WHITE PAPER

The General Data Protection Regulation of the European Union and KMD WorkZone 2018

By KMD WorkZone R&D

KMD
An NEC Company

CONTENTS

1. INTRODUCTION

The EU-GDPR
The European Union's General Data Protection Regulation (GDPR) is a set of rules and regulations aimed at granting citizens increased control over their personal data, especially, but not restricted to, digital data.

The regulation set is intended to simplify and streamline rules for data-generation, storage, protection, retention and removal and applies to all organizations and business – be they public, private, non-profit or any combination.

The EU-GDPR applies to any organization operating in the European Union or any other global organization offering goods or services to parties within the European Union and contains regulations dealing with the gathering and managing of data, reporting requirements regarding breaches or compromises in data security, specifying consumer rights to their own data and defining punitive fines for non-compliance of EU-GDPR set.

Purpose of the white paper
This whitepaper describes the general EU-GDPR feature set as it is implemented in the KMD WorkZone 2018 product. The feature set consists of two system access codes, retention policies and document classification codes as well as a process for deleting cases and documents from the KMD WorkZone application and database.

The whitepaper also describes the configuration settings and parameters that can be defined and enabled in order to set up KMD WorkZone to comply with EU-GDPR as well as the consequences for the KMD WorkZone users when utilizing the EU-GDPR feature set.

Previous and present WorkZone products
When describing the EU-GDPR feature set, it is important to be aware that there are no requirements that already existing systems must be GDPR compliant if these systems do not support or contain setup options or procedures that enable such compliance.

New systems must however contain setup options or procedures that enable such compliance.

If a system is not GDPR compliant, workflow changes and user training regarding GDPR awareness has been suggested as mitigating or stop-gap measures until such systems can be installed.

Previous versions of the KMD WorkZone product (2017, 2017 SP1 and 2017 SP2) already contain many of the required features that satisfy the requirement of the EU-GDPR and the present KMD WorkZone product release closes the gap and now contains features which support Privacy by Design and Default.

The KMD WorkZone product itself is not by default set up to fully utilize the EU-GDPR feature set when installed out-of-the-box. You or your system administrator must configure your KMD WorkZone installation to reflect the conditions under which your organization operates as well as your organization's workflows, legal requirements, structure and work processes.

2. THE WORKZONE GDPR FEATURE SET

WorkZone 2018 release contains a wide range of inter-connected features which collectively can be referred to as the EU-GDPR feature set. The individual components of these features will understandably change as the product undergoes continued releases and the features themselves are augmented and improved.
The feature set has been developed with the specific goal of implementing the requirements, guidelines and recommendations contained in the EU-GDPR but are not and will not be limited to the regulations.

At present, the WorkZone EU-GDPR feature set can be summarized to consist of the following features:

- Encryption of data and communication
- Classification of documents
- Retention policies
- Deleting cases, documents and contacts

These features will be described in varying degrees of detail in this whitepaper.

> **Note**
> Attention must be directed at the two new system access codes, which are formally part of WorkZone's user rights management system but were created in order to facilitate user and administrator operations in a GDPR-based environment.

Finally, the whitepaper will address how and where an administrator can configure enable and set up the EU-GDPR feature set in WorkZone. Some features will have to be enabled and set up while others will affect users immediately.

All EU-GDPR features will require careful analysis and forethought regarding your organization's specific requirements and work processes as well as specific and general legal commitments prior to enabling and setup.

3. SYSTEM ACCESS CODES

Before addressing the specific EU-GDPR features, the two new system access codes must be briefly mentioned as they may affect the rest of the features detailed in this whitepaper. The EU-GDPR feature set relies on the use of two central access codes introduced in KMD WorkZone 2018:

- SOFTDELETE
- RETENTIONADM

The access codes determine the following user rights with regards to the features of the EU-GDPR in WorkZone:

SYSTEM ACCESS	DESCRIPTION
SOFTDELETE	**Grants rights to:** - Send a case or archived document to the recycle bin - Restore cases and archived documents from the recycle bin - Delete cases and documents permanently if a user has access code associated with the case's or document's retention policy.
RETENTIONADM	**The default update code for the two pre-installed retentions codes: None and Forever.** - Grants rights to: - Setup and maintain retention policies in WorkZone Configurator*

*You must have the DATAADM access code to define Delete reasons and set the default retention policy in the WorkZone Configurator, but you must have the RETENTIONADM access code to actually setup and maintain retention policies. See retention policy, delete reasons and defining a default retention policy below.

Additionally, read access is required to display and view cases and documents in their respective recycle bins and Write access to cases and documents is required to send them to the recycle bin in the first place also to subsequently permanently delete them. Like all WorkZone access codes, the SOFTDELETE and RETENTIONADM access codes are set up and assigned to WorkZone users in the Microsoft Active Directory.

The access codes are referred to in the various chapters below.

4. ENCRYPTION OF DATA AND COMMUNICATION

The EU-GDPR recommends encryption of communication and data should be enabled for organizations with sensitive data, especially if the probability and consequences of a data breach are substantial.

This whitepaper does not cover data or communication encryption specifically, although it is the recommendation of the KMD WorkZone Development team to always consider data and communication security, regardless of whether or not you are operating in a GDPR-environment.

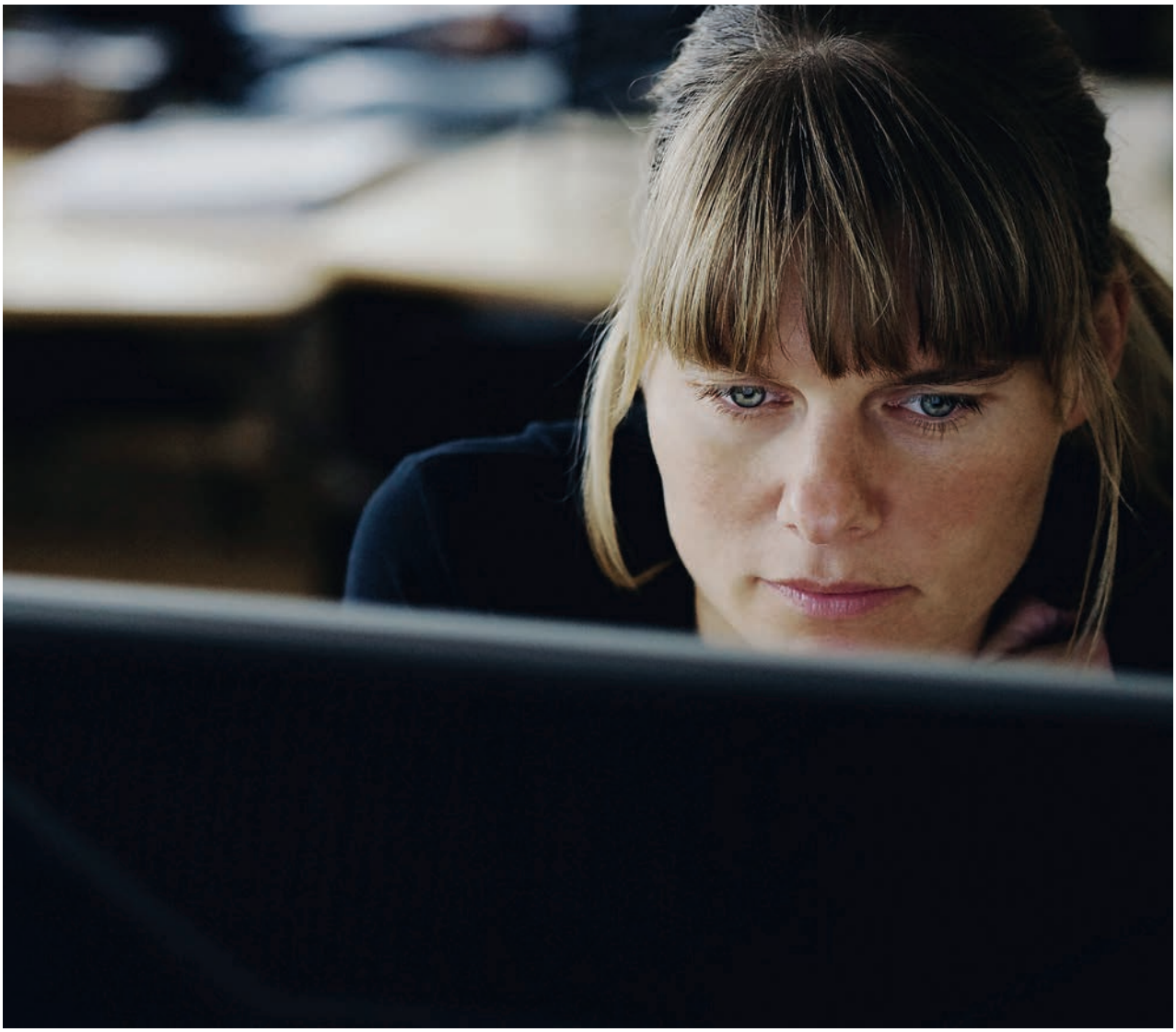
Encryption of data
The WorkZone product runs on top of an Oracle database and you can encrypt an Oracle database by installing the Oracle Advanced Security add-on module which can be purchased from Oracle.

