
# White Paper Data Privacy With censhare

**Whitepaper**

**Version 1.5**

**Manuel Weiss**

**Date 16/02/2018**


Telefon 089 56 82 36-0, Fax 089 56 82 36-501
info@censhare.com, www.censhare.com



turn complexity
into value

# Table of Contents

# 1 Data Privacy With censhare – Introduction

Europe and many other regions in the world move toward a stronger protection of privacy. In the EU, the General Data Protection Regulation (GDPR) sets the gold standard. But many other countries are about to release – or have already done so – similarly strict data protection laws.

Also, for global companies having part of their customer or user base in the EU, the GDPR applies.

We have created a white paper for our customers and partners explaining how to implement privacy measures in censhare in order to fulfill the legal requirements as implied by the law. Much of it has to do with technical implementation, permission concepts etc.

However, data protection and privacy are not all about IT security which is only one aspect to it. Some measures are also organizational, like IT procedures, role separation within a company etc. Other measures are plainly legal or contractual – see chapter “Legal Basis for Processing Personal Data”.

# 2 Legal Background

This whitepaper cannot cover all legal aspects. Be sure you get proper legal consultancy before processing personal data.

## 2.1 Personal Data

Data protection or privacy laws usually protect personal data. Personal data in most law systems, like the EU (GDPR) is defined as everything that makes a person distinctly identifiable – be it directly (e.g. a personal email address, social security number etc.) or indirectly (e.g. a login name, an IP address) where a person can still be identified using additional information.

## 2.2 Legal Basis for Processing Personal Data

In order to be allowed to process personal data, you need to either have the explicit consent of the person, or a legal foundation (like a commercial contract, business relationship, employment etc.).

If you build your data processing on a person’s consent, it is inevitable to document this consent. This can be in writing or using a tool. censhare offers options to document consent for users of a web portal powered by censhare’s Online Channel.

Regardless on what basis you build your data processing, make sure it is auditable by the authorities. In case of electronic consent through a web portal, you can follow the instructions in the chapter “Documenting Consent”. For consent in writing, you may want to use censhare’s DAM capabilities to keep scans of the signed consent letters within the censhare system for audit purposes. Also, if your data processing is based on any kind of contractual relationship, censhare can be used as a DAM to manage electronic copies of your scanned contracts.

Further contractual requirements apply if you either have “sub-contractors” (that would include Freelancers), or if you process personal data of EU citizens in countries outside the EU. In these cases, you will need either data processing agreements (between you and all sub-processors) or EU standard contractual clauses (aka EU model clauses) for processing data outside of the EU.

## 2.3 Data Separation

One of the guiding principles of the GDPR is data separation. The principle implies that data collected for one purpose may not be used for another purpose. As an example, if you have a contractual relationship to send invoices to a person, it does not mean you are allowed to sell this address data to address dealers. This may also mean that data used in one department (like Finance) cannot simply be used by another department (like Marketing).

censhare offers many possibilities to implement data separation. The most prominent one is the domain model. Please refer to the corresponding chapter under “Permission concepts in censhare”.

# 3 Security Features of the Product censhare

## 3.1 Passwords

Passwords are a center piece of IT security. censhare makes no exception. In principal, a censhare system offers you the choice between using external passwords (usually using an LDAP server like Microsoft Active Directory), Single Sign On (SSO) and with internal passwords.

In case of external authentication (LDAP, AD, SSO), no user passwords are stored within the censhare system. The complete authentication is handled by the external authentication server. This also means that password policies like expiration, minimum length, complexity have to be set up on the external server. A complete guide how to configure LDAP and SSO in censhare can be found in our ecosphere:

https://ecosphere.censhare.com/en/documentation/operation/article/2390581

In case of internal authentication, passwords are stored in an encrypted way in the censhare database. The encryption censhare uses is SHA256 + Salt. This is an encryption that according to the current state of technology is regarded as safe.

If you work with internal passwords, censhare offers options to set the desired expiration time and complexity of passwords in the admin client. You can access these settings in the Admin Client under Configuration – Server – General. The section allows you to set the number of invalid login attempts until a user account is locked (and can only be unlocked by the system administrator), the password expiration time and – most importantly – regular expressions that check the complexity rules defined by your organization and responding with meaningful messages to the user (example below).

## 3.2 Client Server Communication

The complete communication between the censhare client (Java client or web browser) can be transport encrypted. For this, the Java client uses the secure TLS protocol, the web browser can access the censhare server through HTTPS. The result is that during transport, the data cannot be intercepted by 3rd parties.

It is highly recommended to configure client-server configuration to only use secure protocols, we have not seen any measurable performance impact when using modern hardware.

