

DOCUMENTATION OF THE DATA PROTECTION AND SECURITY MEASURES OF THE HAUFE ZEUGNIS MANAGER PREMIUM

GENERAL DOCUMENT INFORMATION

Company			
Haufe-Service Center GmbH & Co. KG, Munzinger Str. 9, 79111 Freiburg, Germany			
Title of document			
Documentation of the data protection and security measures of the Haufe Zeugnis Manager Premium			
Person responsible for document	Pages	Version	Next check on up-to-date status
M. Kienzler	21	1.9	01.03.2026

Version history

Date / alteration	Version	Description	Altered by
2014-03-14	0.1	Initial version	A. Alsbih and Raik Mickler
2014-05-06	0.2	Notes from product designer incorporated	A. Alsbih and Raik Mickler
2014-05-07	0.3	Notes from service manager	A. Alsbih and Raik Mickler
2014-09-12	0.4	Recording of notes from head of IT Governance	A. Alsbih and Raik Mickler
2015-01-15	1.0	Finalisation / additions	A. Alsbih and Raik Mickler
2016-10-04	1.1	Update based on changes to product and IT environment	R. Mickler
2017-31-01	1.1	Check on up-to-date status; no changes necessary	R. Mickler
2018-06-30	1.2	Update based on changes due to GDPR	R. Mickler
2019-04-18	1.3	Update based on changes to product and IT environment	R. Mickler und M. Baur
2019-11-18	1.4	Update	M. Kienzler
2021-02-22	1.5	Update based on changes to product and IT environment	M. Kienzler
2023-01-10	1.6	Update	M. Kienzler
2023-03-01	1.7	Update	M. Kienzler
2024-04-24	1.8	Update	M. Kienzler
2025-01-15	1.9	Update based on changes to product and IT environment	M. Kienzler

TABLE OF CONTENTS

General document information	1
General information	4
1.1 Application description	4
1.2 system locations	4
1.3 Architecture / data flowchart for Haufe Zeugnis Manager Premium	5
1.4 More details on data protection and data security organisation	5
1.5 Overview of roles (professional use of Haufe Zeugnis Manager Premium)	7
1.6 Operating the application	12
1.7 Operation of the authentication and authorisation system	12
1.8 Special security measures	12
Technical and organisational measures	13

GENERAL INFORMATION

This document has been compiled by the authors to the best of their knowledge in line with the interviews carried out, on the basis of information submitted by Amazon Webservices, noris network AG and Haufe Group employees from the IT and Development departments.

1.1 APPLICATION DESCRIPTION

Haufe Zeugnis Manager Premium makes it easy to create legally compliant references. An integrated line manager workflow optimises interaction between HR and managers and supports each stage of reference creation, from constructing and evaluating a reference right up to the final reference text. The line manager workflow enables HR employees to directly incorporate line managers into the evaluation process using an access link. With this, the line managers can submit their input directly into the online solution in just a few clicks. The integrated memory function ensures that references can be drawn up promptly.

An overview of the key functions:

- Integrated workflow for incorporating line managers and employees
- Clear homepage for all references (open, archived, all, workflow status and reference type)
- Multiple company profiles can be set up
- Automatic conversion from interim to final references and from references for female employees to references for male employees and vice versa
- Template manager: quickly and easily edit building blocks directly in the reference text and save as your own variants
- Quick evaluation – full reference in one click
- Memory function and reminder for HR, line managers and employees
- Finished formatted reference directly in the tool

Four different versions of Haufe Zeugnis Manager are available: Haufe Zeugnisgenerator, Haufe Zeugnis Manager Basic, Haufe Zeugnis Manager Professional and Haufe Zeugnis Manager Premium. Haufe Zeugnisgenerator is a variant with a small range of functions and contained only in Haufe Office Line products. The Basic version is directed at companies needing few references, while the Professional version is aimed at businesses needing a moderate number of references. The Premium version documented here – the most extensive solution – offers a significantly expanded scope of services and is directed at large companies needing a lot of references.

