DocuWare

White Paper
GDPR

This document was created using AuthorIT™, Total Document Creation (http://www.author-it.com).

Disclaimer

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by DocuWare GmbH. DocuWare GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

DocuWare GmbH
Therese-Giehse-Platz 2
D-82110 Germering
www.docuware.com (http://www.docuware.com)

DocuWare

Contents

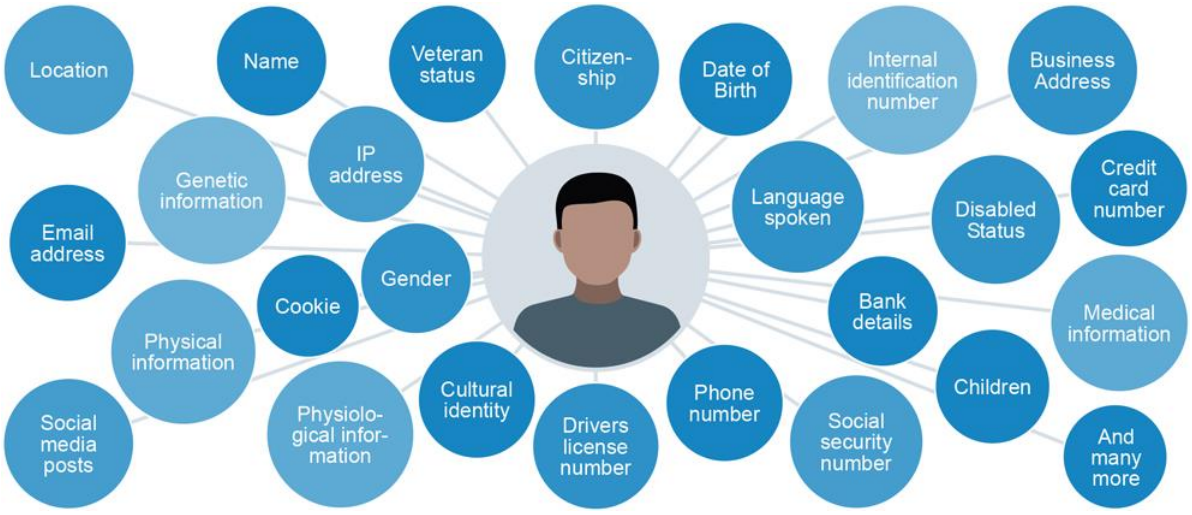
1 Complying With EU GDPR Is a Must

GDPR, or General Data Protection Regulation, is a new set of European rules and standards related to privacy and data governance. It is not just for European companies, but for any company doing business in Europe or with European customers. The regulation requires the active consent of customers and gives them new portability powers to control the transfer of their own information. It sets up significant penalties for non-compliance. All of this goes into effect May 2018.

There is a temptation to assume nothing in GDPR is critically different. After all, Europe has had data governance and data protection regulations since 1995. But GDPR is a set of principles that have been placed at the highest priority level and require every organization's attention.

The six GDPR principles

At its core, GDPR is all about the protection of personal data or personal identifiable information (PII). Personal data can be any information which allows someone, directly or indirectly, to identify another natural person. This includes information like names, email addresses, social media posts, physical, physiological, or genetic information, medical information, locations, bank details, IP addresses, cookies and cultural identity.



This protection is established in six principles:

1 Processed lawfully, fairly and in a transparent manner.

2 Collected for specified, explicit and legitimate purposes.

3 Adequate, relevant, and limited to what is necessary.

4 Accurate and, where necessary, kept up-to-date.

5 Retained only for as long as necessary.

6 Processed in an appropriate manner to maintain security.

You must not only comply with the six general GDPR principles, but also demonstrate your compliance through documentation and/or standard operation procedures (SOPs) regarding data protection.

The important facts you need to know

1 **GDPR is an EU Regulation that overrides everything else:** Unlike the previous EU Directive on data privacy, the new GDPR is an EU Regulation. This means it becomes immediately effective 25 May 2018 after a two-year transition period and, unlike a Directive, it does not require any enabling legislation to be passed by national governments. As any EU regulation, GDPR is like a European law. It overrides the national laws and all previous EU directives.