From Oracle's website:

> Oracle Advanced Security provides two important preventive controls to protect sensitive data at the source: encryption and redaction.
>
> Together, these two controls form the foundation of Oracle's defense-in-depth, multi-layered database security solution.
>
> Transparent Data Encryption (TDE)
> Transparent Data Encryption (TDE) stops would-be attackers from bypassing the database and reading sensitive information directly from storage by enforcing data-at-rest encryption in the database layer.
>
> Data Redaction
> Data Redaction complements TDE by reducing the risk of unauthorized data exposure in applications, redacting sensitive data before it leaves the database.
>
> *Link: http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html*

Encryption of communication
To better secure your communications, you can set up HTTPS communication for WorkZone.

HTTPS is an adaption of the Hyper Text Transfer Protocol (HTTP) and is used to authenticate websites as well as protect the privacy and integrity of any exchanged data – for example by helping to prevent man-in-the-middle attacks. The HTTPS protocol also can help hinder eavesdropping and tampering with communication between client and server.



5. CLASSIFICATION CODES

The KMD WorkZone EU-GDPR feature set includes a new method of classifying documents by the sensitivity of document contents called Classification codes.

Classification codes help identify documents that contain sensitive or personal information. Data Administrators can then restrict access to these documents to only include personnel that have legitimate reasons for accessing or reading the data, for example, documents concerning health information or tax returns.

6. DOCUMENT CLASSIFICATION CODES

The Document classification code defines the document content based the contents sensitivity level and each document must be assigned a classification code.

Documents that contain public or non-sensitive content can be marked Public while documents that contain high levels of sensitive content can be marked with more restrictive classification codes, for example, Personal or Confidential.

Document Classification codes can be defined four places in WorkZone:

LOCATION	DESCRIPTION
On a document	The user can manually apply a classification code to a document by selecting a classification code in the **Classification Code** field on the **Document Detail** page in WorkZone Client or in the **Registration** pane in WorkZone for Office. Classification codes defined on a main document will be applied as the default code for any supplementary documents attached to the main document.
On an individual case	Documents assigned to a case will inherit the classification code defined in the **Default document code** field on the **Case Detail** page in the WorkZone client.
On a case group	Cases created as members of a Case Group will inherit the classification code in the **Classification code** field for the case group. Administrators can define the default classification code for a Case group in WorkZone **Configurator > Taxonomy > Classification** scheme page.
For the entire organization	Document inherits the classification code from the default classification code. Administrators can set this value in WZ **Configurator** on **Document** > **Default document classification** page.

In this hierarchy, document level has the highest priority while global level has the lowest priority. In other words, the default or inherited values help minimize manual work, but users always can overwrite such values if necessary.

Mandatory classification code

Classification codes are enabled by default in WorkZone 2018 and cannot be disabled, which means you must formulate a policy regarding your case documents when migrating to WorkZone 2018 or upgrading your installation.

The classification code is mandatory for all WorkZone documents created in or edited from WorkZone Client or WorkZone for Office. The classification code is not mandatory for documents created through WorkZone Explorer or from other WorkZone integrations. However, if you afterward edit the documents from WorkZone Client or WorkZone for Office, you must specify the classification code.

> **Note**
> Documents created in WorkZone Client 2017 SP1 and earlier versions are not classified automatically. You must apply classification codes to these documents manually.

Customizable classification codes

The actual definitions of the classification codes can be determined by your organization and each classification code may cover different levels of sensitive information and many entail different procedures and security access in different organizations.

Your organization should create guidelines, procedures and descriptions for each classification code utilized.

The WorkZone product includes 5 predefined classification codes:

CODE	TEXT	DESCRIPTION
CONFIDNT	**Confidential**	Suggested code for all documents that contain information considered confidential and not to be publicized.
INTERNAL	**Internal**	Suggested code for all documents that contain information not meant to be distributed outside of the organization.
NOTCLASS	**Not classified**	Suggested code for all documents not yet classified.
PERSONAL, Personfølsom	**Personal**	Suggested code for all documents that contain personal, private or sensitive information.
PUBLIC, Offentlig	**Public**	Suggested code for all documents that contain information that can be publicized or is public knowledge.

You can edit or delete the existing classification codes as well as create new codes in the WorkZone Configurator if necessary.

You can edit or delete the existing classification codes as well as create new codes in the WorkZone Configurator if necessary.

Ranks

The rank is an integer indicating the priority of the classification code with 0 being the lowest priority.

Ranks help solve conflicts of documents sensitivity. For example, if you create a merged PDF document containing multiple documents, the classification code will also be mandatory as the documents may contain varying classification codes. The classification code rank will determine which code will be used in the merged document. The highest classification code rank in the documents of the multi-document PDF will be used to set the classification code rank of the multi-document PDF itself.

For example, creating a multi-document PDF document from three documents with a classification code rank of 2, 3 and 5 will result in a PDF document with a classification code equal to the classification code rank 5.

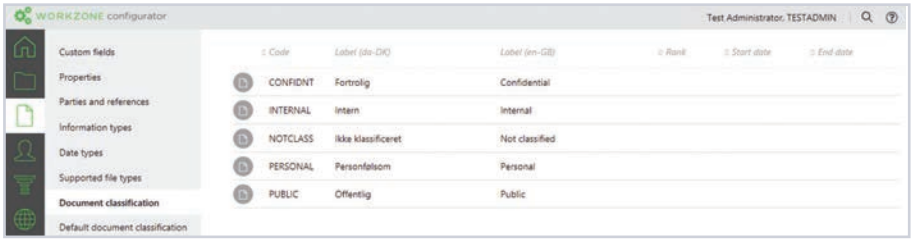
Editing and creating Classification codes

The Classification codes are set up and maintained on the Document classification page in WorkZone Configurator. The global classification code can be set up on the Default document classification page.

> **Note**
> Users must be assigned the DATAADM access code in order to view and configure the classification codes.

The Document classification sub-page

The Document classification sub-page contains all the document classification codes defined for the organization as well as the classification parameters.



Classification code

Each Classification Code contains the following parameters

PARAMETER	DESCRIPTION
Code	The classification code as it appears in the database. It will also appear in the Classification code field in the WorkZone Client and WorkZone for Office.
Label	An explanatory text in Danish or English which will appear beside the code in the Classification code field in the WorkZone Client and WorkZone for Office.
Rank	An integer that indicates classification code priority. The higher the integer, the higher the rank. For example, if you merge two documents with different classification codes, the highest classification code rank will define which classification code must be assigned to the resulting document.
Start Date	The date the classification code is active from.
End Date	The date the classification code is no longer active from.

Define active periods for the classification codes
You can define a period of activation for each classification code by specifying the Start Date and End Date parameters. You do not need specify both dates, one or the other or both can be specified.

Classification codes that no longer are active cannot be selected in WorkZone. However, documents that already contain a classification code that is not active any more will still retain the classification code.

Create and delete classification codes

If your organization needs your own customized classification codes, you can create new classification codes on the **Document classificatio**n sub-page, defining the parameters as needed.

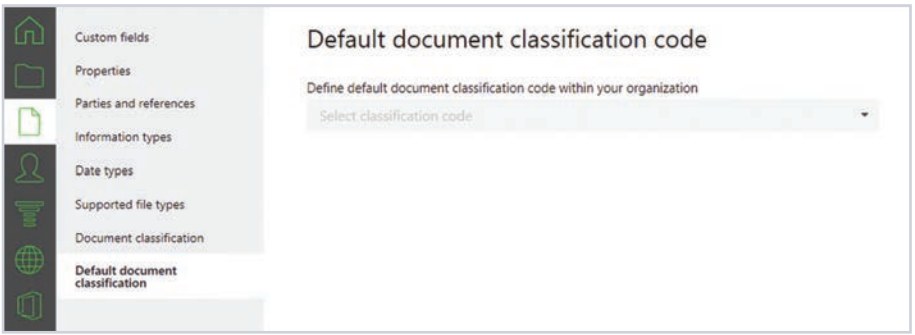
You can also delete a classification code, including any of the predefined classification codes included by default in a WorkZone installation.

You cannot delete a classification code if there are documents in the WorkZone database that are still assigned the classification code. Instead of deleting the classification code, you can define an end date, which prevents the classification code from being assigned to documents after the end date has expired.

The Default classification code sub-page

The **Default classification code** sub-page only contains one field where you can set the default classification code for your organization.

The **Default classification code** field is located in the **WorkZone Configurator > Document** page.



Default Classification code

After you have defined the defined default classification code in the WorkZone Configurator, it will be applied to all documents when the documents are created in the WorkZone client if a different classification code is not defined specifically on the case group, case, or on the document itself.

Example: Default classification codes

The following example illustrates how default classification codes are applied and can be changed going from the general setting to individual documents.

Default classification codes

The following default classification codes are defined in WorkZone Configurator:

In **WorkZone Configurator > Document page > Default document** classification sub-page: NOTCLASS

In WorkZone **Configurator** > **Taxonomy** page > **Classification scheme** subpage > on **Case group 6** > Define default values > **Classification code** field: PUBLIC

Case created – not in Case Group 6
A case is created and attached to the Case Group 5.

The NOTCLASS classification code is applied as the default value in the **Default document classification** field.

- A document is created in the case and the NOTCLASS code is applied from the case to the document as the document's default classification code.
- A new document is created in the case and the NOTCLASS code is applied from the case to the document as the document's default classification code. The user changes the document classification code from NOTCLASS to PRIVATE as the document is considered to contain information of a private nature.

Case created – in Case Group 6
A case is created and attached to the Case Group 6.

The PUBLIC classification code is applied as the default value in the **Default document classification f**ield. The field value is changed to CONFIDNT as the case's documents are determined to be confidential.

- A document is created in the case and the CONFIDNT code is applied from the case to the document as the document's default classification code.
- A new document is created in the case and the CONFIDNT code is applied from the case to the document as the document's default classification code. The user changes the document classification code from CONFIDNT to PERSONAL as the document contains personal information about one of the contacts of the case.
- A new supplementary document is created and already contains the PERSONAL document classification code. The user changes this to PUBLIC because the document is a publicly accessible document of guidelines that might be relevant for the main document itself.

7. RETENTION

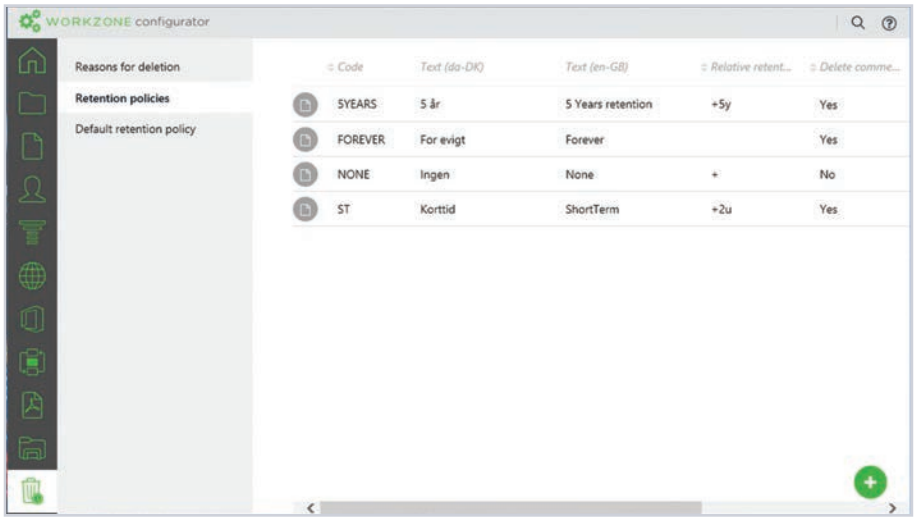
Within the EU-GDPR, users have the right to demand their documents and data be deleted from an organization's database – subject the organization's legal requirements for retention of the user's documents and data. Some documents and data may never be deleted due to legal requirements. This is especially relevant for many public organizations and institutions or private vendors serving public interests.

There exists a potential conflict of interests with regards to the deletion of documents and data: Legal requirements for retention of data and documents and the citizens right to be forgotten by merging the retention policies and delete rights. WorkZone endeavors to combine these different interests. Retention and delete policies are therefore interdependent. Retention is a part of an organization's delete policies and vice versa. Retention in WorkZone refers to a specific time period where cases and documents that have been closed still are to be available in WorkZone but should not be deleted. Retention contributes to the life cycle of a case by defining if and when a closed case can and may be deleted by assigning a retention policy to the case.

Some cases or documents may be required to be retained for a certain time period after being closed, others can and may be deleted immediately after being closed and still other cases and documents may never be deleted.

The Retention Policy
A retention policy can be assigned to each individual case and/or document, indicating whether or not the case or document should be deleted after it is closed and for how long the case and its documents are to be retained, if at all.

Retention policies are defined on the Retention policies page in **WorkZone Configurator** module > **Retention** page where you can set up the retention policies to be used in the organization, as well as define the default retention policy and the Delete Reasons.



A Retention Policy contains a retention code, text, description and the relative retention period, expressed as a number of months or years which a deleted case is to be retained for. The retention policy also contains a start and end date, which can be used to define the activation period of the retention policy. Inactive retention policies cannot be selected.

You can also define if the user is required to select a reason for deleting the case and/or documents as well as define when the retention policy is active.

Finally, a retention policy must be connected to an update code. The update code defines the access codes of organizational units and users who can change the retention code assigned to a case or document.

Additionally, users who want to delete cases and documents with the retention policy's retention code must also be assigned the retention policy's update code.

Apply a retention policy to a case or document
Retention policies are applied to a case or document by selecting a retention code for the case or document. It can be done in two ways:

- manually selecting the Retention code from the drop-down list in the Retention code field of a case or document, or
- automatically through a default Retention code being applied to the case or document when it is created.

Preinstalled Retention policies
The WorkZone product contains two retention codes when installed:

- None: Assigns a retention date equal to the date the case is closed. This enables a case and its documents to be deleted immediately after being closed. Forever: Does not assign any retention date to the case and documents when the case is closed. If the retention date is empty, the case and document cannot be deleted.

The Retention policy elements
A retention policy contains a number of elements which are defined when the policy is created and which can be edited after creation.

The following Retention policy elements are described below:

- Retention code
- Retention text and description
- Delete comment toggle
- Relative retention period
- Update code
- Retention start and end date

The Retention code

The Retention code is a short identifier of the retention policy and is displayed in the drop-down list in the Retention code fields on cases and documents where users can select new retention policies for their cases or documents if they have sufficient user rights to do so.

The user must be assigned the same access code as the access code defined in the Update Code field in the WorkZone Configurator > Retention > Retention policies in order to change a retention policy on a case.

The Retention code must...

- contain eight or less characters
- may not be empty
- may not contain the following characters: \!?”’,<>#$%^|=

The Retention code must also be unique meaning you cannot specify a retention code that already exists.

> **Note**
> The retention code is case-sensitive. The retention code 15weeks is not identical to the retention code 15Weeks.

The Retention code is mandatory when creating a new retention policy.

Retention text and description

The Retention text is mandatory and will be displayed with the Retention code in the drop-down list in the **Retention code** field on a case or document. The retention text is in English by default, but you can localize the retention text to Danish if necessary, making the Danish text available to users selecting the Danish language version.

The Retention description is not mandatory and is only displayed on the retention policy itself in **WorkZone Configurator** > **Retention** tab > **Retention policies** sub-tab. The retention description allows you to provide a longer, more comprehensive text describing the retention policy to yourself or other administrators.

The retention policy text may not exceed 65 characters but the retention policy description can be up to 200 characters.

The Delete Comment

When an element is deleted in WorkZone, the user must provide a reason for the delete action and might also be required to enter a description or delete comment as well. The Delete Reason is mandatory and is set up the **WorkZone Configurator** > **Retention** tab > **Reasons for deletion** sub-tab but you can freely set up whether or not the user will be prompted to enter delete comment on the retention policy.

If the **Delete comment** parameter for a retention policy is enabled, the user must enter a delete comment when deleting a case or document.

Relative retention period

The relative retention period is the period of time a case or document is to be stored after the case has been closed. A relative retention period must be specified as a time unit which is to be added to the closed date of a case. Multiple time units may be specified, for example 3 years or 9 months.

The following abbreviations are valid as time unit designations for the relative retention period:

Time unit	Description	Example
D	**Days**	+80D
W	**Weeks (Uger)**	+20W
U	**Weeks in Danish (Uger)**	+20U
M	**Months**	+20M
Y	**Years**	+5Y
Å	**Years in Danish (År)**	+5Å

*The time unit abbreviation is not case sensitive, so d,w,u,m,y and å are also valid time unit designations.

You must prefix the time unit with the number of units to be applied, for example +2y means two years and you cannot combine time units. For example, +1y+6m is an invalid relative retention period entry. If you need to create a relative retention period of 1½ years, you should use +18m instead.

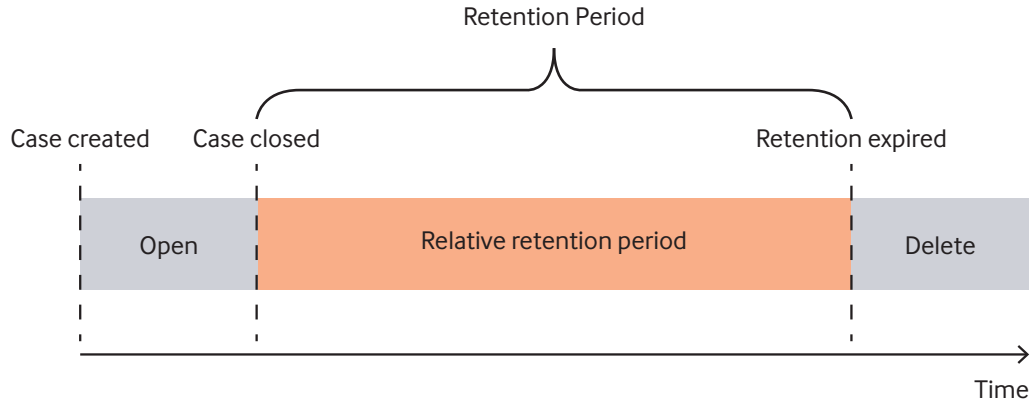
If the Relative retention period field is empty, there is no relative retention period and the case or document will be retained indefinitely. See the Forever retention policy as an example.

Regarding time units

Day is the default time period. If you enter just a number without specifying the time unit, the Day time unit is used. For example, +36 is the same as +36D or +36d. +1 is the same as +1d or +1d and is today's date plus one date, i.e. tomorrow.

If only one plus sign (+) is used, the relative retention period is today's date only.

The retention period
The retention period is the entire retention length of time the case is be retained and therefore is protected from being deleted.

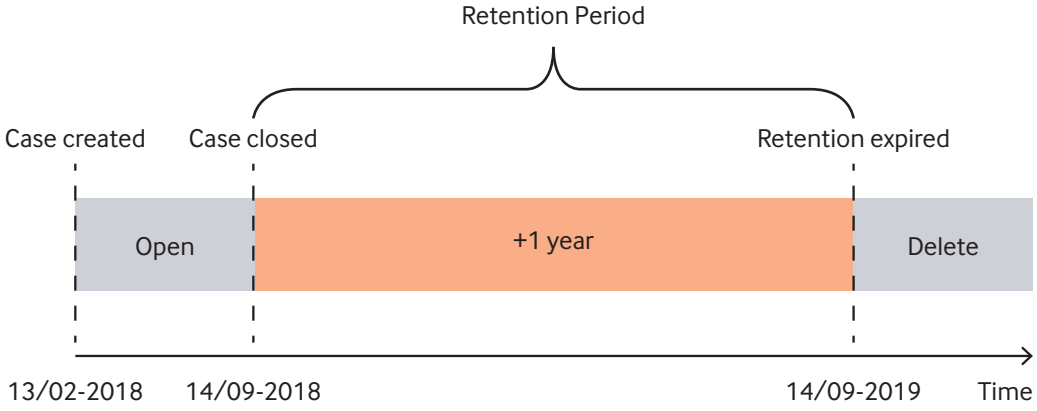


The Retention date is determined by adding the relative retention period to the date when the case was closed.

When the retention period on a case or document has expired, anyone with delete rights may delete the case or document.

Example – Retention period
Date case created: 13/02-2018
Retention code: A01
Retention text: Keep for 1 year
Relative retention period: +1y

Date case closed: 14/09-2018
Retention period: 14/09-2018 to 14/09-2019



The case was created 13th February, 2018 and the A01 retention code was assigned to the case. The Keep for 1 year retention policy contains the relative retention period of one year.

The case is closed on the 14th September, 2018. With a relative retention period of +1 year, the Retention date field on the case will be set to 14th September, 2019.

The case's retention period therefore starts 14/09-2018 (when the case is first closed) and expires 14/09-2019. When the retention period has expired, the case may be deleted from the system by any user with the SOFTDELETE user rights.

If the case is reopened on the 17th November 2018 and then closed again on the 23rd November 2018, the retention date will still be 14th September, 2019 since the retention date is calculated from the first closed date.

Deleting cases in the retention period
As a rule, cases cannot normally be deleted in the retention period, however users with the SOFTDELETE RETENTIONADM access code may delete cases at any time, even in the retention period.

Changing retention policies
If you are assigned the same access code as the Update code on the retention policy, you can change a retention policy on a case and the new retention policy will be applied to the case and all attached case documents. The Retention date will be recalculated to reflect the new policy's relative retention period. This will also happen, even if the case has been reopened after being closed.

Reopening cases
If a case is closed and then reopened, the retention period is not recalculated. When the reopened case is closed again, the original retention period is still in effect and the Retention date field of the case is not updated.

Triggering a new Retention Date
You can deliberately trigger a recalculation of the Retention Date field of a reopened case by selecting a new retention policy for the case. When the reopened case is closed, the Retention date will be calculated, using the new retention policy's retention period. Be aware if you select a new retention policy for the case, all case documents will also be updated to conform with the new retention policy.

You can also toggle the retention policy – first selecting a new retention policy for the reopened case, triggering the calculation of a new value of the Retention Date field and then select the original retention policy in order to obtain a new retention period for the now-reopened case when it is closed again.

Resetting the retention date
You cannot reset the Retention date manually as the Retention date is only calculated automatically using the case's first closed date.

8. UPDATE CODE

The retention policy must be connected to an access code in the Update code field of the Retention policy.

The access code defined in the Update code field determines which user may change a retention policy on a case or document as well as which user may delete a case or document permanently.

If a user wants to change the retention policy assigned to a case or document, the user have the same access code as the Update code of the retention policy.

If a user wants to a delete case or document permanently, the user must have:

_ the same access code as the Update code of the Retention policy
_ Write rights on the case or document
_ the SOFTDELETE access code.

The Update code field is mandatory but can be set to include nearly everyone in the organization or to only include a few select users who may change existing retention policies in cases and documents.

The Update code field is called Default update code in the Edit Retention policy form.

Retention start and end date
Retention policies also have a start and end date, enabling you to specifically set the duration of the specific Retention policy. If the start date is empty, the Retention policy is automatically active. If the end date is empty, the Retention policy will not expire. Inactive or expired retention policies cannot be selected for cases or documents.

You can specify an end date that lies before the current date if required, effectively creating a retention policy that is expired upon creation and cannot be immediately applied to cases or documents. You can then activate the retention policy at a later date by changing the end date to a date in the future.

Inactive and/or expired retention policies
Retention policies that are not active (the start date is in the future) or expired (the retention policy end date has occurred) cannot be selected or used as the default retention policy when creating cases.

Retention policies that already have been selected and assigned to cases and documents are still retained and will not suddenly be rendered invalid when the policy is deactivated or expires.

For example, if a case or document contains a retention policy that expires (the current date exceeds the end date of the retention policy), the selected retention policy will still be applied if the case or document is deleted.

Example – expired retention policy
Date Case A created: 05/04-2016
Retention Code: 3Months

Retention policy start date: 01/01-2016
Retention policy End date: 01/12-2017
Retention Period: +3m
Date Case A closed: 01/01-2018

The retention policy for the 3Months retention policy is still applied to the closed case even though the retention policy is deactivated and cannot be selected for newly created cases.

The case A may first be deleted on (01/01-2018 + 3 months): 01/04-2018.

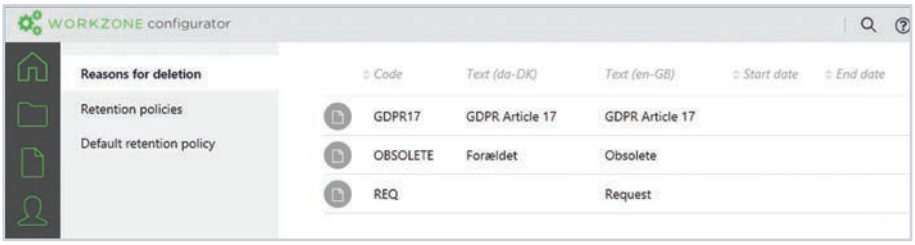
If the user tries to select a new retention policy for the case just prior to closing the case* – for example on 18/12-2017, the retention policy 3Months will not be displayed and cannot be selected because the policy is inactive.

*Assuming the user has sufficient rights to update the retention policy on a case or document and that the user is assigned the same the access code as specified in the Update code field on the retention policy.

9. REASONS FOR DELETION

When a user deletes a case, he must define a reason for deleting the case and might be prompted to enter a description for the delete action – the delete comment.

All the Delete Reasons must be created and maintained in **WorkZone Configurator** > **Retention** > **Reasons for deletion.**



A Delete Reason contains a text which can be localized to Danish, a Delete Reason code and you can define the activation period of the Delete Reason by setting the start and end dates.

The Delete Reason elements
The following Delete Reason elements are described below:

_ Delete Reason text
_ Delete Reason code
_ Delete Reason start and end date

Delete Reason text
The Delete Reason text is mandatory and is displayed in the drop-down list when the user is prompted to select a Delete Reason when deleting a case or a document.
The Delete Reason text may not exceed 25 characters.

Delete Reason code
The Delete Reason code is a short identifier of the Delete Reason and is displayed in the drop-down list when the user is prompted to select a Delete Reason when deleting a case.

The Delete Reason code...
_ must contain eight or less characters
_ may not be empty
_ may not contain the following characters: \!?”’,<>#$%^|=
_ is automatically capitalized

The Delete Reason must also be unique meaning you cannot specify a Delete Reason code that already exists.

The Delete Reason code is mandatory when creating a new Delete Reason.

Delete Reason start and end date
Like the Retention policy activation period, you can specify a time period where the Delete Reasons are active.

Active Delete Reasons will be displayed in the drop-down list when the user is prompted to select a Delete Reason when deleting a case or document. Inactive Delete Reasons will not be displayed in the drop-down list.

Cases and documents that have been deleted prior to a Delete Reasons deactivation will still retain the original Delete Reason.

The start and end dates for Delete Reasons are not mandatory, but care should be exercised if you specify a start and /or end date to ensure the date settings are meaningful and relevant.