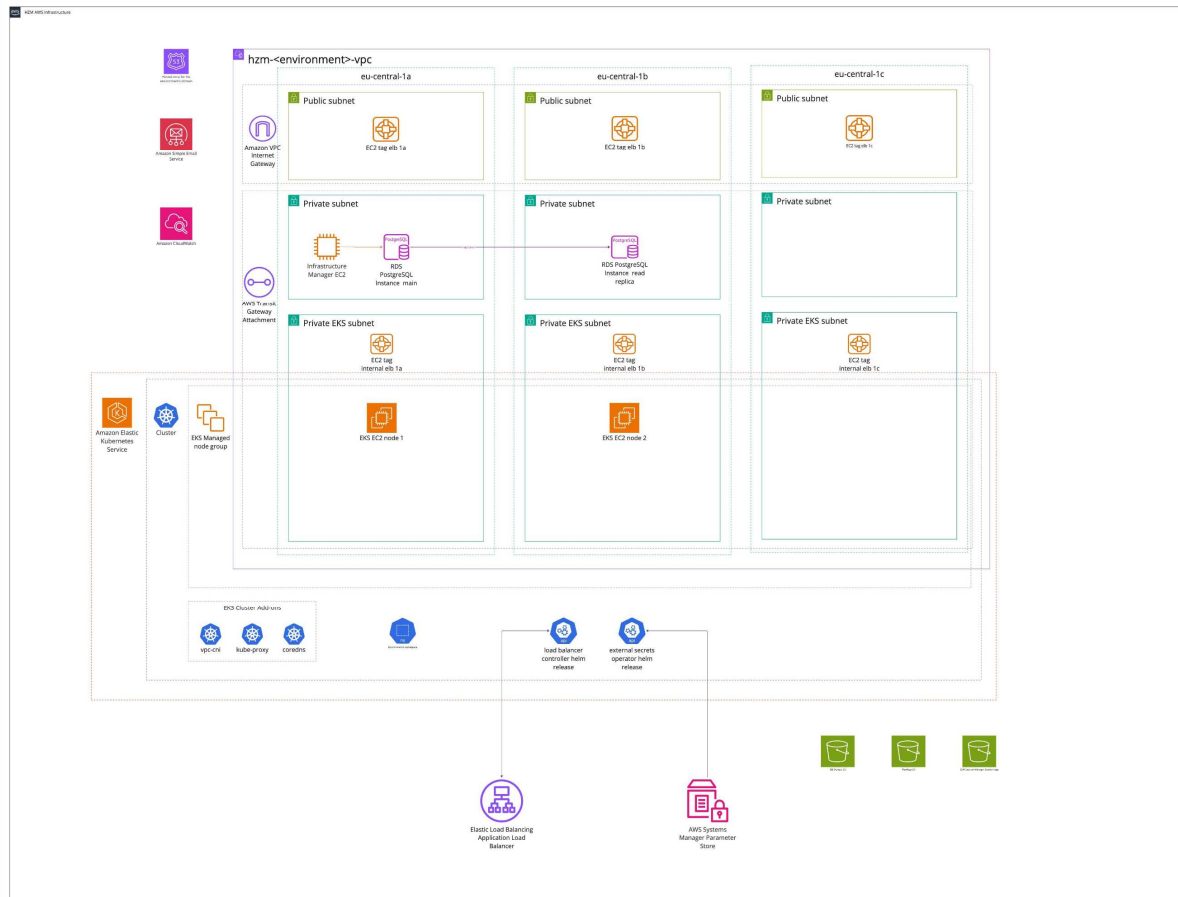
1.2 SYSTEM LOCATIONS

All customer data are saved exclusively on systems in Germany. Data are saved and processed as follows:

- The application is operated by Amazon Webservices in Frankfurt (EU-central-1).

- The authentication and authorisation system of the application (central authorisation system of the Haufe Group) is run by noris network AG, Thomas-Mann-Strasse 16–20, 90471 Nuremberg.

1.3 ARCHITECTURE / DATA FLOWCHART FOR HAUFE ZEUGNIS MANAGER PREMIUM



1.4 MORE DETAILS ON DATA PROTECTION AND DATA SECURITY ORGANISATION

Within the Haufe Group, there are various guidelines and specifications regarding information security and the protection goals of availability, integrity and confidentiality. Our internal guidelines include:

- Confidentiality agreements: within the Haufe Group, there are various templates for unilateral and bilateral confidentiality agreements. Corresponding agreements also form part of the contracts that are created and overseen by the Legal department.
- Data protection policy of the Haufe Group: the objective is to outline the foundations for implementing the data protection requirements of the General Data Protection Regulation (GDPR) and the the BDSG [German Federal Data Protection Act]. Basic principles of data processing, establishment of a data protection organisation, allocation of roles to bodies within the data protection organisation, basics of data protection management, data transmission to third parties, what to do in the event of data protection incidents and sanctions for infringements are determined.

