Everything you need to know about Data Protection Regulation (GDPR)

In our modern world, we use devices connected to the internet in our free time and in business. Smart phones, tablets and computers are connected and become more and more connected to other devices making it easier to do business, making our lives more comfortable and enabling government agencies to better interact with citizens. Doing business is built on trust. Trust in receiving the products and services in time and with the expected quality.

In order to obtain the services and products people will have to register and provide personal data. Customers/ citizens do so on the basis of trust. They would like their data to be handled carefully and only used for the purpose they provided their data. The higher this trust is, the more likely it becomes that customers/citizens turn to your organisation. The commercial power and attractiveness of doing business with your organisation is built on this trust. Data protection today is an important customer value. Organisations that prove they have a high level of data protection and continuously work to improve their protection level have a substantial competitive advantage.

Privacy & Data Protection

It is therefore that privacy is an important aspect in todays connected world. Privacy is interpreted in many different ways. For instance:

- "the right to be let alone"
- protection of personal data
- the right to self-determination over one's personal data
- a basic human right: article 8.1 of the European

Convention of Human Rights states that "Everyone has the right to respect for his private and family life, his home and his correspondence".

In many countries, there are laws and regulations in place to protect privacy. But they differ from country to country hampering the exchange of personal data between public and private sectors, associations and enterprises. If it comes to the digital world, the topic needs to be handled on a supra-national level.

Therefore, the European Union has adopted the General Data Protection Regulation (the GDPR), which entered into force on May 24th 2016. and will be enforced from May 25th 2018 onwards. The GDPR regulates how businesses, government institutions and other organisations in private and semi-public sectors should handle personal data in order to protect the privacy of individuals living in the EU.

Emphasizing the importance of compliance, the penalty for violations of the GDPR can run up to 4% of global revenue (or of € 20 million).

A high-level overview of the GDPR

The definition of Personal Data and Data Subject

In order to know if compliance to the GDPR is at hand it is important to know what data is defined as personal data and what processing actually means.

According to article 4 subsection 1 personal data is: 'any information relating to an identified or identifiable natural person ("the Data Subject")'. This means that a photo, name, email address, telephone number, GPS location, IP address, bank account number or a social security number is personal data. The definition is quite broad leading to the effect that the impact of compliance to the GDPR on your organisation could be substantial.

Controller and Processor

The GDPR distinguishes between a Controller (the party who collects personal data), a Processor (who process data on request of a controller).

What is Data Processing?

Article 4.2 defines data processing as ["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"]. This is slightly different from the way that computer science usually looks at processing as the use of algorithms to transform data. Actions such as data transport and media destruction are usually not considered 'processing' in traditional IT environments, but are definitely in scope from a privacy point of view

When is Data Processing of personal data allowed?

(GDPR, article 6) says that data processing is allowed under the following circumstances:

(a) consent [...] for one or more specific purposes; children should have consent from the holder of parent responsibility (art. 8)
(b) …necessary for the performance of a contract to which the data subject is a party;
(c) …a legal obligation to which the controller is subject;
(d) to protect the vital interests of the data subject or of another natural person;
(e) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special categories of personal data

Special care should be taken when processing of certain special categories of personal data, as described in article 9. These special categories are: data: ["revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"]. Processing of data within one or more of these categories is strictly prohibited, unless one or more of the legal grounds for processing such data (article 6.2a-j, 6.3, 6.4) are applicable.

Principles

The processing of personal data needs to meet six important principles:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality

A seventh, often overlooked principle is accountability: you must be able to show that you comply with the aforementioned principles.

Impact

By working accordingly to these principles both the controller and the processor need to provide the following rights of a person when processing personal data:

- Provide the data subject with transparent information, communication and modalities for the exercise of his/her rights (art 12)
- Provide information as to where the personal data are collected (art. 13)
- Provide extra information if the personal data has not been obtained from the data subject (art 14)
- The right of access to the personal data by the data subject (art. 15)
- The right of rectification and erasure of the personal data of the data subject (art. 16, 17)
- The right to restriction of processing (art 18)
- The right to notification regarding rectification or erasure of personal data or restriction of processing (art 19)
- The right to data portability (art 20)
- The right to object and automated decision-making, including profiling (art 21, 22)

Recording of processing activities

According to article 30 each controller should maintain a record of processing activities that are performed under its responsibility containing at least the following aspects:

- Contact details of the controller
- The purposes of processing
- The categories of recipients to whom the personal data will be disclosed (including recipients in third countries or international organisations)
- Transfers of personal data to third countries or international organisations, including documentation of suitable safeguards
- The time limits for erasure of the different categories of data
- A description of the categories of the personal data
- A general description of the technical and organisational security measures that are taken

The processor should maintain a record of all categories of processing activities carried out on behalf of the controller:

- Contact details of the controller(s) the processor is working for as well as his own contact details, and the data protection officers at hand
- Categories of processing carried out on behalf of each controller
- Transfers of personal data to a third country or international organisation, including documentation of suitable safeguards
- A general description of the technical and organisational security measures that are taken

Organisations employing less than 250 persons do not have this obligation to register processing activities unless:

- They process data that is likely to result in a risk to the rights and freedoms of the data subjects, or
- The processing is not occasional, or
- The processing includes special categories of data as referred to in article 9 and 10 GDPR.

