Data privacy in System 3060

Information

11.07.2023

SimonsVoss technologies

Contents

1 IT basic protection

1.1 What protection requirements do the data processed in the system have?

In general, only non-critical data with so-called normal protection requirements are processed and stored in the software. This means data whose hypothetical loss neither damages the reputation of a person nor the image of a company. A high financial loss is also not to be expected.

1.2 What IT infrastructure requirements are recommended?

According to the German Federal Office for Information Security (BSI), basic IT security is therefore sufficient as a security concept for a SimonsVoss locking system and is regarded as a recommended minimum requirement for your IT infrastructure.

2 Encryption

2.1 Is the data in System 3060 encrypted?

Yes. Data packets are encrypted end-to-end within the system's own communication network. The latest versions of our products offer you a higher level of security since they are always state-of-the-art. Multi-level encryption methods are used (AES, 3DES).

2.2 What data is encrypted?

Within the system's own communication network, no personal data is processed. It pseudonymised instead using the identification numbers. They cannot be associated with a real person even without encryption.

2.3 Are the transmission paths via radio, for example, also encrypted?

No. Due to the end-to-end encryption type used, there is no need to also encrypt the transmission paths.

3 Working in compliance with data protection regulations (GDPR)

3.1 What personal data is stored in the software?

It is possible to store the following data of a person in the software:

- First name
- Last name*
- Title
- Address
- Phone
- E-Mail
- Personnel number*
- User name
- Department
- City/Building
- Set From/To
- Date of birth
- Cost center
- Photo

Only the last name and personnel number (*mandatory fields) are required when using the software. Special categories of personal data according to Art. 9 GDPR are not stored.

3.2 For what purpose is personal data stored in the software?

In order to be able to make full use of the functions of an electronic locking system, it is necessary to be able to assign the identification media used (e.g. transponder) to a specific user (e.g. employee).

3.3 How long is personal data stored in the software?

The data is stored within the locking system for at least the duration of the occupation of an identification medium (e.g. company affiliation).

The duration of data storage, e.g. in logs and access lists, can be changed at will by the locking system administrator.

3.4 Can the right to read access lists be additionally secured?

When using the optional ZK function in our locking components, access to the data collected with it can be equipped with increased user rights.

Example: A separate user is created for the works council. Only this user is given reading rights to the access lists in case of suspicion. In addition, this user can be protected with a shared password. Only one part of the password is known to two or more members of the works council.

3.5 Is personal data in the software protected against access by third parties?

In principle, the user (end customer) of the locking system and the software is responsible for managing and securing access rights.

In the locking system itself, all data is secured using a multi-level encryption process. Opening the graphical user interface to access the data is not possible without a password and appropriate user rights.

There shall be no automatic transmission to third parties, use or processing by SimonsVoss.

3.6 Can the stored data be made available as a copy?

All collected data on a data subject can be made available as a copy by means of an export function (Art. 15 GDPR).

3.7 Can personal data be deleted from the software?

Personal data can be validly deleted from the software (from version 3.4 SP1) and the associated database at the request of a data subject in accordance with Art. 17 GDPR.

4 Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

https://www.simons-voss.com/en/documents.html

Software and drivers

Software and drivers can be found on the website:

https://www.simons-voss.com/en/service/software-downloads.html

Declarations of conformity

You will find declarations of conformity and other certificates on the website:

https://www.simons-voss.com/en/certificates.html

Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

Email

You may prefer to send us an email.

support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

https://faq.simons-voss.com/otrs/public.pl

Address

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germany

SimonsVoss Technologies GmbH, Feringastr. 4, D-85774 Unterfoehring, Germany

This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION