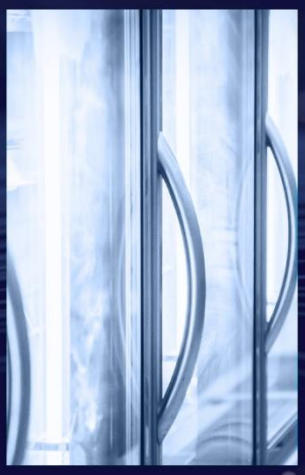
Sense Anywhere
SIMPLY SMARTER

Safe and secure data storage

Version 1.3


SenseAnywhere B.V.

Bergrand 218
4707 AT Roosendaal
The Netherlands

+31 165 796 210

info@senseanywhere.com

www.senseanywhere.com

Safe and secure data storage

Document Status

- Document title: Safe and secure data storage
- Authors: N. Segers
- Version: 1.3
- Date: March 2021

Revision History

Table 1 Revision History

Version	Date	By	Reason
1.0	20180920	N. Segers	Initial version.
1.1	20191014	N. Segers	Added 'Transparent Data Encryption' and 'Real-time geographic redundancy'.
1.2	20200722	N. Segers	'Premium SQL database' has been changed to the 'HyperScale database'.
1.3	20210319	N. Segers	Added ISO 27001 certification.

With SenseAnywhere your data is safely and securely stored in the Cloud

In order to provide the best possible service to our clients with the highest possible reliability and uptime SenseAnywhere makes use of the Microsoft Azure cloud platform. All SenseAnywhere data is stored in the Azure Cloud and all SenseAnywhere SAClient portal services run in Azure Cloud. Microsoft Azure is recognized as one of the best cloud infrastructure platforms nowadays, providing services to many customers worldwide. Azure leads the industry with the most comprehensive compliance coverage, enabling customers to meet a wide range of regulatory obligations.

Database

Sensor data is stored in a HyperScale Azure SQL database. This is a high end, highly scalable, data storage environment with real time triple-redundant hardware and data management software infrastructure. Azure SQL Database is a relational database-as-a-service (DBaaS) hosted in the Azure cloud that falls into the industry categories of Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS). Azure SQL Database is built on standardized hardware and software that is owned, hosted, and maintained by Microsoft. Your sensor data is stored in very reliable infrastructure which is highly protected against hardware and power failures. You will always be the owner of your data. SenseAnywhere stores your data in a reliable and secure way. Even if you terminate your subscription we keep the data stored for you. Depending on your subscription we keep data up to 15 years after we have collected it from your data loggers even if you terminate your subscription.

Transparent Data Encryption

Your sensor data is stored in very reliable infrastructure which is highly protected against hardware and power failures. We use Transparent Data Encryption (TDE) to prevent a malicious party from restoring/attach the database and browsing through the data. TDE performs real-time I/O encryption and decryption of the data, log files as well as the back-ups. TDE provides the ability to comply with many laws, regulations, and guidelines established in various industries.

Real-time geographic redundancy

The High Availability architecture in Azure guarantees that our database is up and running 99.99% of time, without worrying about the impact of maintenance operations and outages. The main database, primary copy and secondary copy are at different physical locations. This further enhances business continuity of our system and makes it resilient to a much larger set of unplanned events, including catastrophic datacenter outages.

Summarizing data storage

- SLA uptime 99,99% of the database (Microsoft SLA agreement)
- Highly scalable
- Triple redundant database infrastructure
- Backups made each 5 minutes and stored for 35 days
- Data centres located in Europe
- Data retention of at least 5 years and up to 15 years

Internationally recognized compliance standards

In order to run a trustworthy service, the Microsoft Azure cloud platform must meet the most stringent internationally recognized compliance standards, and their own internal safety and security standards. Microsoft leads the industry in establishing clear security and privacy requirements and then consistently meeting these requirements. A few examples of these broad set of international and industry-specific compliance standards with which Azure complies are ISO 9001, FDA CFR Title 21 Part 11 and Good Practice quality guidelines and regulations (GxP). Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. Microsoft Azure has a Service Trust Portal where ISO reports and certificates can be downloaded.

ISO 9001 (International Organization for Standardization)

Azure's achievement of ISO 9001:2015 certification demonstrates its commitment to Quality Management Systems. The standard is based on several quality management principles, including clear focus on meeting customer requirements, strong corporate governance and leadership commitment to quality objectives, process-driven approach to meeting objectives, and focus on continuous improvement. ISO 9001:2015 helps organizations improve customer satisfaction by focusing on the consistency and quality of products and services provided to customers.

ISO 27001

SenseAnywhere is ISO 27001 certified. ISO 27001 certification provides independent assurance that SenseAnywhere has a robust, systematic, and risk-based approach for Information Security, compliant to the requirements of this international standard.