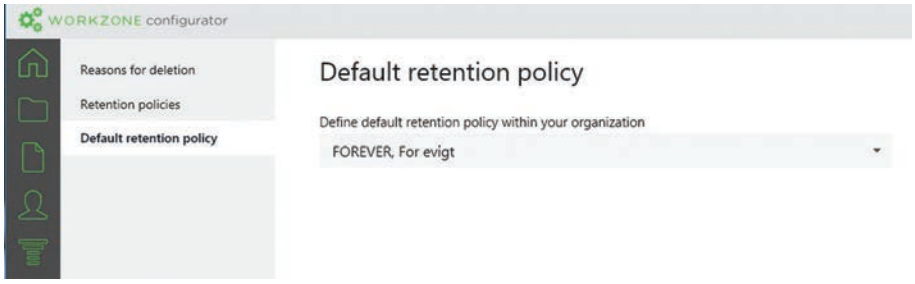
Deleting a Delete Reason
You can delete a Delete Reason in the WorkZone Configurator > Retention tab > Reasons for deletion.

Only unused Delete Reasons can be deleted.

Deleting a Delete Reason in the WorkZone Configurator will not remove the delete reason for any deleted cases or documents in the Delete Log.

10. DEFAULT RETENTION POLICY

You can specify a system-wide default retention code to be applied to all created cases in WorkZone in the **WorkZone Configurator** > **Retention** tab > **Default retention policy** sub-tab.



Default retention policy for a case group
You can also specify a default retention policy for a case group. If a Retention Code has been specified for at Case Group, the Retention Code will automatically be applied for all cases created for that Case Group.

The default case group retention policy will supersede the system-wide default retention policy.

Default retention policy for a case
When you create a new case in WorkZone, the retention policy for the case group will be used as the default retention policy for the case.

If there is no defined retention policy for the case group, the retention policy for the system will be used as the default retention policy for the case.

If there is no defined retention policy for all of WorkZone, the default retention policy for the case will be empty.

The Retention code field is mandatory for cases and documents, so you must select a retention policy when creating cases and documents.

Note
If the retention policy is changed on a case, then the new retention code will automatically be applied to all documents on the case.

Default retention policy for documents
When you create documents on a case, the retention policy of the case will be used as the default retention policy for the document.

Note
The retention policy on a case may be changed by the case handler if the case handler is assigned the retention policy update access code.

The retention policy update access code can be defined for each retention policy in **WorkZone Configurator** > **Retention** tab > **Retention Policies** sub-tab.

11. EDITING A RETENTION POLICY

You can edit existing retention policies in the Edit Retention policy form found in **WorkZone Configurator** > **Retention** tab > **Retention policies**.

To open the Edit Retention policy form
Open the **Edit Retention policy** form by hovering the mouse over the policy you want to edit and clicking the **Edit** icon.

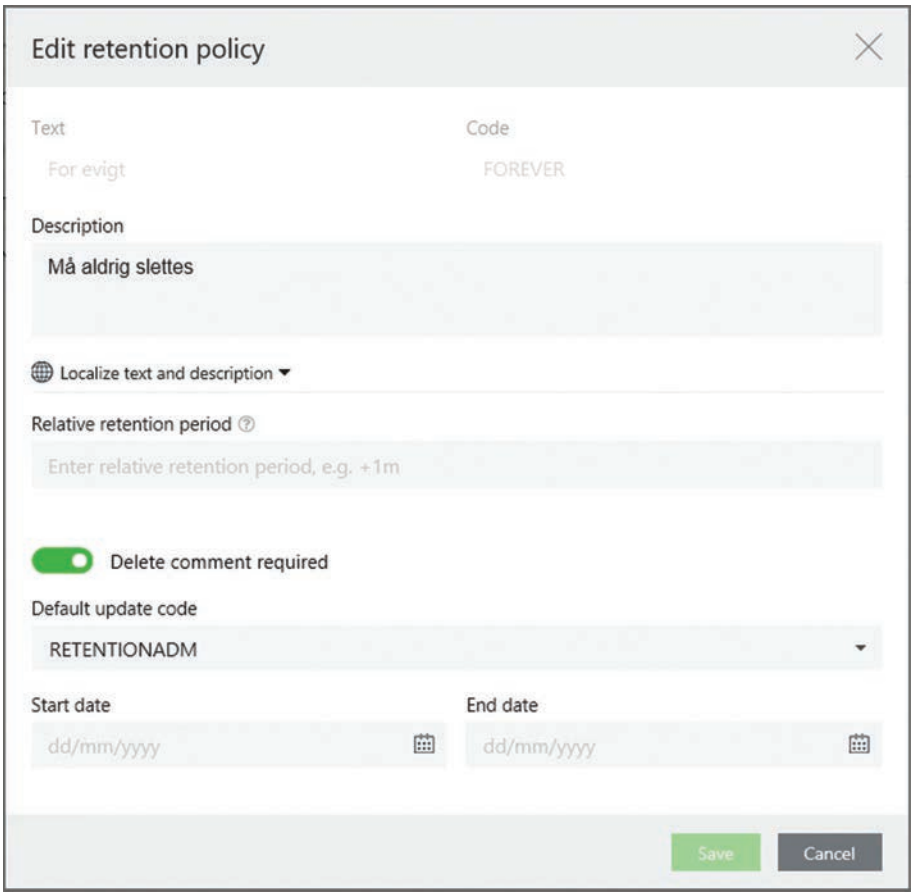
In the **Edit Retention policy** form, update the fields you need and click the Save button to update the WorkZone configuration.

Any changes will be applied immediately to WorkZone but effects based on the settings are not recalculated or re-triggered.

For example, if you change the Relative retention period field, the update will be applied immediately.

Closed cases will not be reopened to trigger the recalculation of the new retention period. (WorkZone calculates the retention period when the case is closed)

Cases that are currently open will use the new value in the Relative retention period field to calculate the retention period when they are closed.



Deleting a Retention Policy
You can delete a Retention policy in the **WorkZone Configurator** > **Retention** tab > **Retention policy**.

Only unused retention policies can be deleted. Retention policies that have been assigned to cases and documents cannot be deleted.

12. RETENTION POLICIES AND SPECIAL WORKZONE CASES

There are several cases in WorkZone which have special uses and functions and therefore must be handled in a different fashion than other standard cases.

Two such examples are Desktop cases and Temporary cases.

Desktop cases
Each user has own desktop case. A desktop case in WorkZone is a special case which cannot be closed or deleted and functions as a case to contain all created but unassigned documents. Desktop cases are automatically assigned the default retention policy, usually the **Forever** retention policy.

In WorkZone, all documents must be saved on a case. If a user creates a document and does not immediately save it on a case, the document will automatically be assigned to the Desktop Case.

Documents saved on the Desktop case can be deleted by any user with Read and Write access to the documents.

Temporary Cases
Temporary cases, (cases in the SJ-TEMP case group) are automatically assigned the **None** retention policy which means SJ TEMP cases can be deleted immediately by any user with Read and Write access to the documents and the SOFTDELETE access code.

13. RETENTION POLICIES AND DOCUMENTS

Retention policies can be applied to cases and documents and while the functionality is similar between the two, there are some differences with regards to documents and retention policies.

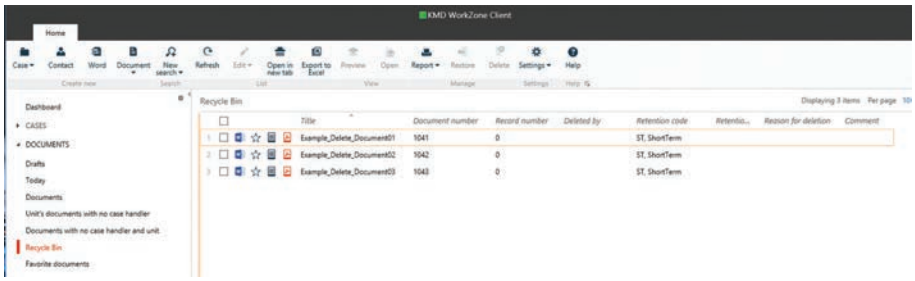
Documents will inherit the retention policy of the case the document is created or imported into as the default retention policy.

Documents that are moved from one case to another will inherit the target case's retention policy as the default retention policy.

Supplementary documents will inherit the main document's retention policy as the default policy when the supplementary document is created or imported.

Note
A document's default policy can be changed if the user has sufficient rights to do so, but if the retention policy is changed on the case, the new retention code will automatically be applied to all documents on the case, including documents that contain a different retention policy than the case.

Changing the retention policy on a case will therefore overwrite all retention policy changes made to the documents of the case.



14. DELETING CASES AND DOCUMENTS

A central theme in the EU-GDPR regulation set is the right of citizens to be forgotten and their data deleted from private and public databases, within certain legislative, administrative and medical exceptions and limitations.

In accordance with this theme, WorkZone 2018 enables deletion of cases and documents, but also ties the deleting of these data items with the user administration and access rights system in WorkZone.

This allows a system administrator to define a set of users with rights to delete cases and documents as well as rights to restore the same items in case of an erroneous deletion. The delete rights are combined with the case status and retention policies to create a simple and robust methodology for retaining and deleting items in WorkZone.

This means WorkZone users can delete cases and documents if required or requested to, but access to deleting cases and documents is managed by a combination of user rights and retention policies/periods.

Two-step delete process
Deleting cases and documents in WorkZone requires two steps – sending the items to the recycle bin and then emptying or removing the items from the recycle bin.