- Guidelines on data protection incidents in the Haufe Group: the handling of data protection incidents or data emergencies, reasonable reactions in accordance with the law in the event of data protection incidents and legal reporting requirements are regulated.
- In addition, the Haufe Group has guidelines regarding data security that contain instructions about secure development, authentication and dealing with passwords.

For Haufe-Lexware GmbH&Co. KG, Haufe-Lexware Services GmbH & Co. KG and Haufe Service Center GmbH:

Mr Raik Mickler, e-mail: dsb@haufe-lexware.com

is appointed as data protection officer.

All employees are obliged in writing to maintain confidentiality. The obligation is documented by the HR department of Haufe-Lexware Services GmbH & Co. KG. There will continue to be annual data protection training on data protection requirements in the form of face-to-face or web-based training.

Haufe Service Center GmbH & Co. KG processes data only in connection with fulfilling the contractual/order obligations of its customers. For corporate clients, contracts are concluded in accordance with Article 28 of the GDPR regarding contract data processing.

1.5 OVERVIEW OF ROLES (PROFESSIONAL USE OF HAUFE ZEUGNIS MANAGER PREMIUM)

Professional roles for using Haufe Zeugnis Manager Premium	HR admin	HR standard	HR official	Line manager	Employee
General					
Calling up support (e-mail / hotline)	•	•	•	•	•
Calling up HZM portal	•	•	•		
Viewing product video	•	•	•	•	
Homepage					
Can see all references of his organization	•	•	•		
Using filters	•	•	•		
Reference requests filter	•	•	•		
'Open references' filter	•	•	•		
'Archived references' filter	•	•	•		
'With HR' filter	•	•	•		
'With line manager' filter	•	•	•		
'Reference type' filter	•	•	•		
Creating a reference	•	•	•		
Creating a reference from master data (if active)	•	•	•		
Search function	•	•	•		
Sorting	•	•	•		
Opening up open references	•	•	•		
Opening up archived references	•	•	•		
Deleting archived references	•	•			
Deleting sample references	•	•			
Converting from archive	•	•	•		
Using reference as template	•	•	•		
Editing archived reference	•	•	•		
Exporting to Word	•	•	•		
Creating interim reference from final reference	•	•	•		
Viewing quickinfo	•	•	•		
Administrator settings					
Editing administrator options	•				

Professional roles for using Haufe Zeugnis Manager Premium	HR admin	HR standard	HR official	Line manager	Employee
Viewing administrator options	•				
Dataprotection settings					
Edit data protection options	•				
View data protection options	•				
General settings					
Editing general options	•	•			
Viewing general options	•	•			
Text element manager					
Calling up text element manager	•	•			
Company profile					
Creating new profile	•	•			
Editing profile	•	•			
Copying profile	•	•			
Deleting profile	•	•			
Using profile	•	•	•	•	
Creating references					
Setting up a reference	•	•	•		
Selecting a professional group	•	•	•		
Selecting reference type	•	•	•		
Selecting occasion for reference	•	•	•		
Selecting language	•	•	•		
Saving job description in combo box	•	•			
Saving department in combo box	•	•			
Amending by first signatory	•	•	•	•	
Amending by second signatory	•	•	•	•	
Entering job description	•	•	•	•	•
Setting up job as a template	•	•			
Evaluating employees	•	•	•	•	
Edit special skills/competencies/career accomplishments	•	•	•	•	
Saving special skills/competencies/career accomplishments as a template	•	•			

Professional roles for using Haufe Zeugnis Manager Premium	HR admin	HR standard	HR official	Line manager	Employee
Line manager workflow					
Sending to line manager	•	•	•		
Editing e-mail to line manager	•	•	•		
Blocking access for line manager	•	•	•		
Employee workflow for job description					
Inviting employees				•	
Withdrawing employee access	•	•	•	•	
Entering job description	•	•	•	•	•
Approval workflow					
Sending to line manager for approval	•	•	•		
Blocking access for line manager	•	•	•		
Leaving comments	•	•	•	•	
Workflow User					
Deleting Workflow User	•				
View number of active workflows per workflow user	•				
Completing a reference					
Selecting variants	•	•	•		
Displaying all templates	•	•	•		
Saving changes to reference as a template	•	•			
Editing references	•	•	•		
Adjusting margins in reference view	•	•	•		
Formatting text in reference view	•	•	•		
Archiving	•	•	•		
Printing	•	•	•		
Exporting	•	•	•		
Change status manually (Reference printed, For signature, reference submitted, Archived)	•	•	•		
Converting references					
Creating final reference from interim reference	•	•	•		
Creating English reference from German reference	•	•	•		
Using reference as template	•	•	•		

