# ShareSimple - Tecnical Whitepaper

A Secure Mail solution.

## Security and Compliance

Published: September 2018[1]

**Danish National Data inspection Office recommendations:**

Datatilsynet - https://www.datatilsynet.dk/emner/persondatasikkerhed/transmission-af-personoplysninger-via-e-mail/

# Introduction

**Introduction**

ShareSimple offers you help to comply with the new regulations regarding the requirements to be able to share sensitive data encrypted when shared over mail as part of the General Data Protection Regulation (GDPR). ShareSimple provides you with a simple way to share sensitive data over email with end-to-end encryption, consent management, One Time Passwords and full audit log.

ShareSimple offers the simplest & safest way to:

- Send data for download, or view-only
- Request data, and keep received data secure
- Obtain the proper consent for sharing data
- Get documents reviewed and signed

Security and compliance:

- All send and receive transactions use 1.2 TLS
- View-only mode limits instances of data
- Audit logs on all consents & transactions
- Data stored in 2048 bit encrypted private cloud on Azure

ShareSimple can be downloaded from the Outlook App store and start sharing data safely in 5 minutes.

No further installation needed.

# What does ShareSimple provide?

**ShareSimple Consent Management**

Consent is a module where you can customize your consent forms when receiving data from a person OR before you allow a person to download sensitive data. This ensures your company a full log of all sharing of personal data. Consent forms are delivered in generic form and must be revised by your company before use.

**ShareSimple Plugin**

ShareSimple is delivered as an O365 plugin for Microsoft and can be downloaded from MS App store, Appsource during Oct. 2018. Until release, installation file will be needed. . It is also possible to install the Add-In for all members in an Office365 tenant

# ShareSimple architecture

**ShareSimple Plugin**

Customers will receive their own Azure blob server, placed in West Europe (Holland), Managed by Microsoft.

