purposes of this regulation, ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is

[1] See GDPR Article 5. The full text can be found at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

> one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

This admittedly very broad definition includes many data types that are typically processed by businesses, such as names, addresses, e-mail addresses or IP addresses. In enterprise contexts, this often means customer data, such as those processed by CRM systems. But even data that are only collected for marketing purposes or data that are collected as a "by-product", such as IP addresses in a log file, are protected by the GDPR.

3. What rights do customers have under the GDPR?

The GDPR describes measures that must be carried out by all businesses that process personal data. While many of the measures were already defined as part of the Data Protection Directive, some new ones were implemented, which means that even businesses that were compliant up until now may be affected. A short overview:

- Right to be forgotten: Customers have "the right to obtain (…) the erasure of personal data concerning him or her" (Article 17).
- Purpose and right to consent: These measures were already partly implemented in national data protection laws, but GDPR further specifies them. Every customer must be informed about the purpose for which the data are required in an "easily accessible form, using clear and plain language". Consent must be given voluntarily – businesses cannot demand consent based on other requirements (for example, consenting to receiving marketing in order to be able to finalize an order). These measures are specified in GDPR recitals 42 and 43.
- Rapid notification to the supervisory authority: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority" (Article 33).
- Right to data portability: Customers have the right to receive personal data about them "in a structured, commonly used and machine-readable format" (Article 20).

The implementation of these requirements in enterprise workflows is not simple. For example, many requirements presuppose that business know exactly which personal data are stored where. This may be true for small firms with only a few IT systems, such as a central customer database. However, as soon as one considers data sources such as video surveillance in publicly accessible spaces or workflows that process data on cloud platforms (such as Salesforce), it becomes clear that many businesses process and store more personal data than they might be aware of. Many of these workflows may not even be within the direct sphere of influence of the company itself. There may also be ambiguity in cases where customers would like to erase data for which there are other (legal) storage requirements.

4. What happens in case of GDPR non-compliance?

New customer rights are not the only concepts to be added to the GDPR: the regulation also defines a new structure of fines for businesses that wrongly implement GDPR regulations (or do not implement them at all). If a supervisory authority discovers a violation, it can impose an administrative fine, based on the severity of the case:

- Up to € 20 million or 4% of the total worldwide annual turnover (whichever is higher)
- Up to € 10 million or 2% of the total worldwide annual turnover (whichever is higher)

The first category includes cases where a business does not comply with the requirements from Article 17 (Right to be forgotten). The second category is meant for comparably small violations, such as an infringement of the notification requirements of Article 33 – but with a maximum fine of € 10 million or 2% of turnover, fines may still turn out to be significant. The fines are defined in Article 83 of the GDPR, which also mentions that the imposition of fines must be “effective, proportionate and dissuasive”.

5. Countdown has started: what to do?

In spite of the increased fines and the rapidly approaching end of the transition period, many businesses have not yet implemented any measures. Gartner estimates that more than half the firms that are affected by GDPR will not have implemented all required measures by the end of 2018[2]. Considering the large number of possible effects, it is advisable to focus on the most vital steps in order to comply.

5.1. Appoint a Data Protection Officer

The first step is to appoint a Data Protection Officer (DPO). According to Article 37, this is mandatory for public authorities and public bodies that process personal data. For SMBs, designating an external DPO can be an option. The officer will be the official spokesperson for the company when communicating publicly or with the data protection authorities. Even firms that are not required to appoint a DPO may benefit from having one, for example in order to establish a single point of information for all internal and external questions about data protection.

5.2. Identify points of focus

For every business, regardless of size, the following questions can be helpful to identify the points of focus for the implementation:

- Which GDPR-relevant data are being collected or processed?
- Are the data sufficiently protected? Is the technology state-of-the-art?
- Can data protection authorities be notified within 72 hours of detecting a data breach?
- Can customers request information about their data and/or can the data be deleted?

[2] Source: https://www.gartner.com/newsroom/id/3701117.

- Are data sent to external parties for storage or processing (e.g. cloud services)? Are any changes to existing contracts required?

5.3. Check workflows and tools

Businesses must inform their employees and check their workflows and tools in order to guarantee compliance with GDPR. It is important to create a set of compliance policies that define the workflows around data. Such policies can be a combination of technical and organizational measures. For example, Policy Management can be an appropriate technical solution to make sure that only those applications that are required for data processing can be used – and no others, such as private cloud storage services. The use of external storage devices should also be restricted, to prevent employees from storing personal data on USB sticks or similar media.

5.4. Check and secure IT infrastructure

Comprehensive protection of IT infrastructure is an essential step. Existing systems must be checked and new systems may have to be planned and deployed. Security starts on the network and communication levels. For example, to block unwanted connections, a firewall should be used. Web traffic and other online communication channels should be scanned, for example by a web protection component or an email scan. Protection against malware can be implemented with a proactive file system and process monitoring system. To make sure that the operating system and all applications are up-to-date, a patch management system helps keep tabs on patch deployment. Last but not least, data availability is a major point: to make sure data cannot be lost, a backup and restore concept should be developed and implemented.

G DATA supports your road to GDPR compliance

To comply with the technical requirements of the GDPR, the protection components of the IT infrastructure and the associated organizational processes must be synchronized. This requires a unified policy for the monitoring of network infrastructure and the notification of administrators in case of possible data breaches. G DATA offers a Layered Security concept for enterprise networks of all sizes, which combines optimized pro-active protection with efficient notification features to enable regular reports and incident notifications. You can install G DATA business solutions on-premises and keep deployment and management in-house, or outsource the effort of installing and managing the solution to an external partner with the SaaS solution G DATA Managed Endpoint Security.

More information about G DATA business solutions can be found at www.gdatasoftware.com/business. The G DATA Security Blog at www.gdatasoftware.com/blog/ features posts about data protection, compliance and IT security.

Please note that this Whitepaper cannot replace comprehensive legal advice about GDPR.