IT Security Concept

Table of Content

I. Information Security Management

1. Is a company-wide, risk-oriented Information Security System (ISMS) available?

An ISMS is implemented through Microsoft Data Governance. This is activated via the Office 365 standard functions and offers a standard data retention of 10 years.

2. Who is responsible for information security?

Responsible is the CEO Christian Groß.

3. Which technical and organizational measures are implemented to ensure information security?

Only Microsoft Azure components with logging, backup and security are used. None of these services is self-hosted. The source code, deployment and all backups are only performed with Microsoft Azure services.

4. Is an emergency management system in place, are emergency plans in existence?

Yes, emergency plans are in place. Through release management, backup and Azure technology, the service can easily be restored.

5. Is it ensured that only trustworthy employees are involved in safety-relevant activities?

Access to security-relevant information via the live system is limited to three employees (based in Germany).

6. Are all employees committed to information security and data protection? Are they trained in appropriate handling of customer data and are they regularly sensitized?

Access to security-relevant information is limited to three employees (based in Germany), who have sole access to the productive environment. All our employees are sensitized in handling customer data and are familiar with our security standards regarding data protection.

7. Is physical security ensured?

The physical security of the data is guaranteed by the Microsoft Data Centre in Europe.

8. Is there a process and a concept for prevention, detection and treatment of security incidents? Does an ISIRT/CERT exist?

Security incidents are handled by Microsoft Threat Management.

9. At which locations (countries) does the provider have its own or third-party branches, data centers, subsidiaries or subcontractors? Are there locations or employees outside the EU?

The company is located in Fürth, Germany. Another branch office exists in Wismar, Germany. Hosting is exclusively provided by Azure in Europe.

10. How are the data centers used for service delivery connected to the Internet?

Details on the connection of the data centers used can be requested from Microsoft.

II. Security of service delivery

1. Which technologies are used for service delivery (e.g. operating systems, application servers, programming languages, frameworks, APIs)

Systems and application servers: Windows Server 2016, Azure Website. Azure Blob Storage, Azure SQL Database, Azure Log Analytics, Azure Application Insights, Azure VM Services, Azure Network Service, Azure Resources Management Recovery Service, virtual network, cdn, storage account

Programming languages: c#, javascript, typescript

Frameworks: SPFx, Telerik, SharePoint Online CSOM, ASP.NET MVC; API: SharePoint Online, Office 365 Graph

2. Which applications and protocols are used to access the service?

The service is accessed via Microsoft Teams. The communication protocol https is used for access.

For the usage of Teams Applications by Solutions2Share an App Registration is needed (Azure AD App Registration), which must be consented by the administrator.

These consist of the following: permission for sign in and read all users full profile; read and write all groups; permission for Microsoft Graph

Directory.Read.All (to Read Company Domain Name)

Directory.ReadWrite.All (optional for Guest Access)

Group.ReadWrite.All (for creating and concerting Teams) – only Teams IDs are saved

Mail.Send (Sending Emails as notification – Feature optional) - this data is not saved

Notes.ReadWrite.All (to create and provision OneNote) – this data is not saved

User.Read.All – User IDs get safed for Group Ownership – nothing else concerning users is saved

This application will be used for every customer and will also be used to access the tenants.

This application is connected to S2S multitenancy Azure environment.

Solutions2Share only uses Team IDs for its applications. Solutions2Share applications do not process Teams Data, Personal Data or Content of Teams.

The customer can also host the complete application in its own Azure environment. There no data is getting passed and every process only happens in the customers tenant.

3. Do effective programming and hardening guidelines exist?

Programming and hardening guidelines are ensured and attested by the Rencore certification of the development process "Best Development Practices" for SharePoint Development.

4. Do regular code reviews, functional, component and integration tests take place, taking into account security aspects?

The existence of regular code reviews, functional, component and integration tests considering security aspects is ensured and attested by the Rencore certification of the development process "Best Development Practices" for SharePoint Development.

5. Is it ensured that all changes are implemented through a systematic change management process?

The development of our solutions is performed in the form of agile software development in sprints using Microsoft's Azure DevOps. Deployment only takes place after automated and manual testing and after approval.

6. Is there a concept for authentification and authorization? Which methods for authentification are available? Are there defined processes for identity and access management? Are federations and/or SSO concepts supported?

Authentification is handled by Microsoft SharePoint / Office 365. We provide no own authentification, we are only passing on the token.

7. Which employees of the provider and which third parties have access to the customer's data and for what purpose? How is this restriction guaranteed and controlled?

Access to sensitive data via the live system is restricted to the following two employees:

Christian Groß, CEO
Bastian John, Senior Developer

There is no possibility of external access. The restriction of access is controlled and ensured by Azure Authentication Log.

8. Do accounts exist for access to customer data in the form of support users, emergency users or backdoors?

There are no further access possibilities than the accounts of the two employees mentioned above (see section II., 7.)

9. Is regular monitoring and logging including regular evaluation and anomaly analysis guaranteed?

Monitoring and logging are guaranteed by Azure Log Analytics. Anomalies are immediately forwarded to the support system using a trigger.

10. What measures were taken to secure the data centre?

Microsoft data centres are used. Detailed information on security can be obtained from Microsoft.

11. What measures were taken to secure the servers?

Servers from Microsoft are used. Detailed information on security can be obtained from Microsoft.

12. What measures have been taken for network security?

The network security is guaranteed by Microsoft. Detailed information on network security can be obtained from Microsoft.

13. What measures have been taken for application and platform security?

Application and platform security are guaranteed by Microsoft. Detailed information on application and platform security can be obtained from Microsoft.

14. What measures have been taken for data security?

The data security is guaranteed by Microsoft. Detailed information on data security can be viewed at Microsoft.

