Performance Characteristics Data Security

Mindbreeze InSpire SaaS

Valid from 01.01.2024

Public

For reasons of simpler readability, gender-specific differentiation, e.g. users, has been omitted. In the interest of equal treatment, the corresponding terms apply to both genders.

1 Introduction

Protecting personal data and safeguarding the information that customers search with Mindbreeze InSpire SaaS is a key concern for Mindbreeze. In this document, Mindbreeze documents how Mindbreeze InSpire SaaS protects and processes data.

Mindbreeze InSpire SaaS Customers may contact Mindbreeze with questions regarding the processing of personal data via the email address privacy@mindbreeze.com. This contact option is also available for security and data protection incident reporting and communication.

2 Performance

2.1 Reversibility and termination process

Mindbreeze is expressly entitled to permanently - i.e., non-recoverably - delete the data stored by the Customer in the Mindbreeze InSpire SaaS data centers after a period of at least 4 weeks and at most 6 weeks, calculated from the termination of the contract. This deletion will be carried out by Mindbreeze irrespective of the quality, nature, value and significance of this data for the Client.

(see Performance Characteristics Data Center Operation Mindbreeze InSpire SaaS, item 2.3).

Objective	
Time period for access to user data (Data retrieval period)	In the event of termination of the contract, Fabasoft shall deactivate the access options to the Fabasoft Cloud for the Customer upon termination of the contract. See Performance Characteristics Data Center Operation Mindbreeze InSpire SaaS, point 2.3
User data retention period (Data retention period)	If the contract is terminated, Mindbreeze shall be entitled to delete the user data no earlier than 4 months and no later than 6 months after termination of this contract. See Performance Characteristics Data Center Operation Mindbreeze InSpire SaaS, point 2.3
Additional retention of user data (Residual data retention)	Not provided

3 Security

3.1 Service reliability

The availability of Mindbreeze InSpire SaaS Services is designed to be highly available The data centers are based on the Tier III specification of the Uptime Institute. For more information, please refer to the document "Data Center Operation Performance Characteristics".

Objective	
Redundancy	See Data Center Operation Characteristics
Service reliability	See Data Center Operation Characteristics

3.2 Authentication and authorization

The following authentication methods are available.

Authentication

- Single sign-on (SAML 2.0)
    - Customer must operate a SAML 2.0 Identity Provider accessible by Mindbreeze InSpire SaaS via the Internet. The authentication service of Mindbreeze InSpire SaaS must be configured as a service provider in the customer's identity provider. For the configuration in Mindbreeze InSpire SaaS, the required metadata (metadata.xml) of the Identity Provider must be provided by the customer.
- OAuth 2.0 using JSON Web Tokens
    - For the configuration, the customer provides the public keys for the validation of a JWT (JSON Web Token). Also the properties to be validated.
- Username & Password
    - The username is a valid e-mail address of the user.
    - If the user has forgotten his password, a new password can be requested through the support. The user will then receive an email to reset the password.
    - The password is not stored by Mindbreeze in plain text and cannot be reconstructed by Mindbreeze.

Authorization

Authorization of access to user data is done via the permission of the data source. No permissions are managed in Mindbreeze InSpire SaaS. Only hits that the respective user is allowed to access are displayed.

Objective	
Security of authentication procedures	Current state of the art
Authentication procedure	Username and password, single sign-on (SAML 2.0), OAuth 2.0 via JSON web tokens
Withdrawal of rights in case of organizational exclusion	On data sources: On the next delta indexing. When accessing Mindbreeze InSpire SaaS Backend: immediately after deactivating a user account by notifying the customer to support.
Protection of credentials	Passwords for logging in are stored in a separate service in encrypted form and cannot be reconstructed.

Support for third-party authentication methods	SAML 2.0, OAuth 2.0 using JSON Web Tokens

3.3 Encryption

Access to Mindbreeze InSpire SaaS is only possible via HTTPS with TLS encryption.

User data is stored on encrypted hard disks (SEDs) that meet at least the FIPS 140-2 Level 2 standard or a comparable standard, or encrypted file systems (EFS). This protects the data in the event of hardware loss.

Objective	
Protection against brute force attacks	Transport: HTTPS with TLS encryption Storage: SEDs, EFSs
Key protection	Keys are created on the target system and do not leave the target systems. Access to the keys is secured via restrictive access rights (TLS) or passwords (for example, SEDs or EFS).