FDA CFR Title 21 Part 11 (Food and Drug Administration)

FDA CFR Title 21 regulates food and drugs manufactured or consumed in the United States, under the jurisdiction of the Food and Drug Administration (FDA), the Drug Enforcement Administration, and the Office of National Drug Control Policy. The regulations outlined in CFR Title 21 Part 11 set the ground rules for the technology systems that manage information used by organizations subject to FDA oversight. Any technology system that governs such GxP processes as Good Laboratory Practices (GLP), Good Clinical Practices (GCP), and Good Manufacturing Practices (GMP) also requires validation of its adherence to GxP.

CFR Title 21 Part 11 sets requirements to ensure that electronic records and signatures are trustworthy, reliable, and generally equivalent substitutes for paper records and handwritten signatures. It also offers guidelines to improve the security of computer systems in FDA-regulated industries. Subject companies must prove that their processes and products work as they are designed to, and if these change they must revalidate that proof. SenseAnywhere has a separate document in FDA compliance of our software that can be made available upon request.

GxP (Good Practice quality guidelines and regulations)

GxP is a general abbreviation for "good practice" quality guidelines and regulations. Technology systems that use GxP processes such as Good Laboratory Practices (GLP), Good Clinical Practices (GCP), and Good Manufacturing Practices (GMP) require validation of adherence to GxP. Solutions are considered qualified when they can demonstrate the ability to fulfill GxP requirements. GxP regulations include pharmaceutical requirements, such as those outlined in the U.S. Food and Drug Administration CFR Title 21 Part 11, and EU GMP Annex 11.

GAMP5

SenseAnywhere follows the rules of GAMP5 for all new software developments; a set of guidelines for manufacturers and users of automated systems in the pharmaceutical industry. GAMP5 describes a set of principles and procedures that help ensure that pharmaceutical products have the required quality. One of the core principles of GAMP is that quality cannot be tested into a batch of product but must be built into each stage of the process.

Validation

SenseAnywhere is doing a lot of validation and unit testing. We have strict controls on the source code and revision control on all software we develop. All hardware, firmware and software in SenseAnywhere products has been developed in the Netherlands and is owned by SenseAnywhere.

Microsoft Responsibilities

Microsoft has the following responsibilities:

- Confidentiality - ensuring that information is secure and accessible only to those authorized to have access;
- Integrity - safeguarding the accuracy and completeness of information and processing methods;
- Availability - ensuring that authorized users have access to information and associated assets when required.

Service Level Agreements (SLA)

Audited controls implemented by Microsoft serve to ensure confidentiality, integrity and availability of data stored on the Azure platform and correspond to the applicable regulatory requirements defined in 21 CFR Part 11 that have been identified as the responsibility of Microsoft. Microsoft is responsible for ensuring that the Azure platform meets the terms defined within the governing Service Level Agreements (SLA). Microsoft provides Service Level Agreements (SLA) related Azure platform services, which may be downloaded from the Azure website: Service Level Agreements

Audited controls

The following points describe the audited controls implemented by Microsoft which serve to ensure confidentiality, integrity and availability of data stored on the Azure platform:

- Microsoft has implemented an Information Security Policy which addresses security, availability and confidentiality for Azure. Procedural controls are in place to support the policy.
- Proper controls are established to provide reasonable assurance that the Azure platform is monitored for known security vulnerabilities and potential unauthorized activity.
- The SOC 1 audit reported that Microsoft has implemented processes which manage the backup of critical Azure components and data. The Azure SQL database is constantly being backed-up automatically in the background and backups are stored for 35 days. When things go wrong we can restore any backup of the database with a 5-minutes interval within the last 35 days. Basically, at any point in time we have over 10.000 backups of your data with the latest backup no more than 5 minutes old.
- The 2011 ISO/IEC 27001:2005 audit reported that procedures and mechanisms are established for effective key management to support encryption of data in storage and in transmission for the key components of the Azure service.
- The 2013 ISO/IEC 27001:2005 audit reported that procedural documents covering change management are in place, in which the methodology for change and release management is defined. Changes are appropriately tested and approved.
- The 2013 ISO/IEC 27001:2005 audit reported that Microsoft effectively follows a documented risk management procedure dedicated to the Azure platform.
- The baseline configuration of Azure components is documented, managed, maintained and controlled for access via access control mechanisms.
- The 2013 ISO/IEC 27001:2005 audit reported that business continuity is documented, implemented, maintained, tested annually and any issues are tracked to closure.

For an overview of business continuity with Azure SQL Databases, please see: Overview of business continuity with Azure SQL Database.