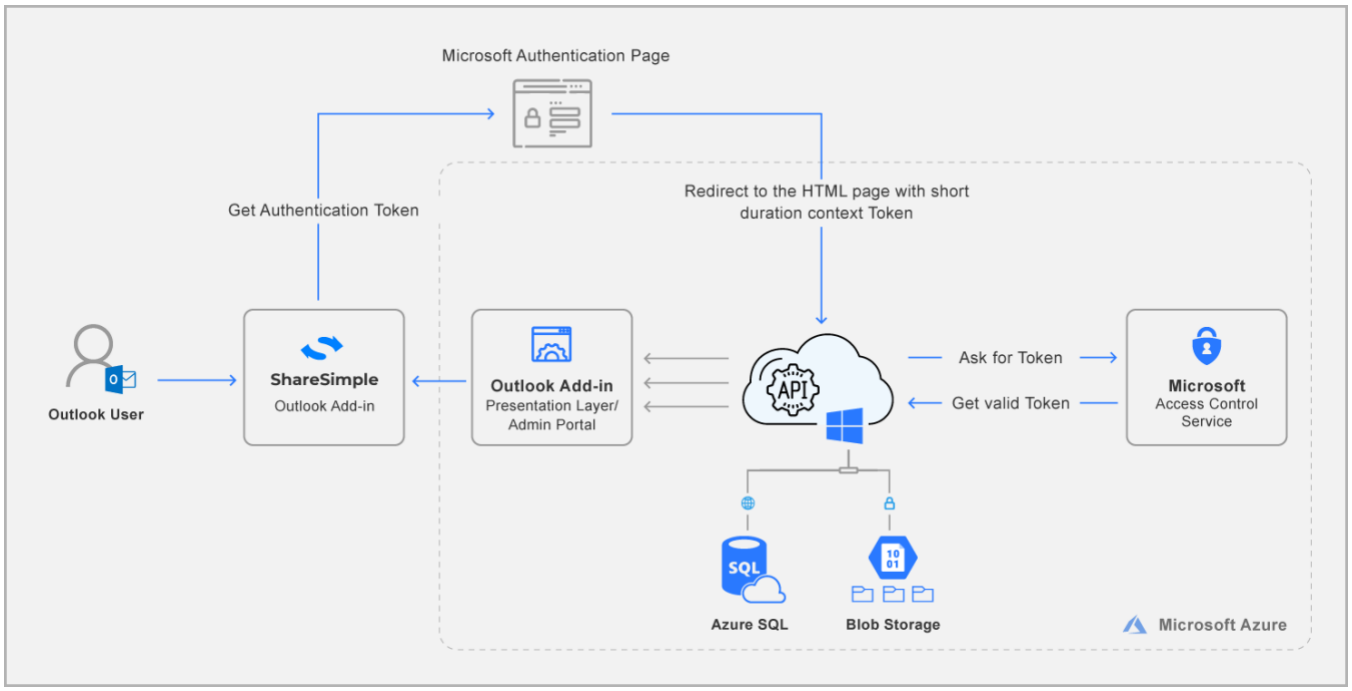
**Accessing the Add-in:**

Users will be able to access the application with a valid Office 365 account. The authorization follows Microsoft OAuth2 process to access any features of the Add-in.

**The Backend API and Portal:**

The backend API and admin portal are hosted in Azure Cloud. Blob Storage is used to keep the files for a temporary period.  Azure SQL is used to keep the related information.

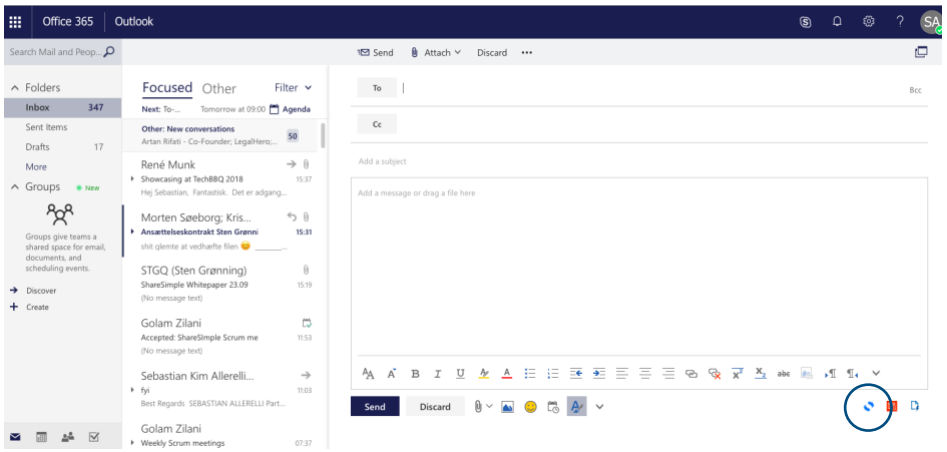
**Below is a high-level diagram showing the solution**

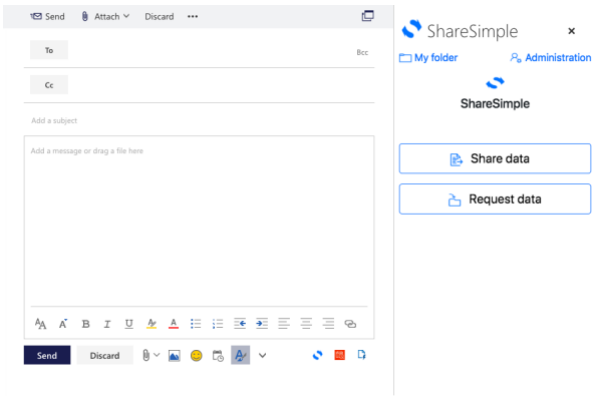


# How ShareSimple works

### Start ShareSimple

- ShareSimple is activated when starting a new mail and pressing the ShareSImple icon



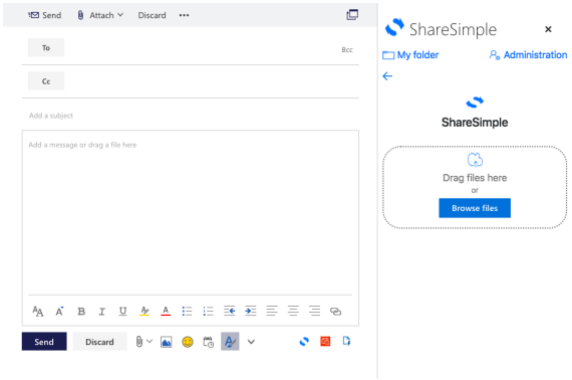




### Share Data through ShareSimple

- When the ShareSimple user wants to **Share** data press the “Share Data” button. This choice is followed by two options:
    - Allow the receiver to view data only or..

- Allow the receiver to Download data (this choice will trigger a consent from the receiver, that they acknowledge they become data owner and understand the responsibility.

Notes:

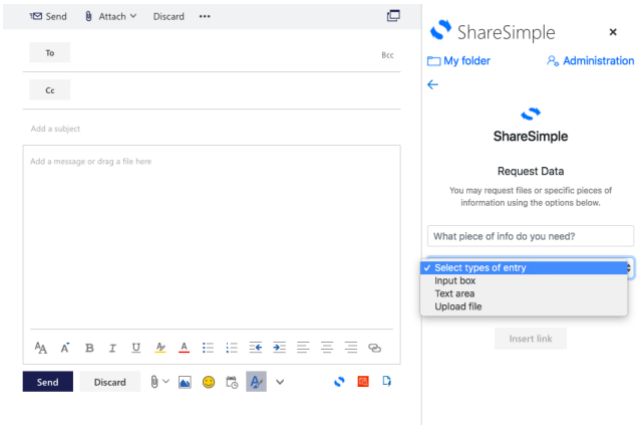



- The receiver will be prompted for a One Time Password before opening link, to ensure it is ONLY the intended receiver opening the data.
- The receiver can ask permission to download the shared data in View-Only mode. This will trigger a request flow where the sender will be informed that the receiver wants to download a file. The sender will then have to approve or reject. There is a build in time limit where the data is only available for 32 days or less.
- All actions will be logged.
- Data shared to a receiver will maximum be stored for 32 days or less.

**Request Data through ShareSimple**

- When the ShareSimple user wants to **Request** data press the "Request Data" button. This choice is followed by one option (all data requests will prompt a consent form with the receiver, when providing data stating that data is given freely and can be used according the companies policies):
  - Name the data that needs to be requested
  - Chose the format of data to be requested. Options are:
    - Short txt format (e.g.. social security number, account number, passport number)
    - Long txt format (e.g.. Sensitive information about health or other)
    - File format request (e.g. Passport image, board member info, other)

Note:



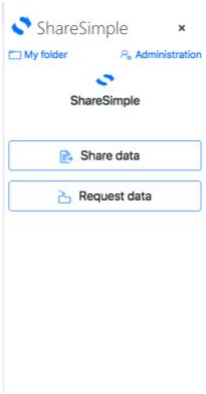

- The receiver will be prompted for a One Time Password before opening link, to ensure it is ONLY the intended receiver entering the data.
- All actions will be logged.
- Data shared by the receiver will only be stored for max 32 days (or less, depending on the company ShareSimple admin)

**Receiver:**

The receiver of the sharing request will receive a link to a portal, encrypted with TLS 1,2 (Transport Layer Security) where the requestor can upload or receive data in secure manner.

# Cloud infrastructure

ShareSimples cloud infrastructure is a purpose built, preconfigured solution that provides the capacity and lifecycle management for the system. Our design point is to focus on continuously delivering the services that applications depend on.




The ShareSimple solution components such as software infrastructure, services, and subscriptions exhibit management interfaces that are intuitive to the end customer.

**Management Capabilities include:**

- **Intuitive experiences:** The ShareSimple portal allows a surface for the common actions the ShareSimple System Administrator or System user needs to take, allowing them to make decisions quickly and intuitively.
- **Monitoring:** Monitoring, notifications and management capabilities that allow the System Administrator to ensure compliance, performance, and service that underlie tenant workloads.
- **Business terminology:** ShareSimple provides several capabilities that are dependent on your ShareSimple system role. There are four levels:
    - System Administrator / purchasing the system, setting up the company, can add users, modify templates, bypass processes.
    - System user / Typical internal daily user of the system.
    - Requestor / Requester of data. A user has NO access to any system data in ShareSimple.

Security and Privacy: ShareSimple has a secure by design approach across network, data and management.

Software lifecycle management: ShareSimple will have validated workflows experience to enable incremental expansion and replacement of failed components.