15. How is a separation of the data of different customers guaranteed?

The separation of the data is guaranteed programmatically. Logs of different customers are stored separately. Only URLs and IDs and the settings in the Solutions2Share applications are stored. No content from the customer is stored.

16. Is the secure transfer of data from and to the platform guaranteed? Which protocols are used (for initial provision, return, regular exchange)?

The secure transmission of data is guaranteed by the communication protocol https.

For the transmission of passwords, SSL encryption is used.

17. Is a regular data backup guaranteed? Are there cycles? Where is the storage location of the backups?

A regular data backup is guaranteed by Microsoft Azure. Within the scope of the standard setting of Azure used by us, a 14-day backup is provided.

18. Are regular restore tests performed?

Solutions2Share does not perform such tests itself, as they are already performed by Microsoft.

19. Is the service fully or partially provided by third parties? How is compliance with the necessary security level ensured (commitments, audits, certifications)?

The service is entirely developed by us and is hosted entirely on Azure. Apart from Microsoft, no other party is involved.

20. Is the code examined by third parties for security vulnerabilities and backdoors before going live?

The examination of the code for security vulnerabilities is ensured and attested by the Rencore certification of the development process "Best Development Practices" for SharePoint Development.

21. Does the service provision involve the execution or installation of code on the customer's side?

Any SPFx Web Parts used will execute JavaScript code in the browser.

22. Does the use of the service require certain settings or versions of browsers, operating systems or are there other technical dependencies?

Reference is made to the browsers recommended by Microsoft for Office 365. We follow these recommendations and adapt our source code accordingly.

23. Can emergency operation be guaranteed in an emergency? For which scenarios do emergency operation concepts exist?

Only the emergency operation concepts provided by Microsoft Azure Active Directory exist.

III. Treatment of personal data

1. Is it a case of data processing by order in the sense of the DSGVO?

No, no personal data are processed.

2. What types or categories of data are collected, processed and/or used?

Following data types/categories are stored:

Tenant-URL; Tenant-ID; App Catalog-URL; Template Name; Teams IDs and settings of the Solutions2Share applications.

3. Where is the data stored/processed? Where are the data centres located?

Only Microsoft data centres in Europe are used to process and store data.

4. Are all other legal requirements met?

Further legal requirements for the service are not known.

5. Is it ensured that no subcontractors are used who do not fulfil the conditions for processing personal data?

Apart from Microsoft, no third parties are involved. The conditions for personal data processing are therefore guaranteed.

IV. Customer relation

1. Is there an exit control with assured formats and open interfaces for data return? What are the costs involved?

Except for URL, GUIDs and their settings in the Solutions2Share applications, all other required data is stored in Microsoft 365. All your data can be completely deleted on demand. This does not incur any costs for you.

2. Is the customer regularly informed about security-relevant changes, security incidents and the results of audits and penetration tests carried out?

Our customers are informed about all security-relevant changes via our newsletter and our knowledge base.

3. Does a classification of security incidents already take place at the provider? How does this classification work?

Since no separate authentication provider is used, a security incident can only through Microsoft Azure. If a security incident should occur, it will be reported at the earliest possible time.

4. Is it ensured that the customer is informed immediately about security incidents that may affect his data?

All kinds of failures, maintenance and safety incidents will be communicated to you by newsletter. General, safety-related information can also be accessed via our knowledgebase.

5. Which subcontractors are used to provide the services?

No subcontractors are used.

6. Under what conditions is there an obligation to disclose data to third parties (in particular government authorities) and to whom? Is the customer informed about data transfers?

Customer-related data will not be disclosed under any circumstances. There are also no legal obligations to pass on data to third parties.

7. Is data - e.g. also usage data, content, license data, company data, account data - passed on to third parties (e.g. parent or subsidiary companies, partner companies)?

Under no circumstances will customer-related data be passed on to third parties.

8. Does the customer have the right to audit the security mechanisms and processes of the provider (himself or through an independent expert)?

There is the possibility of an audit by employees of Solutions2Share. Any costs incurred must be paid by the customer.

For an auditing by a Microsoft employee, please send your request directly to Microsoft.

9. Is the operation or provision of the data in the event of insolvency of the provider guaranteed in compliance with confidentiality commitments and data protection requirements?

In the event of insolvency, the service can easily be continued in your own azure.

10. Is it ensured that the customer's archiving and retention policies are implemented?

Since only URLS, GUIDs and tool settings are stored, there are no archiving and retention policies to ensure. The deletion of all data can be done on request.

V. Risks

1. What are the residual risks for the customer when using the service?

We are not aware of any risks for the use of our service.

VI. Reporting

1. Are planned maintenance and planned changes actively communicated to the customer in advance?

Before each maintenance the customer is informed in time by a newsletter. This newsletter includes the date of the release as well as information about new features, solved problems and further changes.

2. Is there a reporting regarding changes made to the service?

Release notes are communicated both in the newsletter and in the knowledge base.

3. Is there a reporting on the use of the service by the customer?

No, there is no storage of the data. Only the number of license accesses are counted.

4. Is there a logging of actions in the service? What information can be provided to the customer?

On request, the log can be provided to the customer as a csv file. Any costs incurred are to be covered by the customer.

5. Is the customer informed about faults and their processing status?

The customer is informed about processing status and malfunctions via a service dashboard as well as via newsletter.

6. Is the customer promptly informed of any changes to the competences and responsibilities affecting him?

If actions of the customer should become necessary, the customer is informed in time by newsletter.

7. Does a general reporting take place without request? At what intervals does the customer receive the report information?

Information about tickets, invoices and service hours can be viewed at any time in the online system.

Christian Groß

CEO Solutions2Share