WHITE PAPER

The EU General Data Protection Regulation (GDPR):
What it is and what you need to do

STIBO SYSTEMS
MASTER DATA MANAGEMENT

GDPR

All companies involved in processing personal data of EU citizens have to meet legal requirements. The aim is to strengthen the individuals' right to data protection and to make the processes around the data simpler for organizations. However, achieving compliance with the General Data Protection Regulation (GDPR) is anything but simple.

This white paper will give you an introduction to the requirements as well as tools to get your organization started. You will learn what the consequences of the GDPR are for your organization and how you can meet this challenge in the most effective way.

What is the GDPR?

Regulation of personal data protection isn't new. Since 1995, the European private sector has been covered by national (and in some countries state or provincial) information privacy laws. These have been based on the European Union framework directive, Directive 95/46/EC (the Data Protection Directive) and supplemented by Directive 2002/58/EC (the ePrivacy Directive).

But due to fast-moving technology and transformed indiviual and business behaviors, the old directive is outdated and was therefore replaced with the General Data Protection Regulation (REGULATION (EU) 2016/679) also referred to as the GDPR. The regulation has completely changed the groundworks for how organizations can manage personal data of EU citizens, and this of course has significant consequences for the affected organizations.

The GDPR was adopted 27 April 2016 and entered into application on 25 May 2018.

Who does it affect?

The GDPR affects any business that collects and uses data from European citizens regardless of whether that organization is established in the EU or not or if the processing itself takes place in or outside of the EU.

What's the difference between a directive and a regulation?

A **directive** is an act that sets a target which EU countries must achieve. However, it is up to the individual member states to make their own national laws to achieve this target.

A **regulation** – such as the GDPR – is a binding act. It must be followed in its entirety throughout the EU.

What has changed?

- Data Protection Officers
- Breach notification
- Data transfer
- Wider geographic scope
- Consent
- Privacy by design
- Right to erasure
- Fines

The regulation has completely changed the groundworks for how organizations can manage personal data of EU citizens

What are the most important requirements?

The eight most significant requirements that organizations need to comply with:

1. Personal data breaches must be reported to your local supervisory authority* within 72 hours[1]. If the personal data breach also represents a high risk to the data subject*, the controller* shall communicate the personal data breach to the data subject without undue delay.
2. A data protection officer (DPO) must be appointed for all public authorities, and where the core activities of the data controller or the processor* involve "regular and systematic monitoring of data subjects on a large scale" or where the entity conducts large-scale processing of "special categories of personal data"[2].
3. Indiviuals have several rights, the most important being the **right to be forgotten**[3] – the organization will have to delete all the data of an indiviual requesting this. The **right to object**[4] – indiviuals can say no to certain data use such as profiling for marketing purposes. The **right to rectification**[5] – indiviuals can have incomplete data completed. **Right of access**[6] – indiviuals have the right to know what data is being processed and how. And the **right to data portability**[7] – indiviuals can transmit their data from one organization to another without hindrance.
4. Indiviuals have the right to receive "fair and transparent" information about the processing of their data, among other things:
   - Contact details of the data controller and the data protection officer
   - Use of the data, e.g., details of data transfers outside of the EU
   - Purpose of the data – this must be as specific and minimized as possible (purpose limitation* and data minimization*)
   - The retention period for the data – this period must be as short as possible (storage limitation*)
5. Organizations must adopt a constrained consent protocol:
   - Consent from the data subject must be specific to distinct purposes
   - Silence, pre-ticked boxes or inactivity does not constitute consent
   - Organizations processing personal data of children under the age of 13 must collect consent from the child's parent[8]. For children between 13-15 years (both included), member states set individual rules.
6. The definitions of personal and sensitive[9] data have expanded, for instance does the latter include genetic and biometric data.
7. Organizations must consider data privacy at the initial design stages of a project (Privacy by default) as well as throughout the lifecycle of the relevant data processing (Privacy by design[10])
8. The controller is responsible for implementing appropriate technical and organizational measures to ensure and to demonstrate that its processing activities are compliant with the requirements of the GDPR[11].

* Find the definition in the glossary pages 6-8

Diving deeper into the regulation

Whether you're based in Hamburg, Beijing, Atlanta or Sydney, the GDPR will most likely affect your company. Even if your organization isn't located in the EU or if the data processing itself takes place outside of EU, you will need to be in compliance if you are systematically collecting, storing or processing personal data of EU citizens.

Even organizations that don't fall under the GDPR will indirectly be affected since data privacy and protection is increasingly becoming a competitive factor. A survey from Symantec showed that 88% of European indiviuals consider data security to be the most important factor when choosing a company and 86% think the protection of their data is more important than the product quality[12]. Adopting the GDPR principles is recommended, no matter what, in order to guarantee a minimum of data protection.

What is personal data?

As opposed to the former directive, the GDPR enforces a strict definition of personal data as any information that could be used, on its own or in conjunction with other data, to identify an individual. This mean that even a phone number stored on its own or a social media ID without an associated name or address may fall under the regulation and needs to be properly protected.

When are you processing data?