2 **High penalties:** The penalties for non-compliance are significant. Fines can be imposed up to 20m Euro or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83: General conditions for imposing administrative fines)

3 **Explicit customer consent:** Valid consent must be explicit for data collected and the purposes data is used for (Article 7; defined in Article 4). In addition, data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn.

4 **Complying outside the EU:** The old escape clauses for non-European companies no longer work. Non-European companies utilized “Safe Harbor” provisions to comply with the original data protection regulation. In July 2000, the European Commission (EC) decided that US companies complying with the principles and registering that they met EU requirements could transfer data from the EU to the US. But the international Safe Harbor Privacy Principles were overturned on October 24, 2015 by the European Court of Justice after a customer complained that his Facebook data was insufficiently protected.

5 **Personal data can be almost anything:** Managing unstructured information and documents are key to compliance. According to the European Commission, “Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life.” The Commission notes, “It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.” Companies must be able to identify **any place or document** containing personally identifiable information and be able to provide an index of that PII data to the customer if requested – an impossible requirement without a content management system.

6 **Paper documents are included:** GDPR applies to the processing of personal data wholly or partly by automated means. Even more important: It also applies to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. (Article 2: Material scope)

7 **Extended chains of liability:** If personal identifiable information is being stored or handled by a cloud services provider or a document process outsourcer on your behalf, you retain responsibility for the data governance practices of your outsourcers.

Know who you are: data controller or data processor or both

There are five terms or roles you should have heard of in conjunction with GDPR: data subject, data controller, data processor, data protection officer and data protection authority.

- A **data subject** is a natural person. He or she can be a client or an employee of a company, a user of a social media platform or other. The role of the data subject can be compared with the legal concept (or term) of the owner, in this case, of data. Any citizen is meant: "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data." The data subject has several rights to obtain information on what PII is stored and processed, to get them corrected or even deleted and to transfer them to another company. The role of the data subject can be compared with the legal concept (or term) of the owner, in this case, of data.
- A **data controller** "means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". The role of the data controller can be compared to the legal concept (or term) of the possessor.
- A **data processor** is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

Your company can be a data controller or a processor or both. Your customers, clients, prospects and suppliers can all be controllers and processors as well. And your customers, clients, prospects, employees and freelancers are all data subjects, as well as the analog groups of your partners are.

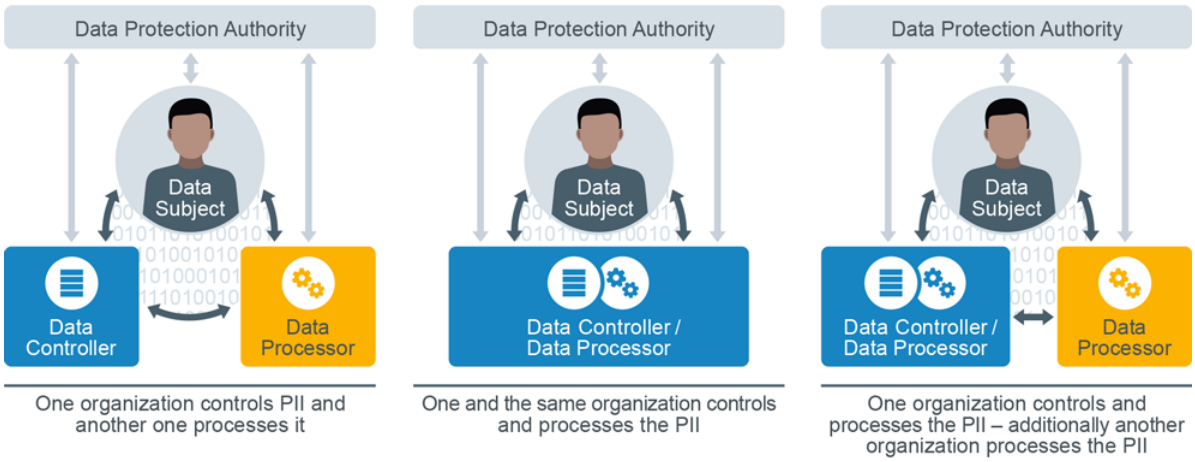
Article 4: Definitions

Both controllers and processors must build security into products and processes from day one. If not yet done, all controllers and processors must appoint a **data protection officer** (DPO) who is also liable if you are:

- processing PII of more than 5000 data subjects per year
- a governmental organization or agency
- mainly processing special categories of data
- performing regular observation on a large scale

Article 37: Designation of the data protection officer

Each EU Member State provides for one or more independent **data protection authorities** (DPA) to be responsible for the monitoring of the private sector.



Who can complain and where?

With GDPR, not only a person can lodge a complaint. He or she can also mandate a not-for-profit organisation, e.g., a consumer protection association, to do so on his or her behalf.

Article 80: Representation of data subjects

A lawsuit is filed in the courts of the EU Member State where the controller or processor has an establishment (One Stop Shop-Principle, OSS). Alternatively it can be the courts of the Member State where the requesting person or data subject has his or her habitual residence.

Article 79: Right to an effective judicial remedy against a controller or processor

2 How DocuWare Helps You Comply With GDPR

Any email, file, paper, note or a document containing PII is a personal data. That means, it must be stored, managed, protected and controlled in accordance with GDPR.

While the GDPR is quite clear on the level of protection required for personal data, it doesn't spell out the processes or technologies companies should use to ensure that protection. In fact, it's unlikely that one single system can meet every facet of the regulation. Compliance will require a coordinated technology and policy effort.

One important technology is a document management system that not only digitizes paper records, but takes advantage of metadata to enforce the security and governance required to protect customer data.

With its control-centric approach, DocuWare directly supports your GDPR compliance projects. For example, file cabinets in DocuWare can be easily set up to prevent downloading, forwarding or printing documents. This does not require programming, coding and lengthy implementation – it's there as a basic feature.

2.1 Find and access personal data

If a person asks you what personal data of him or her is processed in your company, you must first **locate the personal data**. Yet, since GDPR applies to **paper** records stored by a business as well, this can be easier said than done in case you are still managing processes on paper.

How DocuWare aids your compliance

With DocuWare, all your documents are digitalized and stored in a secure system, so that you easily **find and access all personal data** in your documents. They can be emails, contracts, invoices and so on. DocuWare can automate the process of storing, finding, locating, exporting and deleting PII.

That makes this process independent from individuals. Instead it applies corporate data governance policies. The automated approach to protecting PII brings order, consistency and efficiency to your business processes and makes you faster and easier comply with GDPR requirements. The DocuWare team supports you in setting up a digitalization strategy for your paper records.

Metadata plays a key role in complying with GDPR by correctly classifying, categorizing and describing PII according to the regulation's requirements. A basic example would simply be searching by document types (contracts, invoices, correspondence) that you know contain PII.

DocuWare Intelligent Indexing uses machine learning and artificial intelligence (AI) to automate this classification process, supporting compliance but relieving your team of complicated and lengthy data entry.

Once a document is indexed, DocuWare can automatically initiate other actions to ensure proper treatment and handling of information, such as:

- Encrypting all files and objects that contain PII, both during transmission and while at rest
- Applying access control and permission management, to ensure only authorized users can access PII. For example, customer service representatives may be able to view customer purchase orders, but not marketing teams
- Enforcing rules around retention and deleting, to ensure data isn't kept longer than necessary
- Preventing documents containing PII from being inadvertently or intentionally emailed or otherwise transferred outside of the organization
- Tracking any modifications to PII documents, to show who changed what, and when
- Providing an audit trail to prove only authorized employees had access to customer PII

Automating this approach to protecting PII brings order, consistency and efficiency to the task, while applying corporate-level data governance policies.

2.2 Gain the ability to export, correct and delete personal data

If asked about PII, you must be able to **export** the personal data to show to the requestor. This can also enable this person to transfer his or her data in a „commonly used and machine-readable format" to another vendor or service provider.

You must provide a copy of any personal data undergoing processing at no charge the first time it is requested. Plus, you must do so within 30 days.