3.4 Logging and monitoring

Auditing

The following auditing information is collected as part of the traceability process:

- Read access to documents

Audit logs can be viewed in Mindbreeze InSpire SaaS by administrators of the customer with appropriate authorization. Audit log entries are kept for at least 12 months. Customer has the option to export the audit log entries and keep them separately. The audit log entries will be permanently deleted at the latest after termination of this contract together with the user data after a period of at least 4 weeks and at most 6 weeks (calculated from the termination of the contract).

Logging

Fabasoft app.telemetry records every request (HTTPS requests) to the Fabasoft Cloud over time. This transaction information is recorded at the user's workstation in the web browser. This transaction information is used exclusively for ongoing service improvement. The logging does not include user data. The retention period for this transaction information is defined individually for each application and level and is a maximum of 12 months.

When logging operating system and basic software events as well as application-specific events, the information that the respective systems provide by default is logged. Operating system, basic software events and application-specific events are kept for a maximum of 6 months.

Monitoring

Fabasoft app.telemetry is used to monitor the individual system components of Mindbreeze InSpire SaaS and to monitor performance and availability from a user perspective.

Objective	
Selection of data in the log	Security-relevant user data is not logged
Access options of the customer to logs	Access to auditing information is possible for authorized users of the customer in the , there is also an export of auditing information possible.

3.5 Audits and safety verifications

External and internal security analyses as well as audits of the technical, physical and organizational security measures and operating processes make a significant contribution to the security of your data.

Objective	
External verification of security and data protection through certifications and audits	ISO 9001:2015 ISO/IEC 20000-1:2018 ISO/IEC 27001:2022 ISO/IEC 27018:2020 ISAE 3402 Type 2 BSI C5 (Cloud Computing Compliance Controls Catalogue) SOC II Type 2

The Customer may request in writing an audit by independent bodies to prove data security measures or compliance with data security measures, or may conduct an audit itself, provided that the Customer itself demonstrably has the necessary expertise to conduct such an audit.

The customer shall explain and justify the necessity of the audit to Mindbreeze in writing within 14 days of its request at the latest. An audit is to be carried out without disrupting Mindbreeze's operations if possible. The procedure, the selection of the auditing body, the scheduling, and the commissioning are then to be agreed between the client and Mindbreeze.

The client requesting an audit must bear the expenses (= costs of the audit, as well as Mindbreeze's expenses) itself. If additional personnel expenses are incurred by Mindbreeze, these additional expenses are to be compensated by the client according to the usual hourly rates (of Mindbreeze).

Mindbreeze may also provide the Customer requesting an audit with the internal regulations on conducting an audit. The customer must comply with these internal regulations.

The Client, will provide Mindbreeze with the documentation of the audit in the form of the entire audit report.

Mindbreeze may also comply with the Client's request as a matter of priority in the form of providing the Client with a summary of the current audit reports of audits already performed.

In any case, an appropriate non-disclosure agreement (NDA) must be signed in advance between the client and Mindbreeze, as well as with the independent reviewing body.

The summary of the test reports, as well as the test reports themselves, are strictly confidential documents. As a matter of principle, any form of disclosure, dissemination, or disclosure that has not been expressly approved in writing by Mindbreeze is prohibited.

If the submission of audit reports of audits conducted at Mindbreeze becomes necessary for control actions; investigations or measures of the data protection supervisory authority vis-à-vis the Customer, Mindbreeze will support the Customer - upon its request - in fulfilling its obligations vis-à-

vis the supervisory authority and will submit the required audit reports directly to the supervisory authority.

3.6 Governance

Planned maintenance work will be announced by mail to the customer's contact persons at least 7 days in advance. In urgent cases (e.g. in case of imminent danger), maintenance work can also be carried out ad hoc.

Mindbreeze InSpire SaaS updates are generally performed as zero-downtime updates. It is intended that the update process of Mindbreeze InSpire, starts on the next Tuesday after availability of a new version. The news for each update will be documented in the release notes and made available on https://help.mindbreeze.com.

Contractual changes shall be announced at least 14 days before they come into force.

Objective	
Announcement of changes	"Release Notes" at https://help.mindbreeze.com Contractual changes to https://www.mindbreeze.com/contract

4 Data Management

4.1 Data classification

User data

Data that the customer brings into data sources connected to Mindbreeze InSpire SaaS retains the access rights of the data source.