The GDPR considers "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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"[13].

Responsibilities of controllers and processors

If your organization was considered a controller under the old directive it will most likely also be under the GDPR. The definitions of controller and processor have not changed but their responsibilities have extended, which means that while the old directive laid the main data protection responsibility on the controller, the GDPR also places direct obligations on the processor.

What's the difference between a controller and a processor?

An organization working with personal data will do so as either a controller or a processor.

A **controller** is the organization that determines the purposes and means of the processing of personal data. If the controller processes the data itself, it will still be considered the controller. Online retailers will for instance fall under this category (as will the majority of businesses).

A **processor** is someone outside the controller organization processing the data on behalf of the controller. Examples of typical processor companies include payroll companies, accountants, market research firms and most cloud providers.

The controller has the primary data protection responsibility. Controller organizations are legally responsible for reporting personal data breaches to their supervisory authority. They will also have to demonstrate to authorities upon request that a data subject has consented to processing of his or hers personal data.

Additionally, the controller must provide the needed information to the data subject if this is requested by the data subject. This needs to be delivered at the latest one month after the request. Furthermore, this information must be provided in a "structured, commonly used and machine-readable format" and the data subject actually has the right to transmit the data to another controller, meaning that an unsatisfied customer of yours can request their data – including metadata – deleted from your systems and transferred to a competitor.

If a controller is to use a processor, they need to make sure they choose one that has implemented appropriate technical and organizational measures so that the processing ensures the protection of the personal data.

The GDPR enforces processors to maintain a record of all categories of processing activities and to provide the record to the supervisory authority on request. They're also required to notify their relevant controller of any breach or to inform the controller if they have reason to think that an instruction is illegal. The processor is not allowed to use another processor without prior specific or general written authorization of the controller.

Consent collection and right to detailed information

Collecting and proving valid consent is one of the several challenges presented by the GDPR.

Hence the "Privacy by default and design" principle, the protection of personal data must not be an afterthought but be part of any project right from the start. This is also underpinned by the fact that businesses are not allowed to change the use of the data from the purpose for which it was originally collected, meaning that "'one-consent-for-all" cannot be valid. Separate consent is required for different processing activities, which means that organizations must be clear about the purpose of the data when collecting consent the first time to avoid having to do it again at a later stage.

The protection of personal data must not be an afterthought but be part of any project right from the start

Organizations are only allowed to collect the data that is necessary for its purpose, meaning that organizations must carefully consider and be able to validate why they are collecting and storing the data they are. Data such as name and address can easily be justified, but what about social ID, phone number, income, working title?

Why is that relevant? Your business needs to carefully consider the data it collects and why.

Silence or inactivity from the indiviual does not constitute consent, and pre-ticked boxes are banned. The data subject

Controller organizations are legally responsible for reporting personal data breaches to authorities

has to explicitly opt-in to the storage, use, and management of their personal data. And if you are collecting and processing data of children you need to collect consent from their parent or guardian. Without valid consent or not being able to demonstrate it properly, any personal data processing activities will be shut down by authorities immediately and economic sanctions will follow. However, the most damage will without a doubt be the brand damage, resulting in your customers losing trust in your organization.

On top of the more strict consent procedure, indiviuals have the right to receive information about what data the controller is collecting and how it is processed and used. Furthermore this must be done in "a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child"[14].

Organizations can only store the data for as short a period as possible. The expected duration of the storage will have to be communicated to the data subject. The data subject also needs to receive contact information on the data controller and the identity of the data protection officer. Data subjects can object to certain types of processing – profiling for marketing purposes, for example, and organizations must delete or change all data – including metadata – at the request of the data subject.

Not complying will result in huge fines. Sanctions for offences relating to control and mitigation can be up to 10 million Euros or 2% of the total worldwide annual turnover while offences relating to rights and obligations can be as high as 20 million Euros or 4% of turnover.

What do you need to do?

As laid out, the GDPR poses requirements to policies, processes, strategies and even systems. These are time-consuming actions you need to take to be compliant.

5 steps to get you going

1 Get board and top-management level buy-in. There are two main aspects in this. First of all, make sure the allocated budget is big enough so there are no surprises. This will not be a cheap exercise but the investment will be well spent. Secondly, make sure board/management is truly committed to this. The compliance effort must have a holistic company-wide approach to be successful. Your strongest argument for the buy-in will be the economic sanctions if you do not meet the GDPR as well as the potential brand damage if you do not prioritize data protection.

2 Choose a person – or even better – a team, representing different business units, that will be dedicated to the GDPR project. Have them educate themselves thoroughly on the GDPR. If you're required to hire a data protection officer according to the GDPR, do it now, as that person can help guide your team.

3 Have your GDPR team create an enterprise data landscape map in collaboration with different parts of the organization, as the relevant data is probably scattered across different departments and systems. You need to identify: Are we data controllers or processors? Where does the affected data reside? Who has access? Who is responsible for the quality of it? What is the data used for? And also: How do we communicate how we use the data to the data subjects? What does our data protection policy say? How do we train employees to handle personal data?