Professional roles for using Haufe Zeugnis Manager Premium	HR admin	HR standard	HR official	Line manager	Employee
My account / managing users					
Setting up users (including rights, organisations, roles)	•				
Deleting users	•				
Resetting user data (e.g. password)	•				
Assigning users to organisations / sub-organisations	•				
Reference requests					
Configuring / activating reference requests	•				
Deactivating reference request link	•				
Accepting or rejecting reference requests	•	•	•		
Making reference requests	•	•	•	•	•
Changing to English GUI					
Activating English GUI	•				
Switching over to English GUI	•	•	•	•	•
View					
Can see their open references in the organisations to which they are granted access	•	•	•		
Can see all open references in the organisations to which they are granted access	•	•	•		
Can see their archived references in the organisations to which they are granted access	•	•	•		
Can see all archived references in the organisations to which they are granted access	•	•	•		
Report, how many references are in which status and how many references in total have been created per company profile	•				
Konfiguration					
Line manager may edit master data; default: yes	•	•			
Line manager may edit special skills/competencies/work accomplishments; default: yes.	•	•			
Delete comments and reference documentation when archiving; default: no	•	•			
Mark workflow emails as private; default: no	•				

Professional roles for using Haufe Zeugnis Manager Premium	HR admin	HR standard	HR official	Line manager	Employee
Deadline for automatic blocking of the access link for the line manager; default: 2 weeks.	•				
Restrict e-mail domains for the workflow; default: no	•				
Send references as e-mail attachment (PDF/RTF) directly from Haufe Zeugnis Manager; default: no	•				
Deadline for deletion of archived final, interim and simple references; default: no deletion	•				
HR is allowed to change general settings and use the text module manager; default: Yes	•				
Line manager can also select the text module when evaluating an employee; default: no	•				
Line manager may involve employees in the preparation of references; default: Yes	•				
Which templates can line managers and employees select when editing the job description; default: all	•				
Define own fields for master data creation	•				

1.6 OPERATING THE APPLICATION

The Haufe Zeugnis Manager application is hosted in the Amazon Webservices data centre in Frankfurt (EU-central-1). A contract exists with this service provider in accordance with Article 28 of the GDPR regarding contract data processing.

This company has the following certifications:

- ISO 27001: Information security in general
- ISO 27017: Information security for cloud computing
- ISO 27018: Data protection standard for cloud services
- ISO 27701: Extension of ISO 27001 with regard to data protection
- ISO 22301: Standard for business continuity management
- BSI C5: Cloud Computing Compliance Criteria Catalogue of the BSI

1.7 OPERATION OF THE AUTHENTICATION AND AUTHORISATION SYSTEM

The authentication and authorization system is operated in an ISO 27001 certified data center of noris network AG, Thomas-Mann-Straße 16 – 20, 90471 Nuremberg. There is a contract with this service provider in accordance with Art. 28 DSGVO on commissioned processing.

This company has the following certifications:

- ISO 27001: Information security in general
- BSI C5: Cloud Computing Compliance Criteria Catalogue of the BSI

1.8 SPECIAL SECURITY MEASURES

Due to the need to protect data:

- Server systems in the commercial vulnerability management system of the Haufe Group are included. This system carries out authenticated scans of the server systems at regular intervals and checks them for missing security updates.
- External penetration testing of the application by third parties is regularly carried out (generally annually).
- Use of 256-bit AES encryption for the following data:
 - Reference document (PDF)
 - Evaluations and reference scores
 - Reference content (text, including job description)
 - Career content (text)
 - comments (text)

TECHNICAL AND ORGANISATIONAL MEASURES

1. General

1.1 Are independent security reviews carried out (regularly) by external entities?

The HZM solution is operated in Amazon Webservices' data centre in Frankfurt (EU-central-1). Surveillance audits are carried out annually and recertification audits every three years.

Moreover, penetration tests are carried out at regular intervals at web application level (generally annually). These are commissioned by our Information Security department and carried out by external companies.

