# DocuWare Configuration Tips for GDPR-compliant Working

DocuWare GmbH
Therese-Giehse-Platz 2
D-82110 Germering
www.docuware.com

# Contents

# Introduction

The EU General Data Protection Regulation (GDPR) came into force on May 25, 2018 and is all about the protection of personal data. This includes all information that enables someone to directly or indirectly identify another natural person. It might be someone's name, email addresses, phone numbers, social media profiles, medical data, and lots more.

Companies and organizations have the right to process personal data if one of the six reasons as specified in Article 6(1)(a–f) GDPR applies to their particular case – and as long as this data is needed for a specific purpose. These reasons are:

1. Consent
2. Fulfilment of a contract
3. Legal obligation
4. Vital interests
5. Task in the public interest/for official functions
6. Legitimate interests.

Unless there is any other reason for the legal processing of personal data, you should create a concept for data subject consent. You should store the individual consents with a DocuWare index criterion, for example "Data processing consent," in DocuWare so you can locate them as needed.

As a document management and workflow system, DocuWare helps you to establish GDPR-compliant handling of personal data and implement it on a permanent basis.

It is recommended that you first read the DocuWare White Paper GDPR as a basis for the configuration steps suggested here. The paper provides detailed information on the requirements of the regulation.

The following procedures and settings are basic recommendations, which you can apply to your documents and processes. Slight adjustments may be necessary depending on your data protection strategy and use of DocuWare.

These tips are based on the following concept:

1. All documents archived in DocuWare are classified by types.
2. Each document type gets a "Retention period" index criterion.
3. Each new and archived document is indexed with the appropriate retention period.
4. You set up various GDPR statuses for all documents and you regulate the four-eyes principle and deletion of documents after the retention periods have elapsed.
5. The access rights of employees to the various types of documents are restricted in accordance with GDPR.

In addition, you will learn how to restrict the processing of personal data in DocuWare and how to correct and make personal data available for transfer. Finally, we will show you how to use DocuWare to set up a process for data access or data copies.

DocuWare Cloud includes all functions for the steps suggested here. If you work with DocuWare On-Premises, you will need the additional licenses Task Manager, Autoindex, and DocuWare Forms.

Before you process and answer a request about the storage or processing of personal data, you should always check the legality of the request and the identity of the requesting person. For details, please refer to the Guidelines on the right to data portability of the European Commission (p. 13: "How can the data controller identify the data subject before answering his request?").

DocuWare accepts no legal responsibility for GDPR-compliant handling of personal data in DocuWare.

## Classify your documents by types

A consistent classification of your documents by type is the basis for implementing with DocuWare the lawful handling of personal data as defined in Article 6 GDPR. Different legal retention periods and access rights can be defined depending on the document type.

DocuWare Configuration > File Cabinets > Database Fields:

Define a "Document Type" (type: text) database field in each file cabinet. Depending on the file cabinet and the documents contained in it, the user will then see different entries in the selection list of the index field. Enable the "Required" option.

DocuWare Configuration > Indexing Help:

Create a fixed selection list that contains all document types that are required for the relevant file cabinet, for example for HR "Application," "Employment Contract," Sick Note." Your employees will then be able to select the correct document type when storing new documents.

*Inventory data:*

If your documents already archived in DocuWare are not classified according to document types, you can do this with Autoindex. For document type "Invoice," you can specify that whenever the document has an invoice number as an index entry, the index entry for the document type is filled with "Invoice."

## Create an index criterion "Retention period" for document types

There are legally regulated retention periods for all types of business documents. Information on this can be found on the websites of institutions such as the chambers of commerce, the ministries of Economics, the ministries of Finance, (for EU companies' invoices) in the brochure EU Compendium. Or you can get this information from tax consultants and industry advisors. A chargeable "Deletion concept guideline" by the German Institute for Standardization (DIN e.V.) is available here (DIN 66398, Guideline for development of a concept for data deletion with derivation of deletion periods for personal identifiable information).

You store the retention periods relating to your documents in all your file cabinets per document type.

Configuration > File Cabinets > Database Fields:

Create a "Retention Period" database field of type "Date" per file cabinet in order to enter the retention period in a following step. You can also leave the field blank and fill it later using Autoindex.

## Index your documents with a retention period

Use Autoindex to add a retention period to all new and archived documents. You create a configuration for all documents that are newly stored or already archived.

Indexing with a retention period per document type essentially works by loading the value of the "Storage date" field with an SQL command and by also adding the corresponding retention period with an SQL command.

As a source for retention period values, use the file cabinet table as an external data source.

DocuWare Configuration > Autoindex

To add a retention period to your archived documents, create a configuration per document type and give it a separate name, for example, "Retention period stored invoices."