4 Now, combine that data map with GDPR expertise. This forms the basis for auditing the policies, processes and procedures to reveal any non-compliant areas. Once you've identified these areas in a gap analysis, you can create an action plan prioritized according to risk. There will be areas where you and your team do not have appropriate capabilities or systems, leading to step 5:

5 Hire external help for the parts that you cannot do internally.

How can master data management help?

The single customer view is becoming increasingly desired by organizations since it helps them create the best possible customer experiences. With the GDPR, the single customer view becomes even more relevant. Master data management helps organizations achieve this.

A master data management (MDM) solution breaks down departmental data silos and integrates the master data into a single, complete source of trusted data. These golden records or single customer views eliminate out-of-date, incomplete or conflicting sources of data. Furthermore, MDM secures smooth data workflows and enables data governance.

"Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay[15]"

All of which is essential for complying with the GDPR.

MDM creates one single entry to the personal data. That way, organizations will always be able to identify and lay out the relevant data which is needed, e.g., when data subjects request their data, and when demonstrating compliance towards authorities. MDM also ensures that organizations have the technologies and processes in place that will enable them to detect and respond quickly to a data breach if this should happen.

"The controller shall implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary[16]"

Being compliant all comes down to your data quality, your data processes and the organizational data governance. MDM lays the foundation for your compliance with the GDPR. It provides a platform from which your organization can store, manage, collect and share trusted data about individuals – customers, prospects, and employees.

You can find the entire General Data Protection Regulation **here**.

[1] GDPR, 2016/679, Chapter VI, Section 2, Article 33(1)

[2] GDPR, 2016/679, Chapter IV, Section 4, Article 37-39

[3] GDPR, 2016/679, Chapter III, Section 3, Article 17

[4] GDPR, 2016/679, Chapter III, Section 4, Article 21 (1-3)

[5] GDPR, 2016/679, Chapter III, Section 3, Article 16

[6] GDPR, 2016/679, Chapter III, Section 3, Article 15

[7] GDPR, 2016/679, Chapter III, Section 3, Article 20

[8] GDPR, 2016/679, Chapter II, Article 8

[9] GDPR, 2016/679, Chapter II, Article 9

[10] GDPR, 2016/679, Chapter IV, Section 1, Article 25(1-3)

[11] GDPR, 2016/679, Chapter IV, Section 1, Article 24(1)

[12] http://www.itpro.co.uk/data-protection/27428/90-of-businesses-think-its-too-hard-to-delete-customer-data

[13] GDPR, 2016/679, Chapter I, Article 4(2)

[14] GDPR, 2016/679, Chapter III, Article 12(1)

[15] GDPR, 2016/679, Chapter II, Article 5(d)

[16] GDPR, 2016/679, Chapter IV, Section 1, Article 24(1)

Glossary

Term	Definition
Children, data	Data of children under 13 years must only be processed if consent is given or authorized by the holder of parental responsibility over the child. As for data of children between 13 and 16 years, the member state decides if the child can give consent themselves or if it is needed from a parent.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
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.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Data subject	The data subject mentioned in the GDPR is the person whose data is being collected and/or processed.
Directive	A directive is an act that sets a target which EU countries must achieve. However, it is up to the individual member states to make their own national laws to achieve this target.
DPO/Data protection officer	The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this regulation. The DPO's most important tasks are: to monitor compliance with the GDPR and to cooperate and act as the contact point for the supervisory authority.
Employee	The data of your employees is considered personal data and your employees will therefore have the same right to object and access their data as any indiviual and you will need to collect consent as per the GDPR. However, The GDPR authorizes individual member states to implement more specific rules in respect of the processing of employee data, meaning that national rules will still be lawful.
Minimization (data minimization)	Personal data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
PIA (Privacy Impact Assessment)	The GDPR requires data controllers to conduct PIAs where privacy breach risks are high to minimize risks to data subjects.

Term	Definition
Personal data	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.
Privacy by design	The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization and data minimization.
Privacy by default	The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed (amount of personal data collected, the extent of their processing, the period of their storage and their accessibility). In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of persons.
Processing	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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. The data subject has the right not to be profiled.
Purpose limitation	Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Right to data portability	The data subject shall have 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 have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.
Right of access by the data subject	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the purpose.

Term	Definition
Right to be forgotten/ Right to erasure	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.
Right to rectification	The data subject shall have the right to obtain from the controller the rectification of inaccurate personal data concerning him or her (the right to have incomplete personal data completed).
Right to object	The data subject will have the right to object at any time to processing of personal data concerning him or her for marketing, which includes profiling.
Transfers	A transfer of personal data to a third country or an international organization may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization.
Regulation	A regulation – such as the GDPR – is a binding act. It must be followed in its entirety throughout the EU.
Sensitive or special categories of data	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation is only allowed if the data subject has given explicit consent or it is needed to protect the data subject, for archiving purposes or is in the interest of the public.
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
Supervisory authority	Each member state shall have a supervisory authority (one or more independent public authorities) to be responsible for monitoring the application of this regulation.
Withdrawing consent	The data subject has the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.