In addition, the basic systems of the Haufe Group are scanned periodically by vulnerability management.

1.2 Do formal, written, documented guidelines exist regarding information security?

There are various guidelines and specifications regarding information security and the protection goals of availability, integrity and trust, such as:

- Confidentiality agreements
- Data protection policy
- Guidelines on data protection incidents

1.3 Has a data protection officer been appointed? Please provide name and contact details and a scanned copy of the certificate of appointment.

Mr Raik Mickler
E-mail: dsb@haufe-lexware.com

1.4 Has an IT security officer / Chief Information Security Officer been employed? Please provide name and contact details.

Jochen Vogel is the CISO of the Haufe Group.
E-mail: security@haufe-lexware.com

1.5 Are employees obliged to maintain confidentiality? How are these obligations documented?

All employees who work with personal data are obliged to maintain confidentiality. The documentation comes from the HR department.

1.6 Can it be demonstrated that employees have been trained regarding data protection regulations?

Yes, regular training takes place to raise awareness.

1.7 Is there a record of processing activities in line with Article 30 of the GDPR?

yes

1.8 Who will be informed immediately if security incidents are discovered?

The CISO of the Haufe Group. In case of potential personal data protection violations, the data protection officer of the Haufe Group.

1.9 Can the results of penetration tests be viewed?

Viewing the results is possible to an extent, depending on coordination/request. Details of potential vulnerabilities or personal information cannot be viewed for reasons of data protection and security.

1. General

1.10 How is the system protected against external attacks?

- In line with best practices
- Secure Development Lifecycle
- Secure operations
- Independent review

1.11 Is there a password policy?

Any specifications for a password policy for the use of Haufe Zeugnis Manager Premium are possible within the Haufe Suite authentication system in terms of the password's period of validity, length, special characters, password history etc.

In the default configuration of Haufe Zeugnis Manager Premium within the Haufe Suite authentication system

- users are allowed to change their passwords themselves.
- users must change their passwords after logging in for the first time.
- a password may be reset only once a day at the most.
- each password must be at least eight characters long, contain upper-case and lower-case letters and include at least one number or special character. No successive character strings, such as 'aaa', '111' etc., may be used. A password must not begin or end with spaces.
- You can also set stronger password specifications – contact support.

1.12 Is there an internal audit function for the application?

Haufe Zeugnis Manager Premium offers a means of displaying the reference documentation. In addition, an overarching audit log is generated, which logs all actions with user ID and organisation ID.

1.13 Can it be ensured that data do not migrate outside a geographically defined region?

Yes. All personal data remain in Germany.

1.14 Can administrators or support workers view personal data?

Authorized employees of the Haufe Group from the Support department have access to data that a user of Haufe Zeugnis Manager requires for registration. These are name, first name, e-mail address and password. The password can only be changed by the support and cannot be read out.

Access to additional data of the Haufe Zeugnis Manager may be necessary in case of support. During project acceptance, the person responsible defines in the acceptance protocol how Haufe Support should have access in the event of support. There are 3 options to choose from:

- Haufe Support can have access for support purposes without a separate release.
- Access only after explicit individual release for a support case, temporarily limited to 4 hours or

1. General

	<ul style="list-style-type: none"> any access for Haufe Support is not allowed. (Attention! Support support is not possible or only possible to a limited extent. Obligation of the licensor for support support is void thereby). <p>No real data is used on test systems.</p> <p>The program includes a function for customer support. This allows employees to ask questions about the product. The corresponding employee can enter his phone number here.</p> <p>The e-mail to our support is enriched with the following data (name; e-mail address; Haufe Zeugnis Manager program version; browser version and operating system used by the user).</p>
1.15 When are the reference data deleted?	<p>You can delete the references produced in the software itself at any time.</p> <p>You can choose for archived references to be automatically deleted after a certain length of time.</p> <p>If your Haufe Zeugnis Manager licence is cancelled, we will continue to keep the reference data saved for you for 30 days. After that, all reference data will be irretrievably deleted. These include, in addition to the references that have been produced, text elements that you have created yourself and any master data and company profiles that have been added.</p>
1.16 How are the references saved?	<ul style="list-style-type: none"> Data are stored in a shared database. Automated processes (interceptors) ensure that only the specific data needed can be downloaded. Each client has a dedicated key with which the reference data (evaluations, reference text, job description, career details and reference document – PDF) are saved in encrypted form. Information from personnel master data (including name, department, personnel number, job description) is not saved in encrypted form, as you can search for these data in Haufe Zeugnis Manager. If we were to encrypt this information, key functionalities could no longer be used (especially on the homepage) and Haufe Zeugnis Manager Premium would be significantly less easy to use.
1.17 What security and data protection guidelines do you have (e.g. basic requirements regarding IT security, password policy, guidelines for mobile IT etc.)?	<p>Within the Haufe Group, there are: data protection policy, guidelines on handling data protection incidents, guideline for basic requirements regarding IT security, password policy, guidelines for mobile IT, secure coding guidelines, user policy.</p>
1.18 Is there an emergency strategy / manual?	Yes.
1.19 Has the company been reviewed for a specific reason by the data protection line managery authorities responsible?	No.