User data is generally not synchronized between locations, but remains in the location in which it was connected. Synchronization between locations is possible with a separate agreement. The client's user data remains exclusively in the power of disposal of the client and is not known to Mindbreeze in terms of content, nor is it subject to direct access by Mindbreeze - without express authorization by the client.

Contact details

Contact data for the creation of user accounts for access to the administration interface is recorded in the following situations:

- a (future) customer provides his contact details in the course of initiating a contract, at the latest when the contract is concluded,.

Contact data can be stored in the data sources and thus synchronized to Mindbreeze InSpire SaaS.

Commercial data

Commercial data is information that is necessary for the processing of the business relationship with the customer (orders, invoices, utilization information of the licensed service packages per organization ...).

Derived data

Derived data is log and transaction information that does not include user data. This information is used solely for the purpose of maintaining operations, service level compliance, and ongoing service improvement.

Objective	
User data processing	No processing of data other than requested by the customer
Processing of derived data	No processing of data other than requested by the customer

4.2 Areas of responsibility

The customer's user data shall remain exclusively in the power of disposal of the customer. The customer is responsible for the legality of the processing of this data, as well as the data protection obligations associated with the data processing.

In cases where Mindbreeze acts as a processor for the Client, any processing of data that is passed on to Mindbreeze by the Client will be carried out exclusively on the basis of instructions from the Client.

4.3 Data portability

The customer's data always resides in its data sources. There is no possibility of obtaining a copy of the data from Mindbreeze itself. The data of the index can be exported by the respective user for the export functionality within the scope of the respective user authorization.

5 Protection of personal data

5.1 Codes of conduct, standards and certification mechanisms

To the extent that data comprises "personal data" within the meaning of the EU General Data Protection Regulation or the respective nationally applicable data protection law, Mindbreeze shall comply with data secrecy and other data protection regulations within the meaning of the applicable EU standards and the national substantive data protection regulations.

Objective	
Codes of conduct, standards and certification mechanisms	The EU standards and the nationally applicable data protection laws are complied with

5.2 Specification of the purpose of use

Mindbreeze does not process personal data for any purpose other than requested by the Customer and necessary for the performance of the contract.

Objective

Intended use	to fulfill the contractual obligations with the customer (Art 6 para 1 lit b DSGVO); for the implementation of pre-contractual measures (Art 6 para 1 lit b DSGVO); for the purpose of legitimate interests of our company or on the basis of legitimate interests of third parties (Art 6 (1) (f) DSGVO), namely • for the purpose of direct marketing regarding Mindbreeze products and services; • for the purpose of preventing cases of abuse; • for the purpose of internal management; • to ensure network and information security; • for archival purposes.

Mindbreeze will process the contact data that Mindbreeze has obtained in the course of the contractual relationship with the Customer in order to send the Customer e-mails, postal letters or advertising brochures for the purpose of presenting Mindbreeze's products (Art 6 para 1 lit f DSGVO). The Customer has the right to object to this processing of the Customer's contact data for the purpose of direct marketing at any time without giving reasons by sending a postal letter to Mindbreeze or an email to privacy@mindbreeze.com. Mindbreeze will process the Client's contact data for this purpose for as long as the Client does not object, but only for a maximum of three years from the last activity. For other forms of direct marketing, Mindbreeze will only process the Customer's contact data if the Customer has given its explicit consent to the processing of its data (Art 6 para 1 lit a DSGVO). If the Customer has consented to the processing of data, the Customer may revoke such consent without stating reasons by sending a postal letter to Fabasoft or an email to privacy@mindbreeze.com**. The processing of the Customer's personal contact data for the purpose of direct advertising is not necessary for the processing of the contractual relationship.**

The customer's contact details will not be further processed for any other purpose.

The following chapters list the data that is collected and processed.

5.2.1 User data

The user data remain exclusively in the power of disposal of the client and are not known to Mindbreeze in terms of content, nor are they subject to direct access by Mindbreeze - without express authorization by the client.

User data will be processed by Mindbreeze on an exceptional basis in individual cases, based on an express written request and/or release of the specific user data by the Customer. Such User Data will be processed by Mindbreeze InSpire SaaS exclusively for the purposes requested by the Customer in accordance with the "Annex to the Main Agreement/Contract for the Processing of Contractual Data Mindbreeze InSpire" and/or the Customer's instructions.