Governance

RACI

According to the GDPR the responsibilities regarding personal data need to be clearly defined in an organisation. A privacy compliance framework is helpful defining who is Responsible, Accountable, who should be Consulted and who should be Informed ('RACI'). This is done by drawing a matrix (RACI-chart) pointing out which processes are at hand and which positions (CEO, HR, Legal, Finance, IT, users) perform a RACI role. Clear responsibilities and authorizations should be in place regarding access and processing of this data. This is also of help by generating strong engagement within the organisation to comply with the GDPR.

Before using the RACI chart the organisation needs to have a clear inventory of the external and internal personal data flows and where Personal Data is being stored and processed in the organisation or outside the organisation. The data processing needs to be described and risks need to be defined.

Organisations need to proof that they continuously monitor these risks and acted accordingly to it using accurate and appropriate technical and organisational measures, to protect the data against unauthorized or unlawful processing, destruction, accidental loss or damage, focusing on integrity and confidentiality.

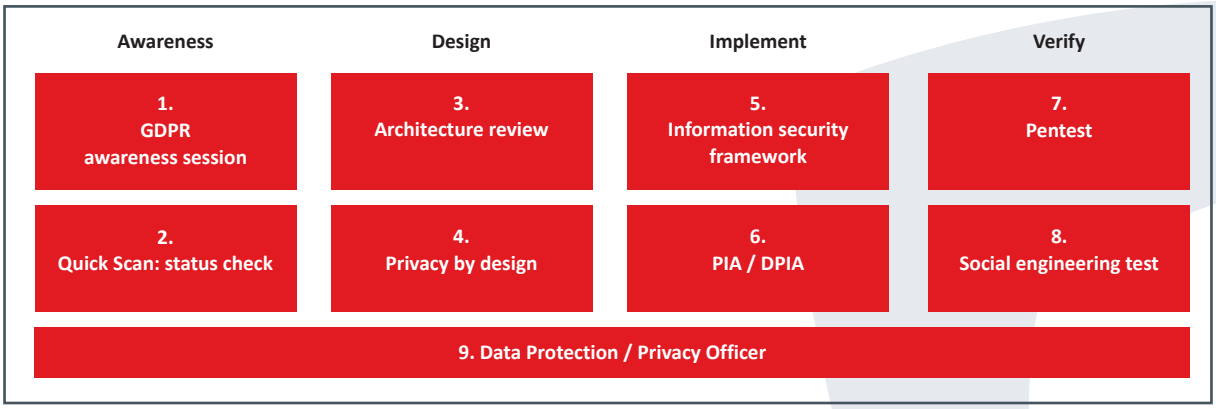
Data protection officer

In some situations, it is compulsory to appoint a Data Protection Officer (DPO):

- Public authorities or -bodies that process personal data
- If a controller or processor conducts processing activities as core activity by virtue of their nature, scope and/or purpose that require regular and systematic monitoring of data subjects on a large scale
- If a controller or processor conducts processing activities on a large scale of special categories of data:
  - Relating to criminal convictions and offences referred in in article 10 GDPR
  - Relating to processing of data revealing racial or ethic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data of the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation.

The definition of 'large scale' depends on:

- the number of data subjects involved
- the volume of data and/or angle of different data items being processed
- the duration, or permanence of the data processing activity
- the geographical extend of the processing activity.



Risk Management & Impact Assessments

In order to prove that the level of protection is continuously monitored and improved organisations need to conduct regular Data Protection Impact Assessments (DPIA) or Privacy Impact Assessments (PIA) if the activities are considered 'high-risk'. They should also perform these assessments to 3rd parties (processors) involved in the processing of personal data conducting Due Diligence into processors suitability and ensuring the GDPR compliance. It is therefore that the organisation needs to have clear Processing agreements (laid down in either contract or other legal act) in place with 3rd parties that handle these personal data in compliance with the GDPR. If personal data is transferred outside the European Union the joint controller(s) and/or processor(s) outside the European Union must ensure compliance to the GDPR and appoint a representative located within the European Union.

Incident Reporting

In case of a data breach or incidents there needs to be an incident policy and clearly described procedures. All incidents should be registered and analyzed to improve the processes involved. Data breaches need to be reported within 72 hours to the regulating authority. If there is a serious risk at hand that data subjects might be harmed in their interests the data subjects involved should be informed as well.

Conclusion

The impact of the GDPR is high for organisations handling (large quantities of) personal data. Most organisations, processes and systems today have not been designed to protect these data sufficiently and to ensure that these can only be accessed by authorized people. This means quite some changes need to be made.

Towards the future, the GDPR leads to a different way of designing and developing these processes and systems: Data should be protected by design and by default (GDPR Article 25)!

Secura is a professional partner who can support your organisation to comply with the GDPR. Please contact us for our GDPR service offerings as shown in the figure above. Professional compliance mitigates the risk of a data breach incident and generates customer value!

Secura

ADVISORY & AUDIT | SECURITY TESTING | CERTIFICATION SERVICES | TRAINING & AWARENESS

Secura B.V.
Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T + 31 (0)40 23 77 990
E sales@secura.com
W www.secura.com

Follow us on
@secura