1. General

1.20 Is the contract fulfilled only in properties and systems located within the EU? The sub-service providers used that have access to personal data as part of order fulfilment are relevant here.

Yes.

1.21 Are there documented and regularly reviewed processes and practices for avoiding and rectifying gaps in security in the services provided?

The server systems are integrated into the Vulnerability Management System of the Haufe Group. These check the status of security updates by means of authenticated scans. Furthermore, static code analyses are carried out as part of software development. This starts in the development process and serves to identify and thus avoid technical implementation errors during the development process.

1.22 What types of authentication based on the authentication system of the customer are offered (e.g. federation based on LDAP)?

A connection via the customer's SSO service via SAML2 is possible via the authentication and authorization systems operated at Noris Network AG in Nuremberg (Haufe Suite).

1.23 Is the customer informed in the event of security and data protection incidents that could affect the data of the client?

There is a process for providing information to the customer in the event of security incidents involving data theft.

1.24 Is there a data protection strategy or security strategy for the application?

This documentation on the technical and organizational measures includes the explanations regarding data protection and data security.

CONFIDENTIALITY (Article 32 para. 1 [b] GDPR)

2. Physical access control

Definition: measures to deny unauthorised parties access to data processing systems with which personal data are processed and used.

2.1 Is there an access permission system documented in writing for employees of the company or persons without access rights (e.g. business customers / visitors, cleaning companies, maintenance companies etc.)?

Only authorised AWS personnel are granted access to the physical data centres. All employees requiring access to a data centre must first submit a request for access and provide a valid business justification. This request is granted based on the principle of least privilege, i.e. employees must specify in the request to which level of the data centre and for how long they require access. The request is checked and approved by authorised personnel. Access is withdrawn at the end of the requested period. Employees with access to a data centre are restricted to certain areas by their authorisations. Third party access must be requested by authorised AWS employees who must also provide a valid business justification for this access. This request is granted based on the principle of least privilege, i.e. employees must specify in the request to which level of the data centre and for how long they require access. These requests are approved by authorised personnel. Access is withdrawn at the end of the requested period. Employees with access to a data centre are restricted to certain areas by their authorisations. Persons with a visitor badge must present it on arrival at the site and are registered and accompanied by authorised personnel.

CONFIDENTIALITY (Article 32 para. 1 [b] GDPR)

2. Physical access control

Definition: measures to deny unauthorised parties access to data processing systems with which personal data are processed and used.

2.2 Is there a security service? What areas of responsibility / tasks does it undertake?	Physical access is controlled by professional security personnel at the building entrances. Surveillance, alarm systems and other electronic devices are used. Authorised personnel gain access to the data centres via multi-factor authentication mechanisms. The entrances to the server rooms are secured with devices that trigger an alarm if the door is broken or held open.
2.3 Does video surveillance take place? How long are the videos stored?	Physical access points to server rooms are monitored by CCTV cameras with recording function. The recordings are stored in accordance with regulatory and compliance requirements.
2.4 Is there an alarm system? Who receives the alerts that it sends?	Electronic intrusion detection systems are installed on the data level, which recognise security-relevant events and automatically alert the responsible employees. The entrances and exits to the server rooms are secured with devices that require multi-factor authentication from each person before they are granted access and a badge before they leave the room. These devices trigger an alarm if the door is forced open without authentication, held open or opened to leave during an emergency. Door alarms are also configured to recognise situations where a person enters a data level without multi-factor authentication or leaves without proper badging. In this case, an alarm is immediately triggered and sent to the AWS Security Operations Centre for logging, analysis and response.

3. System access control

Definition: measures to prevent data processing systems from being used by unauthorised parties.