# 4 Permission Concepts in censhare

## 4.1 Introduction

censhare offers 5 levels of privilege control:

- Domains control which assets a user can see
- Roles control which actions a user can perform on all the assets that belong to the accessible domain scope
- Asset “ownership” allows access control for individual assets
- Permission keys can be assigned to the assets metadata to allow tiered access to individual assets based on roles, rather than domains (not covered in this whitepaper)
- User interface customization controls which metadata becomes accessible for the role

Therefore, it is crucial to draft a solid concept first on how to structure domains and roles within your company (e.g. by department, by level in the organization etc.) in order to be able to match GDPR requirements like the data separation requirements. With a thought-through permission concept, you can prevent personal data to be accessed by unauthorized people, can distinguish between reading, modifying or deleting roles and much more.

## 4.2 Domains

A domain is a tree-like structure that reflects hierarchical organizations. Each asset in a censhare system gets associated a node somewhere in the domain tree. Likewise, every user gets a certain role (see below) for a certain node in the domain tree.

As a result, this user can only access assets that are on the same level of the domain tree as him/herself or below. What he/she can do with these assets is determined by the role he/she has for this domain.

## 4.3 Roles

A role controls the type of actions users can perform on an asset that by their domain permissions can access. Each role can be defined in a very granular way as it consists of a combination of >80 permission keys that control read-only or read-write permissions, but also if assets can be exported, deleted, which editors can be used to open assets and much more.

The combination of domains and roles is an extremely powerful instrument to fulfill all requirements towards protection of personal data in a censhare system when properly planned.

## 4.4 Ownership

In addition to the concept of domains and roles, individual assets can be given an “ownership”. The asset can be “owned” by one or many individual users, or by one or many user groups. You can also determine if non-owners have access to this asset at all (otherwise, they do not even find such assets in their search results) or if they have read-only access.

Ownership usually makes sense for exceptions on individual assets that don’t fit into the domain and role concept. The concept avoids that you have to create separate domains or roles just for one single occurrence.

# 5 Recommendations When Setting up a Permission Concept

## 5.1 Planning

In general, it is highly recommendable that you work with censhare Professional Services or a Professional Services person from a censhare partner when planning your permission concept. Before you work on a technical level, think through all the requirements not only from a product usage perspective but also from a privacy perspective. Determine which users/user groups/departments need which kind of access to which data.

With such a strategic concept in mind, it is much easier to technically implement it in censhare.

## 5.2 Template Users

It is highly recommendable to not set up every censhare user individually – especially if many users are working with a censhare system.

You should rather set up “template users” for each type of distinct task in censhare and name them accordingly. Each of these “template users” would already have the specific set of roles and domain access to fulfill their task but also to be prevented from accessing personal data outside of what they are allowed to according to your processing instructions.

In order to then create real user accounts for each user group or task is as simple as duplicating one of the “template users” in the Admin Client and only edit the personal details of the duplicate like name, login etc.

An alternative censhare offers is to set roles and domain access from an LDAP or AD directory based on data from that directory, like department. censhare allows to pre-define templates in XML that are used to create users based on directory information. This is a similar and less manual approach to creating template users. This approach requires consultancy from a solution developer in order to be set up properly.

# 6 User Interface Customization

## 6.1 Possibilities of Customization

Adapting the UI is one more means to determine what users in certain roles can do or see. censhare uses the concept of role-based workspaces. You can create such workspace for specific roles. A workspace determines what you see on your dashboard, but also what kind of information the different “asset pages” show for each single asset type.

Depending on your data privacy requirements, you could for example determine that certain roles only see the name of a person asset, but not information like phone number or email address.

In principle, one needs to distinguish between the Java and the Web client. Both clients offer options that lead to similar results but the way of customizing the UI is different (XML Editor vs. JSON/JavaScript). In order to perform UI customization, you will need the experience level of a Solution Developer or get the help of a censhare consultant. Therefore, this white paper will only discuss the principal possibilities.

### 6.1.1 Java Client

In the Java Client, all customization from tables through menus and dialogs is performed in the admin client. When you customize any area, a duplicate of the standard customization is being created, and can be assigned to one or many specific user roles (see chapter on roles above). This allows you to create different copies of tables or dialogs for the same situation where as a result, users in different roles are being displayed a different set of features/data.

### 6.1.2 Web Client

In censhare Web, the UI customization is based on workspaces. These workspaces can be adapted to specific roles (and are then being created as variants of the default workspace). A workspace consists of dashboard pages and asset pages, each one of which can contain “widgets”.

A widget is the smallest unit to display data. Therefore, adding or removing complete widgets from a role specific workspace is one option to restrict access to data for that role. Another one is to configure the widget to only display a certain set of data as desired for the role.

