

The Shareworks Platform description

- an understanding of the Shareworks platform and implemented security measures

Technology

Shareworks is an online SaaS platform that organizes your company's information and brand identity. Shareworks is a Danish proprietary software platform. Shareworks customers purchase a license-based subscription for the platform. The Shareworks service is therefore a classic web-based "Software as a Service" service.

The platform's core service is to make the customer BrandCompliant on their marketing material and adapt pre-defined templates to the individual countries and contracts on Shareworks.

Shareworks uses InDesign as the graphics engine to generate PDF files for use in maintaining a uniform layout on their marketing products.

Shareworks makes it possible for customer service managers and team leaders to get inspiration for their marketing from the undefined template and at the same time maintains their brand, so they can use this insight to create even better customer service.

Shareworks entire business foundation is based on Shareworks customers being comfortable with Shareworks processing their data securely and in accordance with applicable regulations.

This Shareworks platform description is intended to be a detailed review of implemented measures that ensures Shareworks is perceived and recognized as a vendor that securely processes data on behalf of their customers from all segments, including government and authorities, municipalities, pension funds, banking, utility, and insurance companies.

Should this description give rise to any questions, we are available to answer such by written request to info@bemiit.dk.

Development method

Shareworks is developed based on agile principles with a focus on creating the right solutions in close collaboration with users and customers. Shareworks development department is structured in cross-function teams and works structured with tasks in a dedicated task management system.

All changes to code undergo automated testing as well as review and approval before release.

The technology stack chosen is the latest languages and modern technologies that ensure high performance, scalability and security.

Web app

The web app is built as a single page web app in .NET that communicates securely with Shareworks backend/server over SSL/TLS 1.2 (minimum requirements).

Technologies:

jQuery / JavaScript / CSS / Web APIs
.NET MVC

Backend / Server

Shareworks backend is built around a number of services that each handle part of Shareworks platform. These services are built so that they are easy to scale and act as an *API* for Shareworks and other integrations that can be integrated into Shareworks.

Technologies:

C# / .NET Core / MSSql

The dynamic content generator is a Shareworks created plugin based on the Adobe InDesign server.

Note that the Shareworks service is a SaaS solution, hence it is operated exclusively on Shareworks environments with full responsibility to ensure updating of versions and frameworks.

Integrations / API

Using our API, you can connect a wide range of different systems to Shareworks, including DAM / PIM, HR among others.

Shareworks integrates to most known systems. Otherwise, the integration work is done as part of start-up, and usually doesn't require great involvement from Shareworks customers. It is a process that is handled solely between Shareworks and the customer's supplier providing the content.

Data retention

Shareworks process the following customer data:

Company relevant information for the templates

Images for the templates, which comes from customer

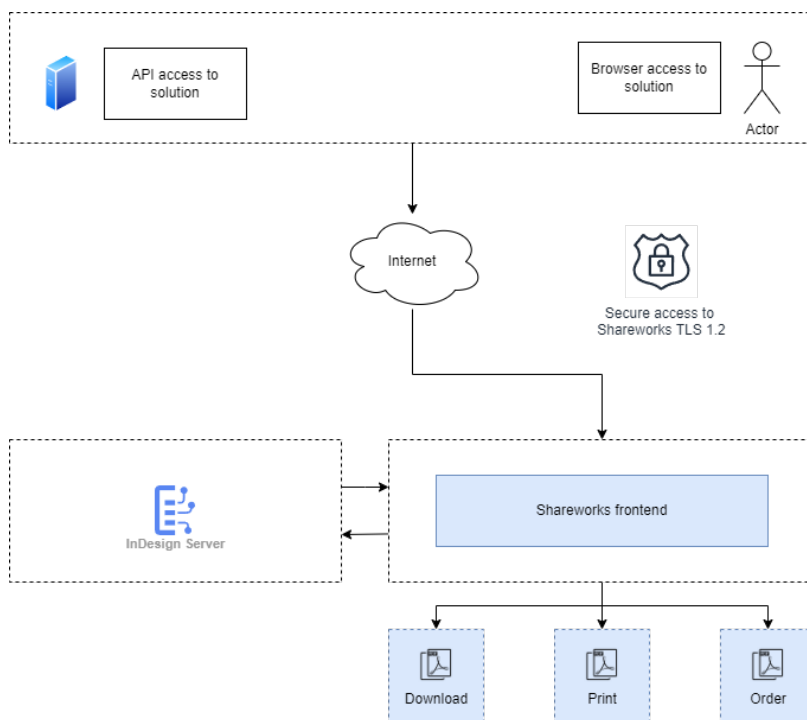
Customer data is processed and stored by the following data center provider:

- *AWS services Stockholm*

All services associated with the Shareworks services, incl. the platform, are mapped. The storage and hosting services provided by AWS do not require the use of other subcontractors, as these services are all performed solely by AWS. All other elements of the Shareworks services, incl. the platform, are thus provided directly and exclusively by Shareworks.

System illustration

The illustration included shows the typical involvement of Shareworks customer infrastructure and the interaction with Shareworks infrastructure.



You can see more about AWS security measures, security certificates, etc. by following this link:

AWS: <https://aws.amazon.com/>

GDPR and security measures

Data retention and recovery

All user generated files are stored at our data center.

All data is fully backed up on a daily basis and are stored for 1 month.

Deletion of data

By default, Shareworks is set up with a deletion policy so that processed files by the users are automatically deleted after certain periods.

Shareworks has chosen a default deletion policy setting to ensure that data is deleted in accordance with our customers' obligations under the GDPR. However, it is possible for each customer to change all default settings to reflect their specific deletion requirements and wishes.

Setting up the platform will always involve clarifying the customer's specific requirements, if such have not already been uncovered in the initial discussions between the customer and Shareworks, and such agreed deletion policy requirements will be reflected by change of the default settings.

In the following, the various data and related deletion possibilities in the Shareworks platform are detailed:

Deletion of data relates to the data that Shareworks is processing on behalf of its customers, including:

- Order files which have been created.
- e-mail address and name of user in Shareworks if no longer required
- data derived from the creation of content

Shareworks is set up with a default deletion policy that

involves:

- Automatic deletion of order files after 180 days
- Automatic deletion of logfiles after 180 days

Please note that the employee's data, including name and e-mail, is kept in the platform, until the customer actively deletes the employee's user profile, e.g. in connection with dismissal of the employee.

Can Shareworks delete customer data?

In general, data, including user data added by the customer to the Shareworks platform, can be irrevocably deleted by the customer's registered users having such deletion rights directly in the platform.

Specific requests for deletion of data, including specific data about users, can also be made with written request to Shareworks.

Does Shareworks retain customer data after termination?

Shareworks allows customers to export their raw data at any time in industry standards such as JSON, CSV or XML for metadata. In addition, customer data may be deleted upon request upon termination as set forth in the section above.

If Shareworks does not receive such a request prior to termination, all customer data at Shareworks will be automatically deleted within 180 days of the termination of the customer contract.

Data security and management

Customers' data is stored in our database system, which contains all of Shareworks customer data.

Our database architecture and logical controls are built around a strong guarantee that no customers can access each other's data. Handling of this approach/access is done by using tokens, keys, etc. which ensures that one customer's data is always kept separate from other customers' data. The way Shareworks ensures that this handling is correct is by automated tests that must solved "lighting green" before it is possible to update the solution. Further, all changes and corrections to the platform or database are reviewed and approved before testing begins. Only by accepting changes and completed tests is it possible to perform the update.

Encryption

All data processed by Shareworks is encrypted.

During transit of data, *HTTPS* and *TLS 1.2* are used, which ensures that should data be intercepted, it will only be encrypted data the interceptors get access to.

Access control

Shareworks access to the database and customer data is subject to policies that ensure that customer data can only be accessed if there is a work-related need to do so in relation to Shareworks delivering their services to our customers, and that access only applies to selected employees. Management continuously assesses whether employees with access still have a work-related need for such access to customer data.

In addition, employees are trained in what appropriate access includes, and logs of access are kept in accordance with the section below in order to monitor and control any irregular access.