3.1 Are there regulations regarding the issue, revocation and regular review (of the necessity) of system access permissions?	This is implemented via the starter-changer-leaver process. Furthermore, cyclical reviews of the necessity of the authorizations take place. These take place at least once a year.
3.2 Are all authorisations given only on the basis of minimum rights (need-to-know)?	Different teams are deployed for the individual levels, which only have access to the components for which these employees are responsible.
3.3 Are there measures for protecting password files and passwords at application level?	The passwords are stored in line with PBKDF2WithHmacSHA256 procedures on a central authentication system at noris Network AG.
3.4 Is there a limit to the number of registration attempts in the event of repeated failed attempts (number / configurability)?	After three failed attempts at signing in, system accounts (operating system etc.) are locked. They can be reset only after the employee has been clearly identified. On the part of the central authentication and authorisation system of the application, brute-force protection can be implemented. This allows an

3. System access control

Definition: measures to prevent data processing systems from being used by unauthorised parties.

	account to be locked after a configurable number of failed attempts in combination with automatic unblocking after a certain time period or only after manual unlocking.
3.5 How does access work within the framework of teleworking / working at home or mobile computing, for instance? What specifications are there?	Teleworking is possible only with the use of a VPN with two-factor authentication (certification in combination with a username and password). The file systems of laptops are encrypted.
3.6 Are there regulations for leaving the workplace (e.g. locking the computer)?	The computers are locked automatically after 15 minutes of inactivity.
3.7 Are intrusion detection/prevention systems used?	No.
3.8 Is a virus scanner used on all server systems? If so, at what intervals are signatures updated?	ClamAV is used for data within the application. This is provided with the latest anti-virus signatures once a day.
3.9 Are there regulations for the use of local administration rights?	No local admin rights are assigned.

4. Data access control

Definition: appropriate measures meaning that those authorised to use a data processing system can access only the data available to them based on their access rights, and that personal data cannot be read, copied, changed or deleted without authorisation during processing, during use or after storage.

4.1 Is there an authorisation strategy for the application for the needs-based configuration of access rights (differentiated authorisations for profiles, roles, transactions and objects)?	There is a role and authorization concept that restricts access, see page 7.
4.2 Is encryption technology used on laptops?	Hard drive encryption is used. Various solutions such as TrueCrypt, BitLocker or hard drive encryption from Apple are used for this.

5. Separation control

Definition: appropriate measures meaning that data collected for different purposes can be processed separately.

5.1 How and where are data separated from the data of other customers / clients (e.g. physically separate server systems for each customer)?	<ul style="list-style-type: none"> The data of different customers are in a central database; separated by the client number. There is not a separate database server or database schema for each client. Each client has its own key for data encryption. All keys are stored in a separate database schema.
5.2 Is there a logical and physical separation of the production, integration and development systems from each other?	In addition to the productive environment, there is a staging environment for tests as well as development environments.
5.3 Are productive data from the client stored on systems other than the productive system (e.g. use of real data on test systems for test purposes)?	Only anonymized data is used on the test systems (staging), where all personal data worthy of protection is anonymized.

6. Pseudonymisation (Article 32 para. 1 [a] GDPR; Article 25 para. 1 GDPR)

Definition: the processing of personal data in such a way that data can no longer be attributed to a specific data subject without the provision of additional information. This is provided that this additional information is kept separate and subject to corresponding technical and organisational measures.

6.1 How are sensitive personal data pseudonymised in Haufe Zeugnis Manager?

Haufe Zeugnis Manager Premium pseudonymizes the data by encrypting the data:

- both during transmission (https)
- as well as during the storage of sensitive personal reference data on database level (256 Bit AES).

6.2 Use of encryption technology in databases?

256 bit AES encryption is used for the following reference data:

- Evaluation or reference grades
- Reference text incl. job description
- Career text
- Reference document (PDF)
- Comments (text)

The key is generated individually for the licensee and stored separately from other personal data.

INTEGRITY (Article 32 para. 1 [b] GDPR)

7. Transfer control

Definition: appropriate measures meaning that personal data cannot be read, copied, changed or deleted without authorisation in electronic transmission or during transport or storage on data storage media, and that it is possible to check and determine the places in which the transfer of personal data using data transmission equipment is intended.

7.1 Are personal data transmitted to other applications / systems (e.g. through interfaces / web services)? Can you name the corresponding interfaces, including the transmitted data categories? How are corresponding transmissions logged?