It is intentionally made difficult to permanently delete an item by mistake as there are several checks in place by the system in order to ensure user rights are sufficient to delete an item and additionally to ensure user participation is required to approve the impending removal of an item.

You can also set up WorkZone to prompt for Delete Reasons and user comments when deleting, pausing the delete process and requiring user interaction to continue the delete process.

Deleting cases and documents consists of two steps:

1. Send to Recycle Bin: Sending the case or document to their respective recycle bins (Case recycle bin and Documents recycle bin) where they can be either restored back into the system if the initial deletion was incorrect or deleted permanently.The contents of the Cases recycle bin and Documents recycle bin can be accessed from the WorkZone Dashboard.

2. Delete Permanently: Deleting the case or document from the recycle bin will irrevocably remove the case or documents from the WorkZone system and database. Deleted cases and documents cannot be restored.

15. DELETING DOCUMENTS

SPECIAL CONSIDERATIONS WHEN DELETING DOCUMENTS

Supplementary documents

A document in WorkZone can have sub-documents attached called supplementary documents.

When a main document is sent to the recycle bin, all supplementary documents are automatically also sent to the recycle bin. However, if you want to permanently delete the main document, you must first permanently delete all supplementary documents attached to the main document.

Supplementary documents may be inaccessible to some users, for example if the supplementary document contains access codes which prevent some users from reading, writing or even deleting a document. These inaccessible supplementary documents cannot be sent to the Recycle bin and therefore cannot be deleted.

Document references

Documents containing non-system or user-created references to cases or other documents cannot be sent to the Recycle bin or deleted until these references are removed. System references that are created and updated by WorkZone such as Replies/Replied by, Copy/Original, etc do not restrict document deletion.

Root documents

Documents that are the root of a branching hierarchy cannot be sent to the Recycle bin or deleted. Root documents are documents that have document versions, more specifically the "old Captia" implementation of document versions.

It was already possible to delete documents in WorkZone prior to the implementation of the EU-GDPR feature set, depending on the document state, for example, archived documents could not be deleted.

The EU-GDPR feature set augments the document delete options by using the access code that enables a user to update the Retention policy (the Update Code) as well as the SOFTDELETE access codes to the parent case of the documents as well as applying the retention policy to the documents themselves.

Sending non-archived documents to the Recycle bin

Documents that are not archived (Document state ARK) i.e. document states UP (Personal Draft), UÅ (Draft) and/or UL (Locked) can be deleted by anyone with update rights and with membership of a security group with the delete right on the record table.

Sending archived and terminated documents to the Recycle bin

For documents that have been archived, i.e. have the ARK document state or are Terminated using WorkZone Captia document state, the user must be assigned the SOFTDELETE access code.

Users that do not have the SOFTDELETE access code cannot delete archived and/or terminated documents.

Archived documents saved on a Desktop case or saved on a case that belongs to the SJ_TEMP Case Group may be deleted by any user.

Retention period expired or no Retention policy

If the Retention policy contains relative retention policy (i.e. the Relative retention policy field is not empty) or if the retention period has expired (the Retain Until date is in the past), only users with Read and Write access to the document and the SOFTDELETE access code may send the document to the recycle bin.

If a Delete Reason is not selected, the OBSOLETE Delete Reason will automatically be applied as the Delete Reason.

If a Delete Comment is required by the Retention policy, the user must enter a comment when prompted.

Retention period active or Retain until field is empty

If the Retention period is still active (The Retain Until date is in the future) or if the Retain Until field is empty, only users with Read and Write access to the document and the SOFTDELETE access code may send the document to the recycle bin.
The Delete Reason is mandatory and the user must select a delete reason from the list in the field.

If a Delete Comment is required by the Retention policy, the user must enter a comment when prompted.

16. DELETING CASES

It was not possible to delete cases in WorkZone prior to the implementation of the EU-GDPR feature set but with the introduction of the EU-GDPR feature set, cases can be sent to the recycle bin and subsequently permanently deleted - much like documents.

Since deleting a case can have serious implications and consequences for an organization, users must have sufficient rights to delete a case and certain conditions must be fulfilled in order to delete a case, for example the rights required to delete a case will depend in the status of a case.

Only cases with assigned retention policies can be deleted. If a case does not contain a retention policy, it cannot be deleted. All documents on a case must be deleted before you delete the case. A case that still contains documents, cannot be deleted.

Sending cases to the Recycle bin
The following situations apply when deleting cases – i.e. sending a case to the Recycle bin.

Retention period expired or no Retention policy
If the case does not contain a Retention policy (Retention code is None) or if the retention period has expired (the Retain Until date is in the past), any user with the SOFTDELETE system access code may delete the case.

If a Delete Reason is not selected, the OBSOLETE Delete Reason will automatically be applied as the Delete Reason.

If delete comments have been enabled for the Retention Policy, the user must enter a delete comment.

Retention period active or Retain Until is empty
If the case contains a Retention policy (Retention Code is different from None) and the retention period is still active (The Retain Until date is in the future), only users with the SOFTDELETE access codes may delete the case.

The Delete Reason is mandatory and the user must select a delete reason from the list in the field.

If a Delete Comment is required by the Retention policy, the user must enter a comment when prompted.

Cases that still contain document references or documents cannot be deleted. The document references or documents must be deleted before you can delete the case.

The two recycle bins
When cases and/or documents are sent to the Recycle bin, they are marked as deleted in the database and placed in the user's Personal Recycle bin.

The user can restore cases and document from the respective recycle bins or delete the them permanently, similar to deleting items from the Windows operating systems recycle bin. A case that still contains documents, cannot be deleted permanently until the case documents have been deleted permanently.

Cases that are restored from the recycle bin will be re-inserted into WorkZone without their documents. If you want to restore some or all of the case documents from the recycle bin, you must do so for each document. Cases that are deleted from the recycle bin are permanently deleted and cannot be restored from within WorkZone.

Documents that are restored from the recycle bin, are restored to the case they belonged to. If the case is also deleted, you can select to restore the case as well. Documents can also be restored to another case, effectively moving the restored document to a new case. Cases and documents that are marked as deleted will not appear in normal searches but can be accessed through the recycle bins or by creating searches that specifically search for deleted items.

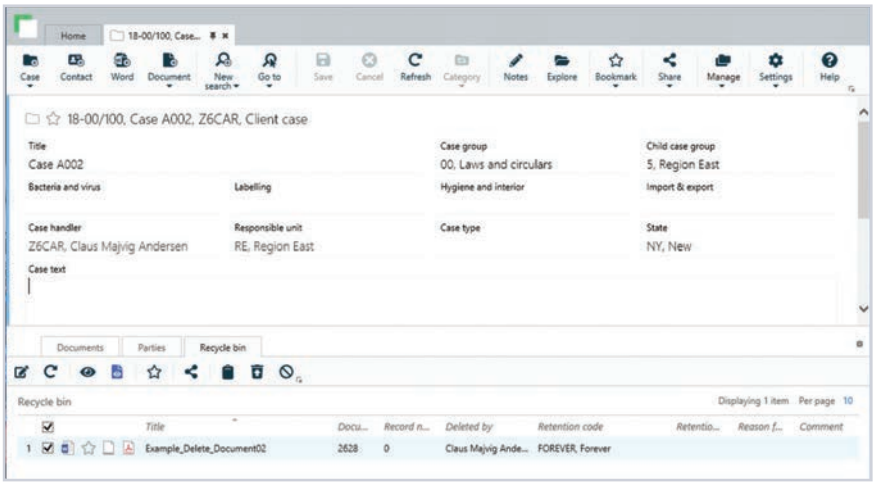
There are two recycle bins in WorkZone:

- **The personal recycle bin:** Contain items that have been deleted by the specific user. Users can restore any deleted cases in their own personal recycle bins. One for cases, one for documents
- **The system recycle bin:** Contains all items that have been deleted by all users.

Users with the SOFTDELETE access code, Write access and have the same access code assigned as the Update code of the Retention policy of the case or document can restore any case (including their own) in the system recycle bin if they have read rights to the case. Restoring deleted cases also requires sufficient user rights as different system access codes grant users access to restoring.

The Case-specific recycle bin

In addition to the recycle bins mentioned above, you can also view all deleted documents on a case by adding the Recycle bin tab to the case detail page.



This recycle bin is a slightly more limited recycle bin than the one opened from the navigation pane. It only displays deleted documents that belong to the active case and the user can only restore the documents to the active case.

New tab pages can be added to case detail pages by clicking the setup button to the far right of the case detail page and selecting the relevant tab pages to display.

Locating items in the recycle bin

Once a case or document has been sent to the recycle bin and marked for later deletion, the case or document will not appear in any widgets or be displayed in any dashboard lists in WorkZone.

If you want to display the case or document again, restore it or delete it permanently, you can still access the case or document in the recycle bin.

To locate a case or document in the recycle bin you can:

- Use a list: There are recycle bin lists which you can add to your Cases or Documents dashboard or the navigation pane. Users can only see their own deleted cases and documents when displaying the recycle bin through the Dashboard lists.
- On a case or document: You can add the Recycle bin tab page to display all deleted documents for the active case only.
- Create a WorkZone Search and in the Deleted by field, specify the user who deleted the cases and documents to be located. Users can see other users' deleted cases and documents by using a WorkZone search.