Each employee's access to customer data requires multi-factor authentication (Software MFA - Google Authenticator).

Shareworks password policy assumes that:

- passwords must be at least 8 characters
- they must contain lowercase letters and they must not contain part of the username
- users cannot reuse their passwords.

Authentication & Authorization

Shareworks software platform uses its own proprietary login functionality, but also allows login with established M365, Google, or other data providers.

It is also an option to setup an integration between Azure AD and Shareworks. By doing that you can manage your users directly from your Azure AD. Both Authentication and Authorization (roles and permissions) can be managed.

Logging

Shareworks keeps various logs, including:

- technical monitor for operations
- audit log for change and development of the hosted platform
- audit and user logs for platform actions

Technical monitor for operation

We log constant response time, CPU load, RAM usage, database read and writes, index usage, and disk usage related to platform activity for the purpose of monitoring availability, response time, failure rate, server load, and more to ensure the platform is always in a healthy state.

Dashboards with this information run in real time and with relevant alerts set up.

Audit log for hosting platform changes and developments

Shareworks employees' access to the backend systems and management console in AWS is logged continuously.

In addition, all releases and/or code changes are logged and stored so that all changes can be traced back in time in the event that there is a need to recreate previous versions of the platform.

Audit and user logs for platform actions

Logging actions in the platform is based on user interactions and is divided between an *audit log* and a *usage log*, each serving their own purpose.

The audit log is the log containing events performed by the user that Shareworks wishes to store within the framework of Shareworks deletion policies as agreed with the customer. The purpose is to be able to track who has performed what actions in the platform. The log includes conditions such as successful login, changing user permissions, creating or deleting content etc.

Usage logging is functional usage monitoring. The purpose of this logging is to further product development in the interest of the customer based on a deeper understanding of the customers' actual use of the platform and Shareworks performance.

HR/company policies

Shareworks runs background checks on all employees or contractors who will work for Shareworks before starting up work for Shareworks. In addition, it is ensured that such individuals have sufficient qualifications to be able to safely perform the tasks in question. Further, all employees and relevant contractors having access to customer information as part of performed services, signs confidentiality agreements that ensure that any customer information is kept confidential.

Shareworks uses subcontractors to provide the software service to Shareworks customers. In addition to the obligations related to switching or adding new subcontractors in the dedicated data processing agreements, Shareworks has a fixed policy for choosing new suppliers, which ensures that only suppliers with high security standards are selected.

The Danish state's minimum technical requirements (2023)

Shareworks continuously considers the minimum technical requirements imposed on Danish government authorities and ensures that the requirements for each minimum requirement are complied with when designing Shareworks safety measures – this is ensured by following the compliance criteria set out in the guideline instructions published by the Danish state.

GDPR

The customer is the data controller for the personal data added by the customers to the Shareworks platform and data created in the platform. Shareworks is the data processor of the customers data for the purpose of providing the Shareworks software services to the customers. Shareworks is thus subject to the instructions of the customer for such processing.

The requirements for Shareworks processing of personal data on behalf of customers, and the parties' relations in relation thereto, are regulated in a separate data processing agreement, and Shareworks never begins processing until such a data processing agreement has been agreed with the customer.

Shareworks data processing agreement is based on the Danish Data Protection Agency's standard data processing agreement, which ensures that the requirements for a valid data processing agreement, cf. GDPR, Article 28, are met.

Shareworks customers have full control over what information they add to the Shareworks platform and are obliged to ensure the legality and legal basis for using Shareworks for the purposes requested by the customer.

Shareworks values GDPR compliance and is dedicated to enabling our customers to comply with their obligations as data controllers under the GDPR.

Audits and security certifications

Shareworks stores customer data with our hosting provider, cf. the section above, which have annual audits based on the following internationally recognized standards e.g. ISAE 3402, ISAE 3000 or SOC reports.

Threat and vulnerability management

Patching and updating of the production environment is carried out by our trusted hosting provider in close cooperation with Shareworks.

The hosting environment is protected by anti-malware scanning software.

Shareworks periodically engages ethical hackers for manual penetration tests.