# Scale

ShareSimple will provide scalability in multiple dimensions: This enables choice and flexibility to meet Legislation requirements and can grow with their needs. The approach to ShareSimple scale is derived from Azure. Cloud: Azure Resource Manager spans across the entire system and provides a single-entry point to the cloud.

- Regions for storage: The storage of the user's data during "REST" will be determined based on the user's location. All EU user data will be stored encrypted for 32 days on MS Cloud storage:
    - EMEA are all stored on MS servers in Holland. (West Europe: Learn more by clicking here)
- Scale Units: There are no limitations.

# ShareSimple data structure

**How to transfer data**

Different structures and different formats, data can be transferred from a company to ShareSimple in 2 different ways.
Common for all companies are that when data is being shared it has to be handled in a secure and documented way and that data has to be forwarded in a Encrypted, structured, and logged format.

The 2 different way that ShareSimple supports are:

1. Drag and drop.
2. Open file structure and choose.

# Delivery and continuous updates

A team is always working for its improvement and updates of new features and functionality. The Add-in dependent on Microsoft platforms like Outlook, Azure, Authentication policy.

The team of ShareSimple always keep on eyes on those policies and regulation and make the application compatible with those policy. On the other hand, any policy regarding GDPR or other regulations are also followed making the changes in the application if required.

# Prequisites for ShareSimple installation

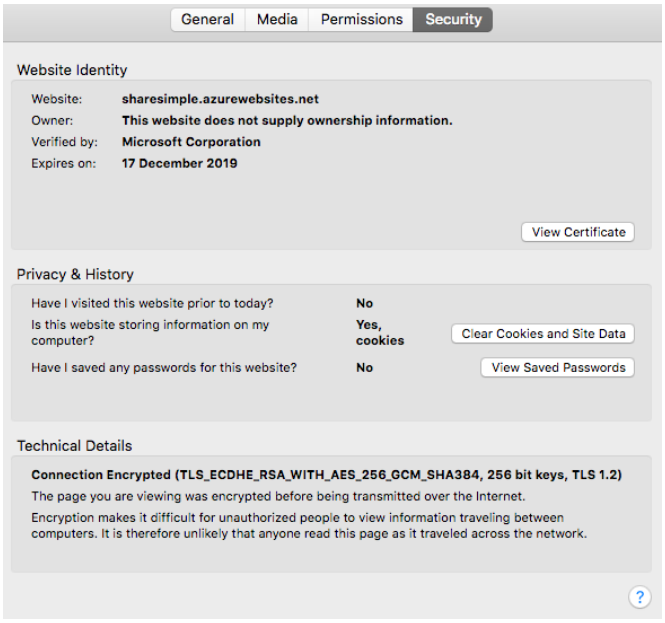
The tool is based on Office 365 Add-in model; therefore, it follows similar prerequisites as Microsoft recommends. Following are the list of prerequisites:

- Outlook 2013 or later for Windows
- Outlook 2016 or later for Mac
- Outlook for iOS (Coming soon)
- Outlook on the web for Office 365

# ShareSimple Security

**Data encrypted in transit**

ShareSimple is using encryption during transit with an asymmetric certificate encryption on both the transport layer (https) and the database connection (different certificate). This is combined with a OTP (One Time Password) which is prompted from the user. Encryption in transit is mandatory for ShareSimple traffic, requires authentication and is not publicly accessible. ShareSimple website portal is encrypted with TLS 1,2 (Transport Layer Security).




**Data encryption at rest**

ShareSimple uses 'always encrypt protocol' for the data. ShareSimple provides a granular encryption of all data and centralised key management from an Azure key vault. ShareSimple encryption algorithms operate on block lengths of 2048 bits. All customers data are kept in Azure private blob storage.

**Encryption key**

The Encryption Key are managed by Azure Key Vault and maintain the highest level or Encryption Key supported by Azure, currently the key size is RSA 2048. In case of breach or suspicion hereof, the keys can be rotated easily, and new keys are generated and applied.

**Backup**

The data shared with customers are kept only for seven days. All requested customer's data are kept in Azure private blob for maximum of 32 days, However, the company can reduce the days as deem necessary.