If your company holds inaccurate personal information, you must **correct** these data on request without delay. If someone wants his or her data to be **deleted**, you must do so as well - according to the right to be forgotten. You can only decline an erasure request because of compliance with a legal obligation, public interest or legal claims.

How DocuWare aids your compliance

Any inquiry to export, correct or delete personal data can be stored in DocuWare and can automatically trigger an appropriate workflow especially designed for exporting, correcting or deleting the PII. The workflow tasks can be automatically distributed to the data protection officer (DPO) who will be taking decision if such query is justified.

Due to its Request module, data portability is an “out of the box” DocuWare feature. You can easily **export and transfer** all PII.

Article 20: Right to data portability

The DocuWare viewer ensures that all document changes made in the viewer are stored as overlays to the document. So you can export an invoice containing a customer's PII without the release stamp and PII of one of your employees.

Workflow tasks can be distributed to the data protection officers (DPO). They will be either updating data holds in the different systems on their own or distributing the tasks to appropriate colleagues. The DPO can easily **access all records** about the data subject and mark them for deletion. Or a DocuWare workflow automatically triggers such actions once the DPO has been confirming that the request was justified.

To **correct** all concerning data, the metadata stored in DocuWare can be automatically or semi-automatically updated as a part of these processes. This ensures consistency between systems and furthers your GDPR compliance.

If required, DocuWare can **delete both documents and metadata**. DocuWare can even open third-party applications, simplifying such tasks. DocuWare can inform the data subject automatically that data is due for deletion and establish a schedule for disposition.

DocuWare keeps the complete **history** of data rectification queries. When a person's request is not justified, DocuWare can help the DPO send automatic response to the requesting person with explanation why it’s **not justified** and why the company will process his/her data longer. The request data will be kept for a required period and automatically disposed of at the end.

2.3 Ensure that personal data is protected and not further processed

On request, your company must be able to **exclude personal data from future processing activities** - either temporarily or permanently. The conditions include contested data accuracy, unlawful processing, and the desire of the data subject to be excluded from processing activities but to not have their personal data erased for various legal and historical reasons.

Article 18: Right to restriction of processing

How DocuWare aids your compliance

DocuWare enforces rules around retention and deleting to ensure data isn't kept longer than necessary. By setting up automatic retention schemes, you can easily prevent documents containing PII from being inadvertently or intentionally emailed or otherwise transferred outside of the organization. This does not require any coding or programming. It's part of the basic configuration available to administrators or DPOs.

On top of that, every modification to PII documents is tracked to show who changed what, and when. With flexible and secure rights management, only authorized employees can access the customer PII; to prove there was no unauthorized access, the system provides an audit trail.

Thus, DocuWare largely takes decisions about how to handle PII out of the hands of individual employees and instead applies corporate-level data governance policies.

3 Define a Company-Wide Strategy for Compliance

Using a document management system like DocuWare is a big step toward complying with GDPR. However, your company also uses other software that processes personal data like a CRM, marketing system, ERP, and others.

To handle personal data across all systems, define a consistent strategy. In your CRM, for example, you should also be able to find, access, correct, export, protect and delete personal data – as well as maintain a record of these processing activities.

Keep your records current

Whether with your document management system, CRM or ERP, if you act as a data controller, your DPO is guaranteeing compliance and therefore must keep a record of the following information:

- your name and contact details and, where applicable, any joint controllers, representatives and data protection officers;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients, including recipients in third countries or international organizations;
- details of transfers of personal data to third countries (where applicable);
- retention periods for different categories of personal data (where possible); and
- a general description of the security measures employed (where possible).

If you engage a data processor, you must contractually ensure that THEY maintain a record of all categories of processing activities on behalf of a controller.

Article 30: Records of processing activities

And not to forget: Carry out a risk assessment and a data protection impact assessment in accordance with Article 35. A Bitkom guide helps you get started.

Further Information

GDPR with table of contents and quick search
Ebook "Information Privacy and Security" by the industry association AIIM
A GDPR To-Do List by attorney Rolf Becker, Cologne
GDPR download in all EU languages