## 6.2 Areas of the UI Showing Personal Data

As mentioned in the introduction, personal data can appear in almost any part of censhare and at any asset type. Since censhare does not restrict companies using it from a wide area of configuration and customization, and since a user cannot be prevented from entering personal data into fields not initially intended for this purpose, you will have to analyze your own censhare system as to where you expect personal data to show up.

There are, however, some hints where in the default configuration it is likely to see personal data, and that should therefore be a special focus on applying the techniques mentioned above to restrict access on an as-needed basis. The incomplete list of areas to check consist of:

- The asset page for person assets with all their different containers and widgets
- The “Status” widget on every asset page displaying creator and modifier of the asset
- The “Workflow” widget on every asset page, displaying a list of workflow targets – usually other censhare users

- Image assets: an image can be irrelevant in terms of privacy as long as it doesn't show a person but may be relevant once it does
- IPTC meta data of image widget (shown in the "properties" widget of the image asset page)
- Search results especially where person assets and partially images are the result of the search

# 7 Documenting Consent

The censhare Online Channel is the publishing channel to the web, being used to publish web sites. For this channel, censhare offers a standard portal that makes it easy to create web portals with user logins. Our own "censhare ecosphere" is just one example.

The censhare standard portal comes readily prepared for documenting consent to terms and conditions as well as to a privacy policy. The portal configuration offers two pre-defined assets, one for the terms, and one for the privacy policy.

The generation of an account refers to these assets via link and offers a checkbox to accept them. The timestamp of acceptance is documented at the person asset of the person having created the account.

If the privacy policy gets updated, the portal will automatically prompt a user to accept the new version upon the next login. The new acceptance will then also be documented at the person asset together with timestamp and version of the privacy policy that has been accepted. This way, our standard portal gives you all means at hands to comply to the documentation requirements requested by GDPR.

Please work with consultants from censhare or a censhare partner to discuss details of the implementation.

# 8 Data Deletion

As per GDPR and many other data protection laws, personal data can only be kept as long as it is still needed to fulfill the legal purpose it was collected for (e.g. the fulfillment of a contract) as long as no other laws mandate you to keep it for a longer period. This could for example be tax laws. This white paper cannot discuss retention periods and deletion requirements for certain data as this is determined by many factors and additional local laws. Please consult local attorneys to understand the requirements.

In addition, GDPR introduces the right to be "forgotten", meaning the erasure of personal data of a data subject on request.

A general recommendation is to develop a combination of 2 documents:

1. a procedure documentation where for each process with which you process personal data you document the retention period.
2. a deletion concept where you describe how exactly the data from document 1. is being deleted (i.e. describe the deletion method). This not only affects censhare but all other tools used to process personal data in your company. If deleting personal data is not feasible a tolerated alternative is usually locking or pseudonymization of data.

When it comes to deleting personal data in censhare, we have to differentiate between master data (mainly the users accounts) and data stored in assets.

## 8.1 Master Data

Master data containing personal data can mostly be found in the "Users" table. The user accounts apart from login names can contain a user's name and email address. Think about what you do with users who left the company, changed departments etc. You should develop clear employee new hire, change and exit processes, part of which is how you deal with their personal data.

In censhare, you can simply delete a user account in the admin client. When doing so, you are being asked for another user to whom everything assigned to the user that needs to be deleted gets re-assigned (e.g. a colleague). This will remove any traces of personal data from the master data and from the UI in censhare itself.

If assigning everything to another user is not feasible (e.g. because the assignments are no longer needed), think of creating a dummy user without any permission in the system, and use this dummy user as the reassignment target for users you delete.

A final option would be to “anonymize” a user by overwriting all personal fields (like names, mail addresses etc.) with dummy values. This way it is no longer possible to know which individual was behind a certain user account.

## 8.2 Assets

Personal data in assets is a lot trickier. There are asset types that are quite obviously related to personal data, mainly the person asset. Other asset types have default meta data that might contain personal data, like the IPTC meta data at image assets. And finally, of course, nobody can prevent personal data stored in arbitrary features at pretty much any asset (e.g. in the description field, even in the asset name of e.g. an image asset.

You should set up deletion rules for the asset types you know contain personal data in your company. This can be a routine manual mass deletion of assets fulfilling certain criteria according to a schedule. But the censhare system also gives you control of what is being kept, and when it is deleted. In the admin client you can determine how many versions of each asset type are being kept how far back into the past. The actual clean-up of versions is being done in the asset deletion modules that can also be found in the admin client. For more details, refer to

https://ecosphere.censhare.com/de/dokumentation/application-administration/article/3561680

and

https://ecosphere.censhare.com/de/dokumentation/application-administration/article/2376033