Technical and Organizational Security Measures

Preamble

When performing the services in accordance with the main contract, we – Smartsign Software AB, Sweden – render purchased services to the customer – hereinafter referred to as the "client" – taking into account the state of the art, the implementation costs and the type, scope, circumstances and purposes of the processing, as well as the different probability and severity of the risk for the rights and freedoms of natural persons, implement the following technical and organizational measures (TOM) to ensure a level of protection appropriate to the risk.

The selection of measures is divided into the following areas:

- Pseudonymization
- Encryption
- Confidentiality and Integrity
- Availability and Resilience
- Controls and Validation

Pseudonymization

Measures for pseudonymization have the purpose of excluding or significantly complicating the determination of the person concerned.

Personal data is stored and merged using a pseudonymized user identification number (User identifier).

Encryption

Encryption measures have the purpose of preventing the use and misuse of the data by unauthorized third parties – in the absence of a key.

- Communication between servers and connected clients is continuously encrypted using the latest technologies and accepted industry standards. Depending on the client of the user, TLS1.2, 256-bit AES in GCM with elliptic curve cryptography and forward secrecy are used.
- Both databases and storage containing customer data are encrypted using AES 256 symmetrical keys meeting FIPS 140-2 Level 1 compliance.
- User passwords are not saved in clear text. A secure method based on cryptographic hash functions is used ("Salted Cryptographic Hash").

Confidentiality and Integrity

Confidentiality and integrity measures serve to protect personal data from unauthorized disclosure, as well as to ensure that the systems function correctly and the data remains intact, i.e. complete and unchanged by external influences.

- The data centers used – unless otherwise agreed or otherwise documented, are Microsoft Azure data centers – which have extensive and modern access controls (e.g. electronic access control systems, camera surveillance, intrusion detection systems, security guards) and implement processes that protect sustainably against unauthorized access (e.g. defined security areas, individual access authorization, role-based authorization concept). More information about the protective measures taken can be found on the Azure Datacenter security overview which can be found at https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security.
- The publicly provided shared cloud services, the client dedicated private cloud services and the development systems, as well as their respective data storage and backup storage locations, are completely separated from each other by separate networks and network segments. Networks and network segments are protected by restrictive firewall rules. System components are reinforced in accordance with generally established and accepted industry standards (e.g. blocking unnecessary ports, regular software updates).
- Administrative access is only possible via secure connections (VPN with end-to-end encryption, separate management networks, 2FA) and is logged in log files. Access to administration and maintenance are clearly assigned to natural persons.
- The granting of access rights takes place in compliance with specific approval regulations and is documented. The principle of least-privilege ("need-to-know principle"), i.e. users only receive the access that is necessary for the fulfillment of their tasks, is used. Access rights to IT systems are regularly checked and withdrawn as soon as the business need for access no longer exists. Critical administrative combinations of rights are monitored ("separation-of-duty principle").
- All employees are familiar with the handling of confidential data and are obliged in writing to maintain confidentiality. There are binding rules for inspecting and disclosing sensitive data, as well as written guidelines for the transfer and transmission of data. The processing of personal data takes place exclusively in accordance with the instructions of the client.
- Work devices are equipped with security software such as firewalls, antivirus software and malware detection. Written regulations exist for handling mobile devices and data carriers, for secure data deletion, for the destruction of data carriers, and for remote work (home office).
- Passwords require a defined minimum complexity and initial passwords must be changed after the first login.

Availability and Resilience

The measures for availability and resilience have the purpose of guaranteeing the services and internal operational processes, as well as their information security, even in the event of operational disruptions and unforeseen events.

- The data centers used – unless otherwise agreed or otherwise documented, are Microsoft Azure data centers – have extensive and modern fire alarm and extinguishing devices, climate and temperature controls, as well as measures for surge protection and uninterruptible power supply (UPS). For more information see the Azure Datacenter security overview which can be found at https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security.
- The provisioning of the production systems provided, their configuration and the application of changes are carried out traceably and transparently via an automated deployment infrastructure ("infrastructure-as-code principle").
- Production data is backed up regularly. All backups are kept redundant and in encrypted form (AES256) and distributed withing the same region as the main data center location resides in – unless otherwise agreed or otherwise documented within the data centers of Microsoft Azure. Technical access restrictions, automatic archiving and deletion policies, as well as strict organizational requirements for handling backups are implemented.
- Disaster recovery processes to restore data and processes for randomly checking the recoverability are defined.
- Capacity management measures to monitor the resource consumption of the systems as well as the planning of future resource requirements are implemented.
- Procedures for handling and reporting incidents (incident management) including the detection and reaction to possible security incidents are defined.

Controls and Validation

The measures for controls and validation serve to manage risks associated with changes as well as regularly checking and evaluating the effectiveness of all the technical and organizational measures described above.

Regular meetings between the responsible parties are held, to review the operating processes that affect the processing of personal data and the revision of the associated technical and organizational measures.

Security checks (e.g. penetration tests) by external parties are possible after consultation and are actively supported.