5.2.2 Support

Mindbreeze provides 1st level support for Mindbreeze InSpire SaaS customers. It is possible to enter a support request at https://tickets.mindbreeze.com. By creating a ticket, the name, email address and the problem description are transmitted to Mindbreeze Support. For better traceability of the problem, the user can optionally send a screenshot and log files. This data and the subsequent communication are collected in a support request. The user can access the support requests at any time at https://tickets.mindbreeze.com.

Access to the support requests and the data transmitted in the course of processing is restricted to Mindbreeze support staff and the submitter of the support requests.

5.2.3 Cookies

The Mindbreeze InSpire SaaS Services use so-called "session cookies" after your login, which can be used to identify you for the duration of your visit. The session cookies contain parts of your login data in encrypted form. After the end of the session, session cookies expire automatically.

Mindbreeze InSpire SaaS Services use "persistent cookies" to record information about users who repeatedly access Mindbreeze InSpire SaaS Services. The purpose of using these persistent cookies is to continuously improve our products and services for you and make them easier to use. Individual profiling of your usage behavior does not take place.

5.3 Responsibility

The contact person named in the Mindbreeze InSpire SaaS Agreements will be informed either by registered letter or by email if Mindbreeze observes unauthorized access to the Organization's user data or contact information, as well as if there is sufficient reasonable suspicion. In addition, Mindbreeze will attempt to contact this person by telephone or email as soon as possible.

Objective	
Data theft policy	See text of this chapter.
Documentation	https://www.mindbreeze.com/trust Performance Characteristics data security Performance Characteristics data center operation

5.4 Geographical location of the data

The customer can choose between different locations for the storage of the user data (contractual location). The choice of a location other than the contractual location is only possible on the basis of a separate, special, written agreement.

5.4.1 Data transfer / download third country

Processing by Fabasoft takes place in Germany or in the USA. Therefore, Mindbreeze does not transfer any data from Germany or USA to a third country.

The User Data remains exclusively in the power of disposal of the Client and is not known to Mindbreeze in terms of content, nor is it subject to direct access by Mindbreeze.

The use of Mindbreeze InSpire SaaS on end devices of the Customer in a third country may result in a data transfer to a third country by the Customer. In this case, the customer is responsible for compliance with the applicable data protection regulations.

5.4.2 Inquiries & Contact Points

The Client may contact Mindbreeze for notification and communication of security and data protection incidents, as well as requests for assistance with data protection obligations of the Client (as a data controller) through the following channels:

- By e-mail: privacy@mindbreeze.com
- By mail: Mindbreeze GmbH, c/o Datenschutz, Honauerstraße 4, 4020 Linz, Austria

All requests and inquiries must be made and submitted to Mindbreeze in writing.

In order to prevent abuse of data subject rights by unauthorized persons, the identity of the inquirer or the data subject must be proven to Mindbreeze in a suitable form.

Mindbreeze has a data security team ("Privacy Team") in charge of data protection issues, which can be reached via the channels listed above.

To the extent required by the GDPR or national regulations, Mindbreeze will appoint a data protection officer. The contact details of this data protection officer are kept up to date on https://mindbreeze.com/privacy kept up to date.

5.4.3 Self-service through customer

The user data remains exclusively in the power of disposal of the client and is neither known to Mindbreeze in terms of content, nor is it subject to direct access by Mindbreeze - without express authorization by the client. Management of this user data (e.g. deletion, etc.) can therefore only be performed by the client itself.

A user can independently query his contact data in the data sources and directly edit it himself. Via Mindbreeze Support, the customer can have his contact data deleted, corrected, made anonymous, or transferred - taking into account the legal data protection requirements.

5.4.4 Complaint option

Any complaints or ambiguities related to Mindbreeze InSpire SaaS can be raised for Mindbreeze through the following channels:

- By e-mail: privacy@mindbreeze.com
- By mail: Mindbreeze GmbH, c/o Datenschutz, Honauerstraße 4, 4020 Linz, Austria

All complaints must be submitted to Mindbreeze in writing. To prevent misuse by unauthorized persons, the identity of the complainant must be proven to Mindbreeze in a suitable form.