Guide GDPR
version 1.0

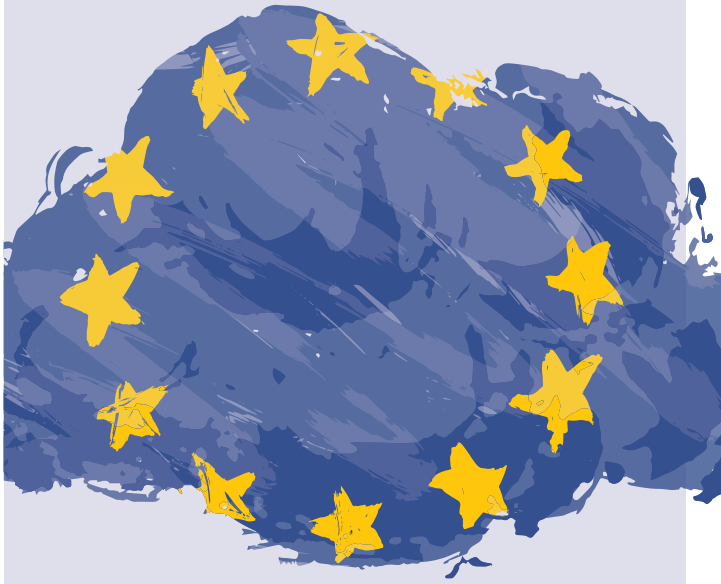

TABLE OF CONTENT

Foreword

This guide is intended as an easy-to-understand, educational and comprehensive tool for those who are responsible for their organization's compliance with the new General Data Protection Regulation (GDPR). The guide can also be of use to those who have academic or other interests. The Data Protection Regulation will be the most important issue for many management teams in 2017/2018. This guide will provide you with much more than just a basic insight into the subject. It provides concrete examples and guides you through the difficult legal jargon and the unique concepts of the regulation.

It is less than one year left until the regulation is applied in member state law, and this guide will be updated continuously as more information about the regulation is published. In the next version of this guide, the following sections will be added: Profiling, Data Privacy Impact Assessment, Transfer of Personal Data to Third Countries, Access Control, GDPR Log Management, Privacy by Design and the Right to Data Portability.

I wish you good luck with your GDPR compliance.

Jonas Gharanfoli
Security consultant

jonas.gharanfoli@24solutions.com
+46 735 24 24 05

1. Background

On May 25th, 2018, the General Data Protection Regulation (GDPR) will apply in member state law. The regulation affects all organizations that process personal data of EU/EEA-citizens, such as companies and public authorities. The purpose of the regulation is to extend and ensure the privacy rights of all EU/EEA-citizens. For example, if your organization has a CRM-system or an employee register, your organization will need to comply with the General Data Protection Regulation.

Prior to GDPR, member states were regulated by the Data Protection Directive, enforced in 1995. A lot has happened since 1995; the digital world we live in today has changed the conditions of how personal data can be collected, disseminated and analyzed. The development of Big Data analytics, marketing and the deployment of services such as Facebook have fueled the privacy debate in Europe. In January 2012, the European Commission presented a proposal to thoroughly reform the Data Protection Directive. As a consequence, the Data Protection Directive was expanded and converted into a regulation.

GDPR is a regulation and not a directive.

Both regulations and directives are called 'legislative acts' in EU law. Directives are goals given to member states. It is up to each member state to decide how to achieve the goals by incorporating the directive into new or existing laws. This means that laws created by directives may differ significantly between member states. By contrast, regulations are basically complete laws that will apply directly in full to all member states on a predetermined date. Regulations thus lead to much stronger harmonization within the EU/EEA.

The burden of compliance will be immense for many organizations, however, an organization that prepares in time can get a significant competitive advantage. In addition to improved privacy protection, many service providers and customers will require your organization to comply with the GDPR as they may be put at risk if you do not. Member States and regulatory authorities are also encouraged by the regulation to introduce certification mechanisms for the GDPR. In the same way as organizations can certify themselves to demonstrate their environmental responsibility, organizations will be able to demonstrate their privacy and cyber security responsibilities.

1.1 Which organizations are affected?

GDPR applies to all organizations that "process" personal data belonging to EU/EEA citizens, even if their base of operations is outside the EU/EEA. The regulation may cause a global uproar as there are many organizations outside of the EU/EEA that process personal data belonging to EU/EEA citizens. The public sector will also be affected because public bodies must comply with the regulation as well. The regulation regulates those who control the processing of personal data (controllers) along with service providers (processors) that process personal data on controllers' behalf. The organizations that are excluded from the regulation are law enforcement agencies like the police. They have a new directive from the European Commission that is similar to the GDPR.

1.2 Key differences between the GDPR and the DPD

- *The privacy-rights of data subjects are enhanced.*
- *The supervisory authorities can impose harsher administrative fines – maximum administrative fines up to 20 000 000 EUR or up to 4 % of the total worldwide annual turnover, whichever is higher.*
- *Privacy by design - privacy protection should be incorporated into systems from the very beginning and permeate their entire life cycle.*
- *More requirements concerning assessments, processes and documentation.*
- *Consent must be gathered in a more transparent manner and is required under more circumstances.*
- *"The right to be forgotten" will be enforced. This means that organizations must, in certain circumstances, delete all personal data of data subjects if they wish.*
- *The processing of children's personal data will require the consent from the holder of parental responsibility over the child for "information society services" (e.g. Facebook, Instagram).*
- *New requirements for marketing (profiling / selection).*
- *Your organization must, under certain circumstances, retain a Data Protection Officer.*
- *Service providers (processors) are liable under GDPR. In the DPD, only controllers were liable, now both processors and controllers can suffer penalties if they violate the GDPR.*
- *More requirements concerning processing agreements, which will need to be rewritten.*

2. Key Concepts

The regulation contains unique terms, definitions and concepts that the reader must know before explaining the more complex aspects of the regulation.

2.1 What is personal data?

According to the regulation, 'personal data' is:

"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is 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" (Article 4(1))

An identified or identifiable natural person means a living person in the regulation (it is up to each individual member state to decide whether it must be a living person or if personal data of the dead should be covered).

"... an identifiable natural person is one who can be identified, ***directly*** *or* ***indirectly****..."*

You can directly identify someone by, e.g., their full name or social security number. If someone has a very rare first and/or last name, this can suffice to directly identify someone. You can indirectly identify someone by combining information such as occupation, location, physical characteristics, and social status. For example, "cyber security consultant + brown hair + Frösunda (a small area in Sweden)" is personal data because this information can be indirectly linked to a very few identifiable natural persons in Frösunda. A guideline used by statisticians in the domain of PII (Personal Identifiable Information), is if the information can be linked to less than seven people, it is considered PII or personal data.

"Identifier such as a name, an identification number, a location or online identifiers ..."

Online identifiers such as IP addresses and cookies are also considered personal data. Location data such as GPS coordinates are considered personal data if they are linked to a person.

Are dynamic IP addresses personal data?

Today, it is very common for people visiting websites to have their IP address stored by the owner of the site. A dynamic IP address, together with the time and the ISP's customer directory, can identify exactly which computer visited a webpage at a certain time; this information can thus be attributed to an identifiable physical person. According to a verdict from the European Court of Justice (The Breyer-verdict), dynamic IP addresses are considered personal data if the owner of the website has "legal means" to request third-party information, such as ISP information, and it should not be "Impossible to implement in practice".

2.2 Processing

The term 'processing' is very broadly defined in the regulation, it basically includes everything you could possibly do with personal data. The full definition from the regulation reads as follows:

"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4(2))