Case and documents can still be displayed in the recycle bin, which enables you to verify cases and documents before they are deleted permanently.

You must have the Read access code in order to see cases and documents in your respective recycle bins.

Deleted cases and documents are dimmed in the Dashboard lists and have crossed-out titles on the Detail tab pages.

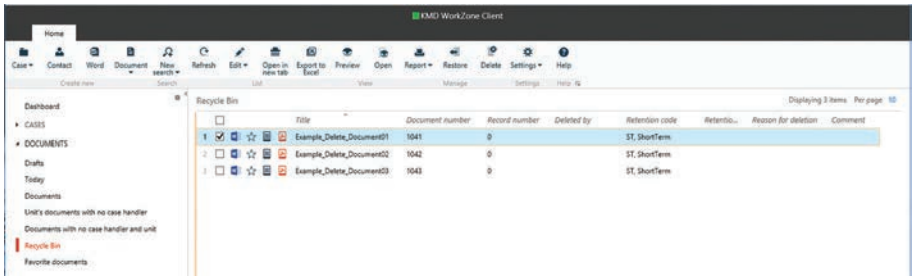
Restoring items from the Recycle Bins

Once a case or document has been deleted (sent to the case or document recycle bin), you can restore the case or document if you have erroneously deleted the case or document or you can delete the case or document from the recycle bin.
If you want to restore a case or document from its respective recycle bin, you first must be able to see the recycle bin and its contents.

Displaying the Recycle Bins

The recycle bin for each WorkZone item (case or document) is displayed in a case or document list which can be added to the navigation pane.

The WorkZone Dashboard must be modified to display the recycle bins for the Cases and/or Documents.



Restoring a case from the cases recycle bin

To restore a case from the Cases recycle bin, open the recycle bin and select the case to be restored. Click the Restore button to restore the case and all its attached documents.

Restoring a document from the documents recycle bin

To restore a document from the Documents recycle bin open the recycle bin and select the document to be restored. Click the Restore button to restore the document. You can restore a document directly to a case, if the case still exists in WorkZone, i.e. the case is not deleted. You can also restore a document to another existing case in WorkZone.

NOTE:
Users must be assigned the SOFTDELETE access code to restore Terminated or Archived documents.

If the case the document belongs to is deleted as well, you can restore document and the case as well.

17. PERMANENTLY DELETING WORKZONE ITEMS

Once a WorkZone item (Case or document) has been sent to the Recycle Bin, the item can be removed from the recycle bin, deleting it permanently.

Deleting an item permanently
The relevant recycle bin (Cases or Documents) is opened and the item or items you want to delete can be selected.

Click the Delete button to delete the selected items.

Permanent means permanent
Items that have been permanently deleted cannot be restored or reinstated through normal procedures in WorkZone.

Permanently deleting documents
Documents are removed from the Recycle Bin by selecting the document to be removed and clicking the Delete button.

Only users that satisfy the following requirements may delete a document permanently:
- Write access to the document
- Assigned the SOFTDELETE access code
- Assigned the same Update code as the retention policy on the document

Archived documents
In previous versions of WorkZone, prior to the implementation of the EU-GDPR feature set, once a document had been archived, it could not be deleted. This was to conform with government and national archive regulations preventing the removal of archived documents. The implementation of the EU-GDPR feature set has enabled permanent removal of even archived material.

Retention period expired or no Retention policy
If the Retention policy is None or if the retention period has expired (the Retain Until date is in the past), the Delete log is updated when archived documents are permanently deleted.

Retention period active
If the Retention policy is None or if the retention period has expired (the Retain Until date is in the past), the Delete log is updated when non-archived documents are permanently deleted.

The archived document record number
When a document is archived, it is assigned a sequential document record number in the WorkZone database and locked for editing on the case.

If the archived document is later deleted, a new document record of the type DEL will be assigned to the now vacant record number in order to fill the gap in the record number sequence and also serve as an indicator that the original document was deleted.

Non-archived documents
Non-archived documents in the Recycle bin – Documents can be deleted permanently from the WorkZone application.

Permanently deleting cases
When cases are permanently deleted, the case is removed from the WorkZone database and all references to and from the case are also deleted permanently.

It is not possible to permanently delete a case that still contains attached documents. You must permanently delete the attached documents before deleting the case permanently.

Only users that satisfy the following requirements may delete a document permanently:
- Write access to the document
- Assigned the SOFTDELETE access code
- Assigned the same Update code as the retention policy on the document

To ensure cases with archived documents are not inadvertently deleted permanently, the user will be prompted to approve the delete action when a case containing archived documents is deleted from the recycle bin.

18. THE DELETE LOG

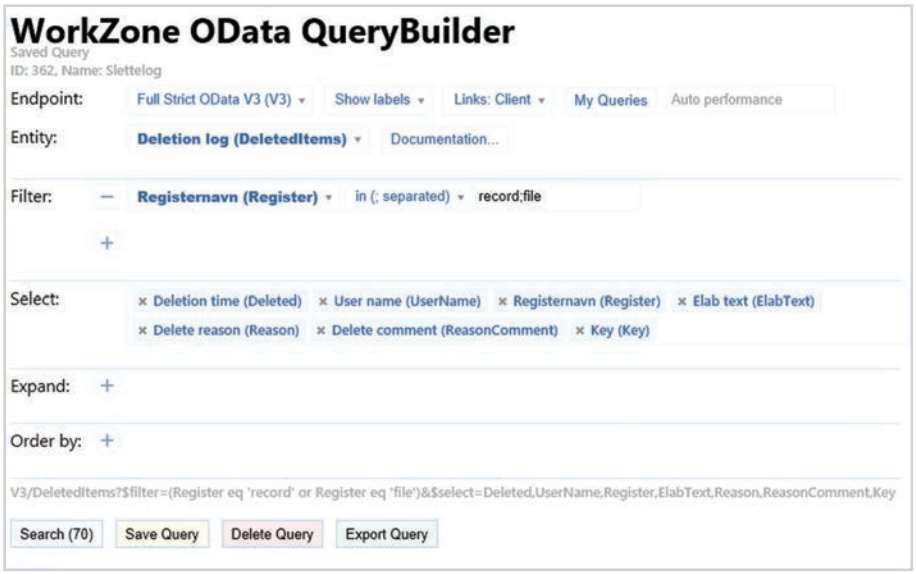
When a WorkZone item (Cases or documents) are deleted permanently, a log of the delete action is made in order to document the deletion for later control and registration.

The DeletedItems table is used to store the delete information with the following information:

- ID of the deleted item
- Type of the deleted item
- Delete Reason selected for the deleted item
- Delete comment defined for the deleted item
- UserKey who deleted the item.
- Delete time and date when the item was deleted.
- Summary (elaborating text) of the deleted item

The Delete Log can be displayed by using the WorkZone Query Builder to create a search which can be accessed from WorkZone. The QueryBuilder search can then be activated to display the contents of the Delete Log.

The following Odata query can be used to display Delete Log for cases and documents:
V3/DeletedItems?$filter=(Register eq 'record' or Register eq 'file')&$select=Deleted,UserName,Register,ElabText,Reason,ReasonComment,Key



Entries in the DeletedItems table (the Delete Log) are permanent and cannot be deleted or edited by any user.

Only users with USELOGADM rights can view and search the contents of the DeletedItems table.

The contents can be exported as Excel files for reporting and processing purposes.

19. DELETE REASONS AND COMMENTS

Whenever a WorkZone item is deleted permanently (removed from the recycle bin) and the item has a defined retention policy, the user must specify a reason for the permanently deletion of the item. Delete Reasons are selected from a pre-defined list of possible Delete Reasons.

If the retention policy contains a mandatory delete comment, then the user must also enter a delete comment.

Delete Reasons
The list of Delete Reason is set up in the **WorkZone Configurator** > **Retention** page > **Reasons for deletion** sub-page.

See the Reasons for deletion section above.

Delete Comment
WorkZone can be configured to require a delete comment whenever a WorkZone item is permanently deleted (removed from the recycle bin).

If the **Delete comment required** parameter is enabled on the retention policy, every time a user deletes a case with that retention policy from a recycle bin (Personal recycle bin or System recycle bin), the user must submit a comment for the delete action of at least 10 characters in order to approve the delete action.

20. DELETING CONTACTS

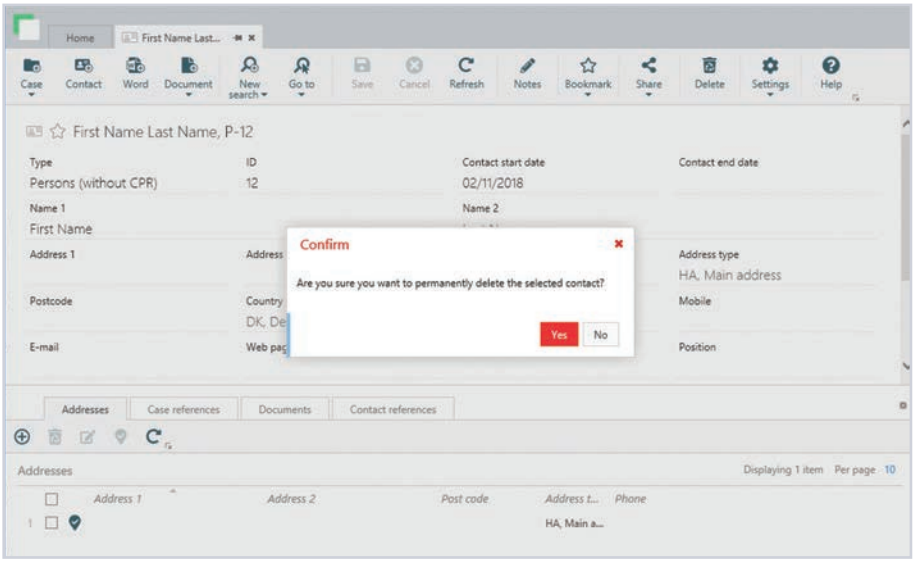
From WorkZone 2018.1 and onwards, Contacts can also be deleted directly from the WorkZone Client.

Contacts are deleted permanently and are not sent to the recycle bin. There is therefore no recycle bin for deleted contacts and there is no restore option for contacts deleted by mistake.

No references, employees or units
Contacts that contain references to cases, documents or other contacts cannot be deleted. If you need to delete a contact with references, you must remove all references on the contact before deleting the contact.

Additionally, you cannot delete Employee or Unit contacts (Contact type is **Employee** or **Unit**) from the WorkZone Client regardless of the presence of references on the contact.
Deleting a contact

To delete a contact, open the contact detail page of the contact you want to delete and click the **Delete** button in the main ribbon. The **Confirm** dialog will be displayed and if you select the Yes button, the contact will be deleted permanently.



21. SETTING UP THE EU-GDPR FEATURE SET IN WORKZONE

The EU-GDPR feature set is an integral part of the WorkZone 2018 product and some features will already be created and enabled automatically such as the two default retention policies (None and Forever), the Delete Reason Obsolete, the five pre-defined Case and Document classification codes as well as the new access codes SOFTDELETE and RETENTIONADM.

Other features must be manually created, set up and enabled in order to take advantage of the entire WorkZone EU-GDPR feature set.

Additionally, some already existing features must be tweaked in order to adjust the WorkZone application and setup to the requirements and work processes of your organization.

Prerequisites
Make sure the user who is creating, setting up and maintaining the WorkZone parameters for the EU-GDPR features in the WorkZone Configurator has sufficient user rights to do so.

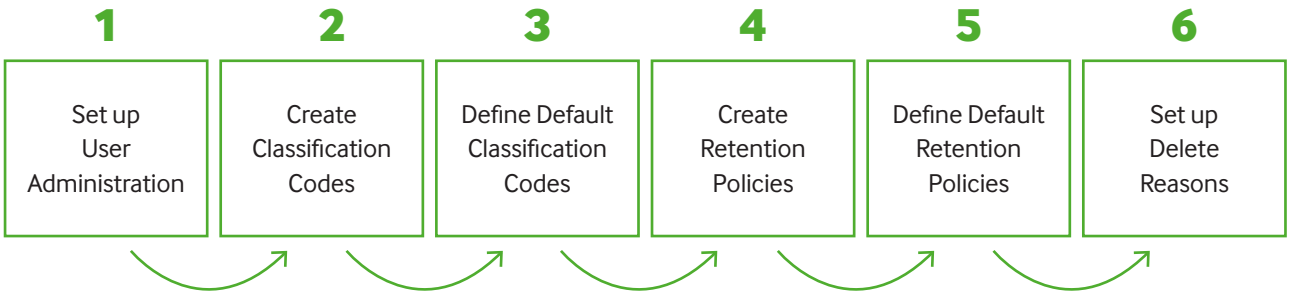
The user must have the DATAADM Access code to save changes in the WorkZone Configurator.

Upgrading cases and documents
When upgrading your WorkZone installation from WorkZone 2017 and earlier to WorkZone 2018 and later, i.e. when upgrading from a non-GDPR environment to a GDPR environment, default document classification codes or retention policies will not be applied to your existing documents.

If you want your existing cases and document to reflect the new retention procedures of your organization, you must either manually edit the affected cases and documents or set up a database script to mass update the relevant cases and documents after the initial upgrade.

The EU-GDPR set up procedure

The following steps should be run through when setting up the EU-GDPR feature set for KMD WorkZone:



1. User Administration

a. Analyze your organization and user-rights

b. Assign relevant access codes to relevant users

2. Create and set up document classification codes

3. Define default classification codes

a. Define default classification codes for WorkZone

b. Define default classification codes for specific Case Groups

4. Create and set up retention policies

5. Define default retention policies

a. Define default retention policies for WorkZone

b. Define default retention policies for specific Case Groups

6. Create and set up Delete Reasons

1. User Administration

Analyze your organization, the workflows and requirements and the WorkZone users and identify which users (if any) need to be able to delete and restore WorkZone items and which users need extended rights regarding deleting and restoring other users' WorkZone items as well as having expanded delete and restore rights.

Use the standard WorkZone procedures to assign SOFTDELETE and RETENTIONADM access codes to the relevant WorkZone users – the ones you identified previously.

This user access right setup must be maintained regularly in order to reflect changes in the organizations' user base as well as incorporating work flow changes and procedures and legislation changes.

2. Create and set up document classification codes

Create and set up any new Document classification codes and customize the codes (new and existing) to your organization's needs.

Document classification codes are created and maintained in the **WorkZone Configurator** > **Document** page > **Document classification** sub-page.

Defining Case and Document classification codes is not mandatory in the WorkZone Client by default and must be specifically set up by a system administrator.

3. Define default classification codes

Once you have created and set up the necessary document codes, you can define the default document classification codes. Defining default codes is not mandatory, but can make every day work a bit easier on the users.

Additionally, if WorkZone is set up to prevent users from selecting or changing codes and policies, defining correct default classification codes and retention policies is required to avoid administrators from constantly having to adjust document classification codes and retention policies on newly created WorkZone items.

You can define default classification codes for your entire organization (WorkZone) as well as for Case Groups.

You cannot select a classification code that is not active i.e. has expired or not started yet.

WorkZone
Define the default document classification code for the entire organization (all of WorkZone) in the WorkZone Configurator > Document page > Default document classification sub-page.

Case group
Define the default document classification code for the case groups in the WorkZone Configurator > Taxonomy page > Classification scheme sub-page.

Select the case group you want to define the default classification code for and click the Define default values button to open the Define default values form.

4. Create and set up retention policies

Retention policies are the base of the EU-GDPR feature set and apart from the two pre-defined retention policies (None and Forever), you must create and set up all retention policies which may be relevant for your organization's work flow and retention requirements.

Create and set up the retention policies that are to be applied to the cases and documents in WorkZone.

Retention policies are created and set up in the **WorkZone Configurator** > **Retention** page > **Retention Policies** sub-page.

To create a new Retention policy, click the **Create** button in the lower right-hand corner of the form and define the following fields and parameter settings:

- **Text:** Name of the retention policy
- **Code:** Short 8-character code for the retention policy
- **Description:** Longer, more descriptive text about the retention policy
- **Relative retention period:** The length of the retention period, calculated from the date the case is closed.
- **Delete comment required:** Enable this parameter is make delete comments mandatory when permanently deleting WorkZone items.
- **Default update code:** Select the access code users must have to change retention policy on a WorkZone item as well as delete cases and archived documents permanently.
- **Start Date:** Define the retention policy activation period by setting the start date.
- **End date:** Define the retention policy activation period by setting the end date.

If the retention policy is to be localized in another language – typically Danish – you can select the **Localize text and description** drop-down field and define the Danish version of the retention policy.

5. Define default retention policy

Once you have created and set up the retention policies, you can define which retention policy is to be the default. Like default classification codes, defining a default retention policy is not mandatory, but can make every day work a bit easier on the users.

You can define default retention policies for your entire organization (WorkZone) as well as for Case Groups.

You cannot select a retention policy that is not active i.e. has expired or not started yet.

WorkZone
Define the default retention policy for the entire organization (all of WorkZone) in the WorkZone Configurator > Retention Page > Default retention policy sub-page.

Case group
Define the default retention policy for the case groups in the WorkZone Configurator > Taxonomy page > Classification scheme sub-page.

Select the case group you want to define the default policy for and click the Define default values button to open the Define default values form.

6. Create and Set up Delete Reasons

Regardless of whether or not the delete comments are enabled, you must create and set up any Delete Reasons necessary for your organization to categorize any permanently deleted WorkZone items.

Delete Reasons are created, set up and maintained in the **WorkZone Configurator** > **Retention** Page > **Reasons for deletion** sub-page.

To create a new Delete Reason, click the **Create** button in the lower right-hand corner of the form and define the following fields and parameter settings:

- **Text:** Name of the Delete Reason
- **Code:** Short 8-character code for the Delete Reason
- **Start Date:** Define the Delete Reason activation period by setting the start date.
- **End date:** Define the Delete Reason activation period by setting the end date.

If the Delete Reason is to be localized in another language – typically Danish – you can select the Localize label drop-down field and define the Danish version of the Delete Reason.

KMD
An NEC Company

© KMD 2019
Lautrupparken 40-42
2750 Ballerup
Tlf. 4460 1000
www.kmd.dk