Instead of "File cabinet event" select "Scheduling." On this tab, create the following rules:

1. "Document type" | "equals" | <Document type, e.g. "Invoice">
2. "Retention period" | "is empty"

> tab "Index data" (source):

1. Enable "Index with external database."
2. Click "Configure data source."
   a. Configure data source:
      Connection: Select the database connection "Content" (On-Premises) or the GUID (DocuWare Cloud) of your organization.
   b. Enable "SQL command."
   c. Copy the following SQL command into the field:
      *SELECT DWDOCID, DATEADD(year, 10, DWSTOREDATETIME) AS DateAdd FROM <FileCabinetTablesName>*
      This command adds 10 years to the storage date. Adjust the number of years in accordance with the retention period for the relevant document type.
3. Click "OK."
4. Under "Matching field" select: "DWDOCID" | "equals" | "DWDOCID."

> tab “Assign data”:

1. Add a new entry: Retention period | Field | DateAdd
2. Enable "Overwrite" and "Even if empty."
3. Save the configuration.

You automatically start the configurations per document type with scheduling: On the "Trigger" tab, under "Scheduling," set the run time which does not fall within your business hours, as a larger inventory of documents requires longer for indexing.

For example, if you run the Autoindex jobs at 9 p.m. daily, a stored document is indexed with the retention period the next day.

## Index all documents with a GDPR status and regulate the deletion of documents

GDPR requires data economy, in other words documents with personal data must not be retained for longer than is justified under Article 6 GDPR. So you must regulate the deletion process of documents containing personal data and no longer being subject to a legal retention period (Article 17 GDPR). You have already established the basis for this by classifying the document type and by indexing each document with a retention period.

However, you should only delete documents that are due for deletion at the end of their retention period if one employee (two-eyes principle) or two employees (four-eyes principle) have released them manually. This is the only way to rule out mistakes.

In order to restrict access to documents whose legal retention period is still running (see "How to restrict the processing of personal data"), you need a GDPR status as an index criterion.

Configuration > File Cabinets > Database Fields:
Define a "GDPR status" database field per file cabinet of type "Text." Enable the "Required" option for the database field.

DocuWare Configuration > Indexing Help:
Create a fixed selection list with the following four entries:

1. Retention
2. Retention with restricted access
3. Check for deletion
4. Released for deletion

**1. Retention**

The retention period for the document is running and the document is normally available in the file cabinet.

For archived documents without a GDPR status, assign this status using Autoindex:

DocuWare Configuration > Autoindex > Start Condition > Scheduling:

Select the required file cabinet and run Autoindex once with the following setting: Select "GDPR status" and "Is empty" as the filter.

"Index Data/Source" tab:

Enable "Index with fixed index entries."

"Data Allocation" tab:

Select "GDPR status" and "Fixed entry" and enter "Retention" as a value.

### 2. Retention with restricted access

The retention period for the document is still running, but access to it is restricted to a minimum number of users who still need the document. This case occurs when a person has asked your company to delete personal information but the retention period has not expired.

DocuWare Client > Search:

In the case of a request, start a manual search for the documents and set them to GDPR status "Storage with restricted access." Restrict access to the documents using an index value profile.

### 3. Check for deletion

The retention period for a document has expired and it now needs to be manually released for deletion by two employees in accordance with the four-eyes principle.

First, create two roles for a first and a second auditor. The users of the "First auditor" role cannot be the same as the users of the "Second auditor" role. First and second auditors release the document for deletion with their own public stamps. A document can only be deleted with both stamps.

DocuWare Configuration > Autoindex > Start Condition > Scheduling:

Select the required file cabinet and run Autoindex daily with the following settings: Filter "Retention period" and "In the next 0 days."

"Data Allocation" tab:

Select "GDPR status" and "Fixed entry" and enter "Check for deletion" as a value. Enable "Overwrite."

DocuWare Configuration > File Cabinets > Dialogs > List > Details:

a. Create a list so that authorized employees receive the document via their role: Select "GDPR status" and "Equals" and enter "Check for deletion" as a value.
b. Create a second list for the second auditor role. This list looks for the status of the first auditor stamp (for example, "First check completed").
   The second auditor stamp writes "Released for deletion" in the GDPR status.

### 4. Released for deletion

The retention period has expired and the document has been released for deletion by the authorized first and second auditors by public stamp. In the background the GDPR status has changed to "Released for deletion."

The documents can either be deleted manually or you can set up a deletion rule to be applied as soon as a document has GDPR status "Released for deletion."

## Optimize your permission concept for accessing the document types

As a general rule, only grant employees access to the document types if they require access for specific task-related purposes. This particularly applies to all documents containing personal data.

DocuWare has a rights concept that can map complex scenarios. The scope of action can be defined in detail for each user. In order to handle the individual access right of individual employees on an independent basis, you should use profiles and roles wherever possible for assigning rights. DocuWare's Security White Paper provides comprehensive information about the various options for assigning rights for document access.

## Restricting personal data processing

If your company is requested to delete personal data and the documents concerned cannot be deleted on account of a legal retention period, you must at least restrict data processing (Article 18 GDPR). In other words, you must restrict access to the affected document strictly to those users who need the documents for specific business purposes.
Ideally, you have already done this when setting up DocuWare with your permission concept (see "Regulate access to documents with a clear permission concept").

Whereas the standard and user-defined profiles relate to the entire file cabinet, with an index value profile you make only specific documents accessible for a profile.

DocuWare Configuration > File Cabinets > Permissions > Advanced Settings > Index Value Profiles:

Create an index value profile by mapping access to documents with GDPR status "Retention with restricted access" only to the data protection officer (DPO) and to those employees who still need these documents for business purposes.

Now run a full-text search for the relevant documents. (You can also run the search across several file cabinets at the same time. However, the searching person or role needs extensive file cabinet rights.) In the result list, make the documents invisible to unauthorized groups by setting their status to "Retention with restricted access." The index value profile enables access only for a few authorized employees.

## Correcting personal data

If a person asks your company to correct personal data (Article 16 GDPR), you do this only in the document index data, also called metadata. You must not retrospectively edit personal data in the documents themselves because in most cases this would be a violation of the legal retention requirements.

You can amend the metadata as follows:

1. Search your file cabinets for the metadata that needs to be corrected. The corresponding documents will then appear in the result list.

2. Edit the metadata for a single document or for multiple documents in one go.

   If the information to be edited is only in the index field, the index entry can be edited for all documents in one go (Context Menu > Edit multiple index entries).

   If the information to be edited is only part of an index entry and the other part appears different for the various documents, edit the index entry per document.

If you are asked to make amendments to the backup metadata of your file cabinets, you can refuse to do so where appropriate on the grounds that the associated expense would be unreasonable where appropriate (see Recital 39 GDPR).

As described above, it is important to ensure that your company does not retain a document longer than necessary for the purposes of task fulfillment while respecting the legal retention period.

## Providing personal data for transfer

With DocuWare you can provide a requesting person with the relevant documents plus metadata or just the metadata to comply with Article 20 GDPR.

If documents and metadata are to be transferred:

1. Search for the relevant documents in each of your file cabinets.
2. Use DocuWare Request to export the documents containing the personal data and provide them to the person requesting a transfer.

DocuWare Request has a search function and a viewer with which the requesting person can independently search and view the data and documents.

If it's only metadata that needs to be transferred:

1. Search for the relevant documents and associated metadata in each of your file cabinets.
2. Run a CSV export of the metadata from the result list.

## Setting up a process for data access or data copies

You should establish a process in your company for requests from data subjects in accordance with Article 15 GDPR (Right of access by the data subject / data access) and in accordance with Article 20 (Right to data portability / data copy). DocuWare can also help you in this process with DocuWare Forms and Workflow Manager.

You need two forms that you create with DocuWare Forms:

1. Request form

   The request form should include at least:

   a. Text field for the email address of the requesting person
   b. Checkboxes for types of request: Data access and/or data copy

2. Response form
   The DPO completes this form in response to the requesting person. It should include at least:
   a. Text field for the email address of the requesting person
   b. Checkboxes for every possible type of stored personal data, e.g. email address, date of birth, home address
   c. Text field for entering the legal basis on which the data is stored and processed (this might be a contract with the requesting person)
   d. Checkbox confirming that files are attached
   e. Element to attach files

You also need two workflows that you create using Workflow Manager:

1. "GDPR request" workflow
2. "GDPR response" workflow

You publish the request form on your website. When a requesting person completes the form and sends it, a document is created and stored. This triggers the "GDPR request" workflow.

The DPO runs a search for the personal data in the relevant file cabinets and completes the response form. When it is stored in the file cabinet, this triggers the "GDPR response."

The individual steps look like this:

1. A requesting person completes the request form on your website and sends it.
2. The request form is automatically stored in the file cabinet when it is sent and this triggers the "GDPR request" workflow.
3. In the "GDPR request" workflow, the DPO receives the task of processing the request.
4. The DPO processes the task. In the case of a simple access request, the DPO searches for personal data. In the case of a data transfer, the DPO creates a data copy. The DPO confirms the task and receives a link to the response form as the next task. This completes the "GDPR request" workflow.
5. The DPO completes the response form and attaches a data copy in case of a data transfer. The DPO sends the response form, which is saved as a document in the file cabinet, and the "GDPR response" workflow is triggered. The requesting person automatically receives an email containing the DPO's response and, if applicable, a data copy as an attachment. Delivery of the email completes the workflow.

If necessary, include further steps in the "GDPR request" and/or "GDPR response" workflows for consultation with your legal department or an external legal advisor. If the data protection officer does not have access to certain data, for example your CRM, other employees with access rights may need to be involved.