There is no transmission of personal data from the HZM application to other systems. Only authentication and authorisation are conducted using a central authentication and authorisation system, operated by noris Network AG in Nuremberg. An interface can optionally be configured for importing employee master data. However, this can happen only if desired by the customer and is not enabled by default.

7.2 Is access to the application possible only if encrypted? Identify the procedure (e.g. TLS), including the algorithms used (e.g. RSA 2048 in combination with AES 256).

Yes, we support TLS 1.2 and TLS 1.3 using RSA 4096 bits.

7.3 Are data storage media (e.g. backups) transported to an additional location (e.g. catastrophe archive, TRESOR, safe deposit box)?

No, there is no backup outside the AWS data centres (EU-central-1).

8. Input control

Definition: appropriate measures for allowing subsequent review and determination of whether and by whom personal data has been entered into, changed in or removed from data processing systems.

8.1 What is logged in the application (e.g. input, alteration, deletion etc. of data, authorisations etc.)?

In the application itself, the data are logged in the process of reference creation for handover from HR to a line manager and from the line manager to HR.

8. Input control

Definition: appropriate measures for allowing subsequent review and determination of whether and by whom personal data has been entered into, changed in or removed from data processing systems.

The following data are cached here:

- Job description
- Skills
- Special career accomplishments
- Grading for criteria
- Text element recommended by the line manager
- Comments on the evaluations
- Date and time of handover to the next instance in the process

The administrator of the application can configure the settings such that this documentation is deleted automatically when the reference is archived.

An overarching audit log is generated. Here, all actions (no reference data) are logged with user ID and organisation ID. This logging is for the purposes of security and records:

- Calling up Zeugnis Manager
- Transactions (downloading references, editing references, forwarding references to line managers, archiving references, deleting references, editing references from the archive, converting references)

Log data are kept for up to 90 days:

8.2 What is logged at database level (transaction log / database audit log)? Please state corresponding log categories and log content according to category. How long are these log data kept?

Transaction logs are created and used on an hourly basis as backup. Using these, changes to content can be reconstructed accordingly. These data are stored for 30 days.

8.3 How is it ensured that the log data cannot be altered?

Through the transmission of log data to a central Syslog server.

AVAILABILITY AND RESILIENCE (Article 32 para. 1 [b] GDPR)

9. Availability control

Definition: appropriate measures meaning that personal data are protected against accidental deletion or loss.

9.1 Is there a emergency and restart procedure with regular testing (emergency plan)?

Yes, according to ISO 22301.

9.2 Are two independent computer centres used with sufficient geo-redundancy (two different risk environments)?

The infrastructure is distributed redundantly across data centers, so the service is still available even if one data center fails completely

9.3 Are there tests and approval procedures (e.g. after patches, new releases etc.)? If so, what are they?

The processes are based on the Information Technology Infrastructure Library (ITIL) in this regard.

Fast recoverability (Article 32 para. 1 [c] GDPR)

PROCEDURES FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION (Article 32 para. 1 [d] GDPR; Article 25 para. 1 GDPR)

10. Order control

Definition: appropriate measures meaning that personal data that are processed by contract can be processed only according to the instructions of the Customer.

10.1 Which sub-contractors / service providers have access to data belonging to the Customer?	Only selected employees at Haufe have access to the certificate data. AWS has no access.. Access to authentication data: noris Network AG in Nuremberg, which operates the authentication and authorisation system and the underlying infrastructure.
10.2 Which sub-contractors outside the EU have access to the personal data of the Customer?	None.
10.3 Are there written contracts regarding the processing of order data in line with Article 28 of the GDPR, NDAs or obligations to maintain confidentiality in place with sub-contractors?	There is a contract in line with Article 28 of the GDPR in place with the service providers named above. The employees who have access to data belonging to the Customer are obliged to maintain data confidentiality.
10.4 Is it possible to review technical and organisational measures if notified in advance and agree a date for an on-site audit with the sub-contractor?	No.
10.5 How often is an audit of technical and organisational measures carried out with the sub-contractor?	Audits are carried out by the data protection officer with the service providers named above. The review cycle is based on the protection needs of the data.
10.6 Is the Customer immediately informed about errors regarding data processing or violations of data protection, as well as IT security incidents? Who receives this information?	Yes, the information is provided to the entity designated in the contract with the client.