After 32 days, data is automatically deleted by a scheduled job that runs every day, early morning. Following figure shows the running cycles of the delete operation of customer data.


*Figure 1: Configured scheduler for deleting data at rest*

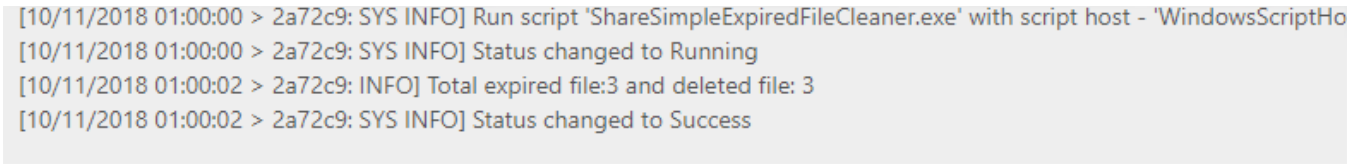



*Figure 2: Delete logs of number of files deleted for each operation*

The Admin user of a company can see the audit log from the administration page to identify which file is deleted with the deletion date.

# Data loss prevention

Malware and targeted attacks can cause data breaches, user error is actually a much greater source of data risk for most organizations. ShareSimple relies on MS Azure data loss prevention (DLP) technology that identifies, monitors, and protects sensitive data.

# Privacy by design

When you entrust your data and the data of your requesters to ShareSimple you and your requesters remain the sole owner of this data: you retain the rights, title, and interest in the data you store in ShareSimple. The data you store in ShareSimple is "your data and the data of your users."

It is with this clarity of principle that we ensure that we maintain your privacy and operate our online services with certain key principles:

- We use your data only to provide you with the online services you have paid for, including purposes compatible with providing those services.
- We do not mine your personal data for any purposes.

- If you ever choose to leave the service, you can take your data with you with full fidelity
- We tell you where your data resides, only you have access.
- Access to your data is strictly limited.

Beyond this, we have privacy controls to allow you to configure exactly who has access to what within your organization. Strict controls and design elements that prevent mingling of your data with that of other organizations using ShareSimple and from ShareSimple datacentre staff having access to your data.

In addition, ShareSimple redirects government requests for your data to be made directly to you unless legally prohibited and has challenged government attempts to prohibit disclosure of such requests in court.

## Privacy by default

In addition to service-level capabilities, ShareSimple enables you to collaborate through the use of transparent policies and strong tools while providing the distinct ability to control information sharing.

- Data will be encrypted with a RSA 2048-bit encryption key and only accessible to your company.
- Rights Management in ShareSimple—Allows administrators to specify access permissions to requests, ongoing work and audit logs. This helps you prevent sensitive information from being printed, forwarded, or copied by unauthorized people by applying intelligent policies.
- Privacy controls for One Time Passwords — ShareSimple provides verification functionality that has a number of privacy controls. This can be adjusted by the system admin in the setup page.

Privacy controls for new system users are always set to highest privacy setting by default. This setting can only be edited by the system admin for security purposes. One example is that a system user by default only has access to their own folder. Shared folder access can only be given by the administrator. Another is that a system user cannot see the data of a requester in the email body, only in the folder option where the sensitive data resides.

## Auditing and retention policies

By using ShareSimple auditing policies, all events will automatically be logged on your users, including Saving, deleting and editing data. Audit log is enabled as part of an information management policy, administrators can

view the audit data and summarize current usage. The system administrator can use these reports for internal or external audits.

For business, legal, or regulatory reasons, ShareSimple retain e-mails sender and receiver, related to the requests. The records management technology in ShareSimple is accomplished by using retention policies.:

- **Automatic retention policy tags for requests and sent Items.**

The retention period for data collected is 32 days by default but can be lowered by the company admin. After this, only the logs and tags will remain.

# Integrated systems

ShareSimple is purchased as an online Outlook application. It requires the below browser version to run from the web.

Internet Explorer 11, Edge

Latest versions of Safari

Latest version of Chrome

Latest version of Firefox.

# Help

Please help find videos here: https://www.youtube.com/channel/UCrcRJvCq6tNMiVYFXSOb1xA/featured