



Information about the processing of personal data in HAN

- The document describes which personal data is processed in the HAN data processing procedure and with which mechanisms this data is protected. -

Contents

| | |
|---|---|
| Introduction..... | 1 |
| Data protection mechanisms..... | 2 |
| HAN role and user system..... | 2 |
| Anonymization/pseudonymization | 2 |
| Regular deletion | 2 |
| Password protection of database | 2 |
| Processed data | 2 |
| Active directory user data | 2 |
| Configuration of authentication services | 2 |
| E-mail data in case of error | 3 |
| HAN log data | 3 |
| Web server logs | 3 |
| Event Viewer..... | 3 |
| Summarized Log..... | 3 |
| Detailed Log..... | 3 |
| HAN Statistics | 3 |
| HAN protection against misuse (data transfer) | 4 |
| License Monitor | 4 |
| User Administration | 4 |
| E-script Properties | 4 |
| Release | 4 |

Introduction

HAN follows the principles of data avoidance and data minimization, meaning that it does not process personal information that is not required for internal HAN processes. The total amount of personal data processed in HAN is small. HAN supports both anonymization and pseudonymization mechanisms to remove the personal reference from data. Read in the following chapters which data HAN processes and how this data is protected.

Data protection mechanisms

The basis of all data security in HAN is that you secure your Windows system accordingly and define suitable access rights, as HAN integrates into this system. Define the circle of authorized users as narrowly as possible and assign strong passwords.

HAN role and user system

HAN has an integrated role concept that gives users a predefined HAN role. Certain rights are linked to the roles, so that members of a role receive exactly the rights in HAN that they need to perform the role. Only HAN administrators have access to HAN management programs.

Anonymization/pseudonymization

By default, log data is anonymized in HAN, that is, any personal reference is removed from the log data. The anonymization function can be configured via the HAN settings. Instead of anonymization, a pseudonymization can be applied to the log data, in which the personal reference of the log data is replaced by a pseudonym (irreversible). These settings are protected by the dual control principle.

Regular deletion

Log data that is not used for statistical evaluation is deleted at regular (user-defined) intervals.

Password protection of database

In addition to Windows authentication, the HAN database is password-protected by the HAN role system.

Note: The H+H installation team will discuss the data protection mechanisms with you before acceptance and activate the data protection according to your specifications.

Processed data

In the following, you will read which data HAN processes and which protection mechanism is used. The document describes all data. Personal data, or data about that a personal reference can be made, **are highlighted**.

Active directory user data

HAN accesses user data from Microsoft Active Directory Services. The following HAN programs and processes use this data:

- HAN Data Editor > Permissions > AD user
- HAN Data Editor > Data groups > User

Data: According to the configuration of the system administrator

Protection: Backup of the domain controller, HAN role and user system (access to administrative programs only with administrative HAN user account)

Configuration of authentication services

When configuring authentication services, information in third-party databases or directory services (including Microsoft ADS) is also accessed via interfaces. The data from the databases can then be used to log on to HAN. HAN queries the databases in real-time and only when needed from the respective database. The data is not stored in HAN. Only the access data for the respective database are stored in HAN:

- HAN Settings > Login > Authentication

Data: Access data to the respective database (*username* and password), *IP lists*

Protection: HAN role and user system

E-mail data in case of error

- HAN Settings > Global > System Monitoring

Data: *sender*, *recipient*, *username*, password, domain membership of an administrative account

Protection: HAN role and user system (access to administrative programs only with administrative HAN user account)

HAN log data

HAN generates various log data for error analysis and statistical evaluation. Data that allow inferences to a real person - username and station - are anonymized by default or alternatively can be pseudonymized. The following HAN programs and log files process log data:

Web server logs

Access log files of the HAN web server

Data: *User and station ID*

Protection: Are deleted after a defined interval (such as statistics).

Event Viewer

Logging events for error analysis

Data: *Computer name, username*

Protection: Automatically deleted on a regular basis.

Summarized Log

Logging of e-script usage

Data: *Username, computer name*, used e-script (protocol ID), timestamp, amount of bytes transferred, session ID

Protection: HAN role and user system, anonymization/pseudonymization

Detailed Log

Logging of e-script usage

Data: *Username, computer name*, used e-script (protocol ID), timestamp, amount of bytes transferred, session ID

Protection: HAN role and user system, anonymization/pseudonymization

HAN Statistics

Analysis of HAN usage

Data: *Username, computer name*, used e-script

Protection: HAN role and user system, anonymization/pseudonymization

HAN protection against misuse (data transfer)

Notification system against the misuse of HAN (only from HAN 5)

Data: *Usernames* from login, *e-mail address* of the administrator, administrative website that shows misuse log and allows unlocking of users (only for defined role)

Protection: Database logon, HAN role and user system, regular deletion of the log file according to user-defined interval

License Monitor

Monitoring of license usage with display of user name and IP address

Data: *username*, *IP address*, license used

Protection: HAN role and user system (only according to assigned role)

User Administration

Administration of HAN users and assignment of HAN roles

Data: *Usernames* (derived from Windows system or freely assigned)

Protection: HAN role and user system (access to administration programs with administrative HAN user account only), database login

E-Script Properties

Configuration of e-scripts

Data: Logging of last change: *username* and date

Protection: HAN role and user system

Release

The information has been compiled to the best of our knowledge and belief. We hope you will find them useful when preparing your data protection documentation.



Markus Libiseller
Product Manager Hidden Automatic Navigator