

HAUFE



Dokumentation der Datenschutz und Informationssicherheit

Des Haufe Zeugnis Managers Premium

Allgemeine Dokumenten- informationen

Unternehmen

Haufe-Service Center GmbH & Co. KG,
Munzinger Str. 9, D-79111 Freiburg

Dokumenten Titel

Dokumentation der Datenschutz- und
Sicherheitsmaßnahmen des Haufe
Zeugnis Managers Premium

Dokumentenverantwortliche

M. Kienzler

Seiten

22

Version

1.9

Nächste Aktualitätsprüfung

01.03.2026



Versionsverlauf

Datum/Veränderung	Version	Beschreibung	verändert durch
2014-03-14	0.1	Initiale Version	A. Alsbih und Raik Mickler
2014-05-06	0.2	Anmerkungen von Product Designer übernommen	A. Alsbih und Raik Mickler
2014-05-07	0.3	Anmerkungen vom Service Manager	A. Alsbih und Raik Mickler
2014-09-12	0.4	Aufnahme der Anmerkungen des Bereichsleiters IT-Governance	A. Alsbih und Raik Mickler
2015-01-15	1.0	Finalisierung/Ergänzungen	A. Alsbih und Raik Mickler
2016-10-04	1.1	Aktualisierung aufgrund von Änderungen am Produkt und der IT-Umgebung	R. Mickler
2017-31-01	1.1	Aktualitätsprüfung, keine Änderung erforderlich	R. Mickler
2018-06-30	1.2	Aktualisierung aufgrund von Änderungen durch DSGVO	R. Mickler
2019-04-18	1.3	Aktualisierung und Erweiterungen	R. Mickler und M. Baur
2019-11-18	1.4	Aktualisierung	M. Kienzler
2021-02-22	1.5	Aktualisierung aufgrund von IT-Änderungen	M. Kienzler
2023-01-10	1.6	Aktualisierung	M. Kienzler
2023-03-01	1.7	Aktualisierung	M. Kienzler
2024-04-24	1.8	Aktualisierung	M. Kienzler
2025-01-15	1.9	Aktualisierung aufgrund von Änderungen am Produkt und der IT-Umgebung	M. Kienzler

Inhaltsverzeichnis

Allgemeine Informationen	5
Applikationsbeschreibung	6
System-Standorte	7
Architektur/Datenflussdiagramm Haufe Zeugnis Manager Premium	7
Weitere Angaben zur Organisation des Datenschutzes und der Datensicherheit	8
Rollenübersicht	9
Betrieb der Applikation	16
Betrieb des Authentifizierungs- und Autorisierungssystems	16
Spezielle Sicherheitsmaßnahmen	17
Technische und organisatorische Maßnahmen	18
Allgemeines	23
Zutrittskontrolle	24
Zugangskontrolle	24
Zugriffskontrolle	26
Trennungskontrolle	26
Pseudonymisierung	27
Weitergabekontrolle	28
Eingabekontrolle	29
Verfügbarkeitskontrolle	30
Auftragskontrolle	31

Allgemeine Informationen

Dieses Dokument wurde auf Basis von vorgelegten Informationen von Amazon Webservices und Mitarbeitern der IT und Entwicklungsabteilungen der Haufe Group nach Durchführung von Interviews durch die Autoren nach bestem Wissen erarbeitet.



Applikationsbeschreibung

Mit dem Haufe Zeugnis Manager Premium können Arbeitszeugnisse einfach und rechtssicher erstellt werden. Ein integrierter Vorgesetzten-Workflow optimiert das Zusammenspiel zwischen HR und Führungskräften und unterstützt in jedem Schritt der Zeugniserstellung – von der Anlage eines Arbeitszeugnisses über die Bewertung bis zum finalen Zeugnistext. Der Vorgesetzten-Workflow ermöglicht es HR-Mitarbeitern, Vorgesetzte über einen Zugangslink direkt in den Bewertungsprozess einzubeziehen. Diese können so ihren Input nach einem Login und wenigen Klicks direkt in der Online-Lösung abgeben. Die integrierte Erinnerungsfunktion stellt sicher, dass Zeugnisse zeitnah ausgestellt werden können.

Die wesentlichen Funktionen im Überblick:

- › Integrierter Workflow zur Einbindung der Linienvorgesetzten und Mitarbeiter
- › Übersichtliche Startseite über sämtliche Zeugnisse (offen, archiviert, alle, Workflow-Status und Zeugnisart)
- › Es können mehrere Unternehmensprofile angelegt werden
- › Automatische Umwandlung von Zwischen- in Endzeugnis sowie von Zeugnis für weibliche Arbeitnehmerinnen in ein Zeugnis für männliche Arbeitnehmer und umgekehrt
- › Vorlagen-Manager: Bausteine einfach und schnell direkt im Zeugnistext bearbeiten und als eigene Varianten speichern
- › Quickbewertung – Vollständiges Zeugnis mit einem Klick
- › Erinnerungsfunktion für HR, Vorgesetzte und Mitarbeiter
- › Fertig formatiertes Zeugnis direkt im Tool

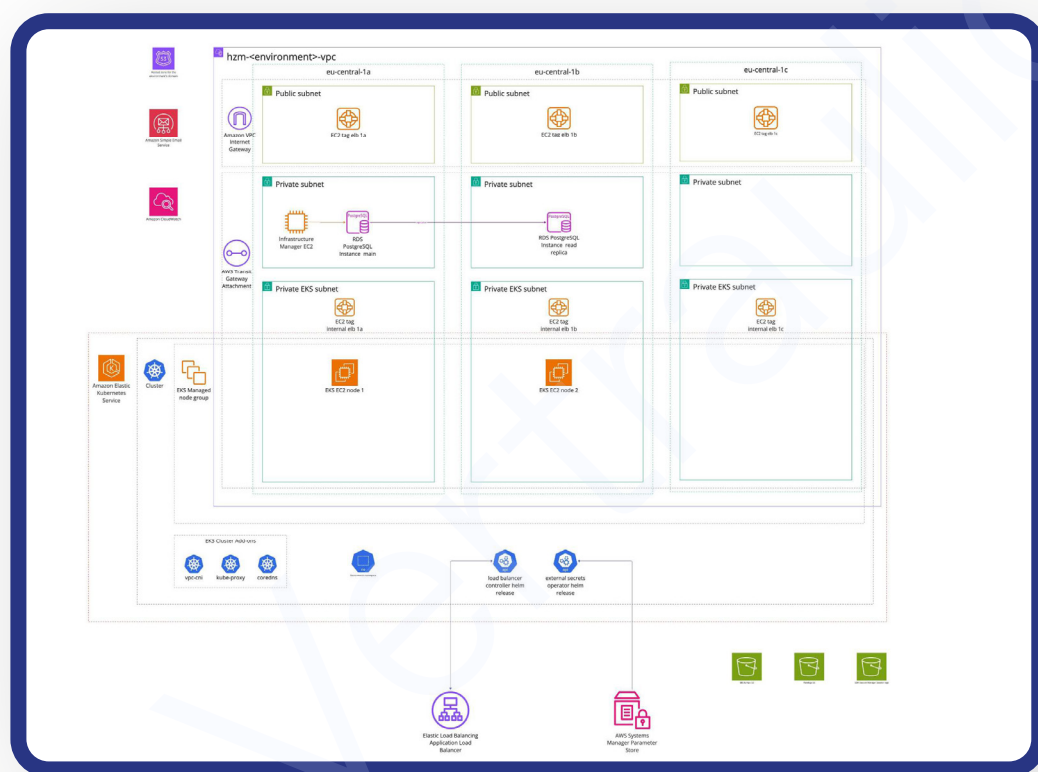
Den Haufe Zeugnis Manager gibt es in vier Versionen: Haufe Zeugnisgenerator, Haufe Zeugnis Manager Basic, Haufe Zeugnis Manager Professional und Haufe Zeugnis Manager Premium. Der Haufe Zeugnisgenerator ist eine Variante mit geringem Funktionsumfang und lediglich in Haufe Office Line-Produkten enthalten. Die Basic-Version richtet sich an Unternehmen mit geringem Zeugnisaufkommen, die Professional-Version richtet sich an Unternehmen mit einem mittleren Zeugnisaufkommen. Die hier dokumentierte Premium-Version bietet als umfangreichste Lösung einen deutlich erweiterten Leistungsumfang und richtet sich an Großunternehmen mit einem hohen Zeugnisaufkommen.

System-Standorte

Sämtliche Daten der Kunden werden ausschließlich auf Systemen in Deutschland gespeichert. Es erfolgt eine Speicherung und Verarbeitung der Daten wie folgt:

- Die Applikation wird bei Amazon Webservices in Frankfurt (EU-central-1) betrieben.
- Das Authentifizierungs- und Autorisierungssystem der Applikation (zentrales Autorisierungs-System der Haufe Group) erfolgt durch die noris network AG, Thomas-Mann-Straße 16 – 20, 90471 Nürnberg.

Architektur/Datenflussdiagramm Haufe Zeugnis Manager Premium



Weitere Angaben zur Organisation des Datenschutzes und der Datensicherheit

Innerhalb der Haufe Group existieren diverse Richtlinien und Vorgaben hinsichtlich der Informationssicherheit beziehungsweise der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit. Zu unseren internen Richtlinien gehören unter anderem:

- Vertraulichkeitsvereinbarungen: Innerhalb der Haufe Group existieren diverse Vorlagen für ein- oder beidseitige Vertraulichkeitsvereinbarungen. Auch sind entsprechende Vereinbarungen Teil der Verträge, die durch den Stabsbereich Legal erstellt sowie betreut werden.
- Datenschutzrichtlinie der Haufe Group: Ziel und Zweck ist es, die Grundlagen für die Umsetzung der Datenschutzanforderungen aus der Datenschutz-Grundverordnung (DSGVO) und dem BDSG festzulegen. Festgelegt sind Grundprinzipien der Datenverarbeitung, der Aufbau der Datenschutzorganisation, Rollenverteilung der Organe innerhalb der Datenschutzorganisation, Datenschutzmanagement-Grundlagen, die Datenübertragung an Dritte, das Verhalten bei Datenschutzvorfällen sowie die Sanktionen bei Verstößen.
- Richtlinie Datenschutzvorfälle in der Haufe Group: Geregelt werden der Umgang mit Datenschutzvorfällen oder Datenpannen, angemessene und rechtskonforme Reaktion bei Datenschutzvorfällen und die rechtlichen Meldepflichten.
- Darüber hinaus existieren bei der Haufe Group Richtlinien zum Themengebiet der Datensicherheit, welche Handlungsanweisungen hinsichtlich sicherer Entwicklung, Authentifizierung und dem Umgang mit Passwörtern enthalten.

Für die Haufe-Lexware GmbH & Co. KG, Haufe-Lexware Services GmbH & Co. KG und Haufe Service Center GmbH ist:

Herr Raik Mickler, E-Mail: dsb@haufe-lexware.com

als Datenschutzbeauftragter bestellt.

Alle Mitarbeiter/-innen sind schriftlich auf die Vertraulichkeit verpflichtet. Die Dokumentation der Verpflichtung erfolgt in der Personalabteilung. Weiterhin erfolgen jährliche Datenschutzbildungen der Datenschutzvorgaben in Form von Präsenzbildungen oder webbasierten Trainings.

Die Haufe Service Center GmbH verarbeitet die Daten ausschließlich im Zusammenhang mit der Erfüllung von Vertrags-/Bestellverpflichtungen ihrer Kunden. Bei Firmenkunden werden Verträge gem. Art. 28 DSGVO über die Auftragsdatenverarbeitung abgeschlossen.

Rollenübersicht

(fachlich in der Anwendung Haufe Zeugnis Manager Premium)

Fachliche Rollen in der Anwendung Haufe Zeugnis Manager Premium	HR Admin	HR Standard	HR Sach- bearbeiter	Vorge- setzter	Mit- arbeiter
Allgemein					
Support (E-Mail/Hotline) aufrufen	•	•	•	•	•
Zeugnis Manager Portal aufrufen	•	•	•		
Produkt-Video ansehen	•	•	•	•	
Startseite					
Sieht alle Zeugnisse seiner Organisation	•	•	•		
Nutzung der Filter	•	•	•		
Filter Zeugnisanträge	•	•	•		
Filter „Offene Zeugnisse“	•	•	•		
Filter „Archivierte Zeugnisse“	•	•	•		
Filter „Bei HR“	•	•	•		
Filter „Beim Vorgesetzten“	•	•	•		
Filter „Zeugnisart“	•	•	•		
Zeugnis erstellen	•	•	•		
Zeugnis erstellen aus Stammdaten (wenn aktiv)	•	•	•		
Suche	•	•	•		
Sortieren	•	•	•		
Offene Zeugnisse öffnen	•	•	•		
Archivierte Zeugnisse öffnen	•	•	•		
Archivierte Zeugnisse löschen	•	•			
Musterzeugnisse löschen	•	•			

Fachliche Rollen in der Anwendung Haufe Zeugnis Manager Premium	HR Admin	HR Standard	HR Sach- bearbeiter	Vorge- setzter	Mit- arbeiter
Wandlung aus Archiv	•	•	•		
Zeugnis als Vorlage verwenden	•	•	•		
Archiviertes Zeugnis bearbeiten	•	•	•		
In Word exportieren	•	•	•		
Aus ZZ ein AZ erstellen	•	•	•		
Quickinfo ansehen	•	•	•		
Administrator Einstellungen					
Administrator Optionen bearbeiten	•				
Administrator Optionen ansehen	•				
Datenschutz Einstellungen					
Datenschutz Optionen bearbeiten	•				
Datenschutz Optionen ansehen	•				
Allgemeine Einstellungen					
Allgemeine Optionen bearbeiten	•	•			
Allgemeine Optionen ansehen	•	•			
Textbausteinmanager					
Textbausteinmanager aufrufen	•	•			
Unternehmensprofil					
Neues Profil erstellen	•	•			
Profil editieren	•	•			
Profil duplizieren	•	•			

Fachliche Rollen in der Anwendung Haufe Zeugnis Manager Premium	HR Admin	HR Standard	HR Sach- bearbeiter	Vorge- setzter	Mit- arbeiter
Profil löschen	•	•			
Profil nutzen	•	•	•	•	
Zeugniserstellung					
Zeugnis anlegen	•	•	•		
Auswahl Berufsgruppe	•	•	•		
Auswahl Zeugnisart	•	•	•		
Auswahl Zeugnisgrund	•	•	•		
Auswahl Sprache	•	•	•		
Tätigkeitsbezeichnung in Combobox speichern	•	•			
Abteilung in Combobox speichern	•	•			
Änderung 1. Unterzeichner	•	•	•	•	
Änderung 2. Unterzeichner	•	•	•	•	
Tätigkeitsbeschreibung eingeben	•	•	•	•	•
Tätigkeit als Vorlage anlegen	•	•			
Mitarbeiter bewerten	•	•	•	•	
Besondere Fähigkeiten/Kompetenzen/ Arbeitserfolge bearbeiten	•	•	•	•	•
Besondere Fähigkeiten/Kompetenzen/ Arbeitserfolge als Vorlage speichern	•	•			
Vorgesetzten Workflow					
An VG senden	•	•	•		
Mail an VG bearbeiten	•	•	•		
Zugang für VG sperren	•	•	•		

Fachliche Rollen in der Anwendung Haufe Zeugnis Manager Premium	HR Admin	HR Standard	HR Sach- bearbeiter	Vorge- setzter	Mit- arbeiter
Mitarbeiter Workflow für Tätigkeitsbeschreibung					
Mitarbeiter einladen				•	
Zugang für Mitarbeiter sperren	•	•	•	•	
Tätigkeitsbeschreibung eingeben	•	•	•	•	•
Freigabe Workflow					
An VG zur Freigabe senden	•	•	•		
Zugang für VG entziehen	•	•	•		
Kommentare hinterlassen	•	•	•	•	
Workflow Nutzer					
Workflow Nutzer löschen	•				
Einsicht in Anzahl aktiver Workflows pro Workflow Nutzer	•				
Zeugnis abschließen					
Varianten auswählen	•	•	•		
Alle Vorlagen anzeigen	•	•	•		
Änderung im Zeugnis als Vorlage speichern	•	•			
Zeugnisse editieren	•	•	•		
Seitenränder in Zeugnisansicht einstellen	•	•	•		
Schrift in Zeugnisansicht formatieren	•	•	•		
Archivieren	•	•	•		
Drucken	•	•	•		

Fachliche Rollen in der Anwendung Haufe Zeugnis Manager Premium	HR Admin	HR Standard	HR Sach- bearbeiter	Vorge- setzter	Mit- arbeiter
Exportieren	•	•	•		
Status manuell ändern (Zeugnis gedruckt, Zur Unterschrift, Zeugnis übergeben, Archiviert)	•	•	•		
Zeugnisse wandeln					
Aus Zwischenzeugnis wird Abschlusszeugnis	•	•	•		
Aus deutschem Zeugnis wird englisches Zeugnis	•	•	•		
Zeugnis als Vorlage verwenden	•	•	•		
Mein Konto/User verwalten					
Benutzer anlegen (inkl. Rechte, Orga, Rollen)	•				
Benutzer löschen	•				
Benutzerdaten zurücksetzen (z. B. Passwort)	•				
Benutzer Organisationen/ Sub-Organisationen zuweisen	•				
Zeugnisanträge					
Zeugnisanträge konfigurieren/aktivieren	•				
Zeugnisantragslink inaktiv setzen	•				
Zeugnisanträge akzeptieren oder ablehnen	•	•	•		
Zeugnisanträge stellen	•	•	•	•	•
Umstellung auf englische GUI					
Englische GUI aktivieren	•				
Umschalten auf englische GUI	•	•	•	•	•

Fachliche Rollen in der Anwendung Haufe Zeugnis Manager Premium	HR Admin	HR Standard	HR Sach- bearbeiter	Vorge- setzter	Mit- arbeiter
Sichten					
Sieht seine offenen Zeugnisse in den berechtigten Orgas	•	•	•		
Sieht alle offenen Zeugnisse in den berechtigten Orgas	•	•	•		
Sieht seine archivierten Zeugnisse in den berechtigten Orgas	•	•	•		
Sieht alle archivierten Zeugnisse in den berechtigten Orgas	•	•	•		
Report, wie viele Zeugnisse sich in welchem Status befinden und wie viele Zeugnisse ins- gesamt je Unternehmensprofil erstellt wurden	•				
Konfiguration					
Vorgesetzter darf Stammdaten bearbeiten; default: ja	•	•			
Vorgesetzter kann besondere Fähigkeiten/Kom- petenzen/Arbeitserfolge bearbeiten; default: ja	•	•			
Kommentare und Zeugnisdokumentation beim Archivieren löschen; default: nein	•	•			
Workflow-E-Mails als privat markieren; default: nein	•				
Frist für die automatische Sperrung des Zugangslinks für den Vorgesetzten; default: 2 Wochen	•				
E-Mail-Domains für den Workflow einschränken; default: nein	•				
Zeugnisse als E-Mail-Anhang (PDF/RTF) direkt aus dem Haufe Zeugnis Manager versenden; default: nein	•				

Fachliche Rollen in der Anwendung Haufe Zeugnis Manager Premium	HR Admin	HR Standard	HR Sach- bearbeiter	Vorge- setzter	Mit- arbeiter
Frist für die Löschung von archivierten Abschluss-, Zwischen- und einfache Zeugnisse; default: keine Löschung	•				
HR darf Allgemeine Einstellungen verändern und den Textbaustein Manager benutzen; default: Ja	•				
Vorgesetzter kann bei der Bewertung eines Mitarbeiters auch den Textbaustein auswählen; default: nein	•				
Vorgesetzter darf Mitarbeiter bei der Zeugnis-erstellung einbeziehen; default: Ja	•				
Welche Vorlagen können Vorgesetzte und Mitarbeiter bei der Bearbeitung der Tätigkeitsbeschreibung auswählen; default: alle	•				
Eigene Felder für die Stammdaten-Anlage definieren	•				



Betrieb der Applikation

Das Hosting der Haufe Zeugnis Manager Applikation erfolgt im Rechenzentrum der Amazon Webservices in Frankfurt (EU-central-1). Mit diesem Dienstleister besteht ein Vertrag nach Art. 28 DSGVO über Auftragsdatenverarbeitung.

AWS verfügt über die folgenden Zertifizierungen:

- ISO 27001: Informationssicherheit allgemein
- ISO 27017: Informationssicherheit beim Cloud Computing
- ISO 27018: Datenschutz-Standard für Cloud Dienste
- ISO 27701: Erweiterung der ISO 27001 hinsichtlich Datenschutz
- ISO 22301: Standard für Business Continuity Management
- BSI C5: Cloud Computing Compliance Criteria Catalogue des BSI

Betrieb des Authentifizierungs- und Autorisierungssystems

Der Betrieb des Authentifizierungs- und Autorisierungssystems erfolgt in einem Rechenzentrum der noris network AG, Thomas-Mann-Straße 16 – 20, 90471 Nürnberg. Mit diesem Dienstleister besteht ein Vertrag nach Art. 28 DSGVO über Auftragsverarbeitung.

Dieses Unternehmen verfügt über die folgenden Zertifizierungen:

- ISO 27001: Informationssicherheit allgemein
- BSI C5: Cloud Computing Compliance Criteria Catalogue des BSI

Spezielle Sicherheitsmaßnahmen

Wegen des Schutzbedarfs der Daten werden:

- Die Server-Systeme in das kommerzielle Vulnerability Management System der Haufe Group aufgenommen. Dieses System führt in zyklischen Abständen authentifizierte Scans der Server-Systeme durch und überprüft diese auf das Fehlen von Sicherheitsupdates.
- Externe Penetrationstest der Applikation durch Dritte werden zyklisch durchgeführt (i. d. R. jährlich).
- Verwendung einer AES 256 Bit Verschlüsselung für die folgenden Daten:
 - Zeugnisdokument (PDF)
 - Bewertungen bzw. Zeugnisnoten
 - Zeugnisinhalte (Text, inkl. Tätigkeitsbeschreibung)
 - Werdeganginhalte (Text)
 - Kommentare (Text)



Technische und organisatorische Maßnahmen

1. Allgemeines		
1.1	Werden (regelmäßig) unabhängige Sicherheitsüberprüfungen durch externe Stellen durchgeführt?	<p>Der Betrieb der HZM-Lösung erfolgt im Rechenzentrum von Amazon Webservices in Frankfurt (EU-central-1). Es werden jährlich Überwachungsaudits und alle drei Jahre Re-Zertifizierungsaudits durchgeführt.</p> <p>Des Weiteren werden in zyklischen Abständen Penetrations-tests auf Web-Applikationsebene durchgeführt (i. d. R. jährlich). Diese werden von unserer Information Security Abteilung beauftragt und durch externe Unternehmen durchgeführt.</p> <p>Ergänzend werden die Basis-Systeme der Haufe Group zyklisch durch das Vulnerability Management gescannt.</p>
1.2	Existieren formale schriftlich dokumentierte Richtlinien hinsichtlich der Informationssicherheit?	<p>Es existieren diverse Richtlinien und Vorgaben hinsichtlich der Informationssicherheit beziehungsweise der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit, wie z. B.:</p> <ul style="list-style-type: none">• Vertraulichkeitsvereinbarungen• Datenschutzrichtlinie• Richtlinie Datenschutzvorfälle
1.3	Ist ein(e) Datenschutzbeauftragte/r bestellt?	Raik Mickler als Konzerndatenschutzbeauftragter E-Mail: dsb@haufe-lexware.com
1.4	Ist ein IT-Sicherheitsbeauftragter/Chief Information Security Officer beschäftigt?	Jochen Vogel als CISO E-Mail: security@haufe-lexware.com
1.5	Werden die Mitarbeiter/-innen auf Vertraulichkeit verpflichtet? Wie werden diese Verpflichtungen dokumentiert?	Sämtliche Mitarbeiter, die mit personenbezogenen Daten arbeiten, sind auf Vertraulichkeit verpflichtet. Die Dokumentation erfolgt in der Personalabteilung.
1.6	Sind die Mitarbeiter/-innen hinsichtlich der datenschutzrechtlichen Vorgaben nachweislich geschult?	Ja, es finden regelmäßige Trainings zur Sensibilisierung statt.

1.	Allgemeines	
1.7	Gibt es ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DSGVO?	Ja.
1.8	Wer wird bei entdeckten Sicherheitsvorfällen unverzüglich informiert?	Der CISO der Haufe Group; bei möglichen Verletzungen des Schutzes personenbezogener Daten der Datenschutzbeauftragte der Haufe Group.
1.9	Sind die Ergebnisse von Penetration-Tests einsehbar?	Eine Einsichtnahme ist möglich. Details zu möglichen Schwachstellen oder Informationen mit Personenbezug können aus Datenschutz- und Sicherheitsgründen nicht eingesehen werden.
1.10	Wie ist das System vor Fremdangriffen geschützt?	<ul style="list-style-type: none"> • Gemäß Best Practices • Secure Development Lifecycle • Secure Operation • Unabhängige Überprüfung
1.11	Gibt es eine Passwortrichtlinie für die Applikation?	<p>Als Passwort-Richtlinie zur Nutzung des Haufe Zeugnis Manager Premium sind innerhalb des Authentifizierungssystems „Haufe-Suite“ beliebige Vorgaben möglich: bzgl. Laufzeit des Passworts, Länge, Sonderzeichen, Passwort-History, etc.</p> <p>In der Standardeinstellung von Haufe Zeugnis Manager Premium innerhalb des Authentifizierungssystems „Haufe-Suite“</p> <ul style="list-style-type: none"> • darf der Benutzer sein Passwort selbst ändern. • muss der Nutzer sein Passwort nach dem ersten Login ändern. • ist die Zurückstellung eines Passworts maximal einmal am Tag möglich • muss das Kennwort mindestens 8 Zeichen lang sein, Groß- und Kleinbuchstaben enthalten, mindestens eine Ziffer oder ein Sonderzeichen enthalten. Es dürfen keine aufeinanderfolgenden Zeichenketten, wie „aaa“, „111“, ... verwendet werden. Das Passwort darf nicht mit Leerzeichen anfangen und enden. <p>Sie können auch stärkere Passwortvorgaben einstellen. Bitte kontaktieren Sie den Support.</p>

1. Allgemeines

1.12	Besteht eine interne Audit-Funktion bzgl. der Applikation?	Der Haufe Zeugnismanager Premium bietet die Möglichkeit, die Zeugnisdokumentation anzuzeigen. Zudem wird übergreifend ein Audit-Log generiert, welches sämtliche Aktionen mit UserID und OrganisationsID protokolliert.
1.13	Kann sichergestellt werden, dass Daten nicht außerhalb einer geographisch-definierten Region weitergegeben werden?	Ja. Alle personenbezogenen Daten verbleiben in Deutschland.
1.14	Haben Administratoren oder Supportmitarbeiter Einblick in personenbezogene Daten?	<p>Berechtigte Mitarbeiter der Haufe Gruppe aus dem Bereich Support haben Zugriff auf Daten, die ein Nutzer des Haufe Zeugnis Manager zur Registrierung benötigt. Dies sind Name, Vorname, E-Mail-Adresse und Passwort. Das Passwort kann durch den Support nur geändert und nicht ausgelesen werden.</p> <p>Zugriff auf darüberhinausgehende Daten des Haufe Zeugnis Manager kann im Supportfall notwendig sein. Der Verantwortliche definiert bei Projektabnahme im Abnahmeprotokoll, in welcher Weise der Haufe Support im Supportfall Zugriff haben soll. Hier stehen ihm 3 Optionen zur Auswahl:</p> <ul style="list-style-type: none">• Haufe Support kann zu Supportzwecken ohne gesonderte Freigabe Zugang haben• Zugriff nur nach expliziter Einzelfreigabe für einen Supportfall, temporär auf 4 Stunden begrenzt oder• jeglicher Zugang für den Haufe Support ist nicht gestattet. (Achtung! Supportunterstützung ist hier nicht oder nur begrenzt möglich. Verpflichtung des Lizenzgebers zur Supportunterstützung entfällt dadurch). <p>Auf Testsystemen werden keine Echtdaten verwendet.</p> <p>Im Programm enthalten ist eine Funktion für den Kunden-Support. Damit können uns Mitarbeiter Fragen zum Produkt stellen. Der entsprechende Mitarbeiter kann hier seine Telefonnummer eintragen.</p> <p>Die E-Mail an unseren Support wird angereichert mit folgenden Daten (Name; E-Mail-Adresse; Haufe Zeugnis Manager-Programmversion; vom Nutzer eingesetzter Browserversion und Betriebssystem).</p>

1. Allgemeines

- | | | |
|------|--|--|
| 1.15 | Wann werden die Zeugnisdaten gelöscht? | <p>Sie können jederzeit im Programm selbst die erstellten Zeugnisse löschen.</p> <p>Sie können festlegen, dass archivierte Zeugnisse nach einem bestimmten Zeitpunkt automatisch gelöscht werden.</p> <p>Nach dem Ende des Vertrags für den Haufe Zeugnis Managers haben wir die Zeugnisdaten noch 30 Tage für Sie gespeichert, danach werden sämtliche Zeugnisdaten unwiderruflich gelöscht. Dazu gehören neben den erstellten Zeugnissen auch die selbst angelegten Textbausteine, angelegten Stammdaten und Unternehmensprofile.</p> |
| 1.16 | Wie sind die Zeugnisse abgespeichert? | <p>Die Daten sind in einer gemeinsamen Datenbank abgespeichert. Es wird durch automatische Prozesse (Interceptoren) sichergestellt, dass nur die eigenen Daten geladen werden können.</p> <p>Jeder Mandant hat einen eigenen Schlüssel, mit dem die Zeugnisdaten (Bewertung, Zeugnistext, Tätigkeitsbeschreibung, Werdegangtext und das Zeugnisdokument-PDF) verschlüsselt abgespeichert sind.</p> <p>Nicht verschlüsselt abgespeichert sind Angaben in den Personalstammdaten (u.a. Name, Vorname, Abteilung, Personalnummer, Geburtsdatum, Tätigkeitsbezeichnung), da Sie im Haufe Zeugnis Manager nach diesen Daten suchen können. Würden wir diese Angaben verschlüsseln, wären wesentliche Funktionalitäten nicht mehr nutzbar (v.a. auf der Startseite) und die einfache Handhabung des Haufe Zeugnis Managers Premium massiv eingeschränkt.</p> |
| 1.17 | Was für Sicherheits- und Datenschutzrichtlinien existieren bei Ihnen (z.B. Basisanforderung ITSicherheit, Passwort-Policy, Richtlinien zur mobilen IT ...) | <p>Innerhalb der Haufe Group gibt es folgende Richtlinien: Richtlinie Datenschutz, Richtlinie zum Umgang mit Datenschutzvorfällen, Richtlinie Basisanforderung ITSicherheit, Passwort-Policy, Richtlinien zur mobilen IT, Secure Coding Guidelines, Benutzerrichtlinie.</p> |
| 1.18 | Existiert ein Notfallkonzept/-Handbuch? | <p>Ja</p> |
| 1.19 | Wurde das Unternehmen anlassbezogen durch die zuständige Datenschutz-Aufsichtsbehörde geprüft? | <p>Nein</p> |

1. Allgemeines

1.20	Erfolgt die Vertragserfüllung ausschließlich in Liegenschaften und auf Systemen mit Standorten innerhalb der EU? Relevant sind hierbei die eingesetzten Sub-Dienstleister, die im Rahmen der Auftragserfüllung Zugriff auf personenbezogene Daten haben.	Ja
1.21	Existieren dokumentierte und regelmäßig gereviewte Prozesse und Praktiken zur Vermeidung und Behebung von Sicherheitslücken in den bereitgestellten Diensten?	Die Server-Systeme sind in das Vulnerability Management System der Haufe Group integriert und werden i. d. R. alle zwei Wochen auf Schwachstellen geprüft. Diese prüfen den Stand der Sicherheitsupdates durch authentifizierte Scans. Entsprechende Erkenntnisse fließen in die Patch-Prozesse der Dienstleister ein. Weiterhin werden statische Code-Analysen durchgeführt. Diese setzen im Entwicklungsprozess an und dienen dazu, technische Implementierungsfehler während des Entwicklungsprozesses zu identifizieren. Darüber hinaus werden zyklisch externe Penetrationstests der Applikation durchgeführt (i. d. R. jährlich).
1.22	Welche Formen von Authentifizierung, auf Basis des Authentifizierungssystems des Kunden, werden angeboten (z. B. Federation auf Basis von LDAP)?	Über die bei der Noris Network AG in Nürnberg betriebenen Authentifizierungs- und Autorisierungssysteme (Haufe-Suite) ist eine Anbindung über den SSO-Service des Kunden via SAML2 möglich.
1.23	Erfolgt eine Information des Kunden bei Sicherheits- und Datenschutzvorfällen, welche die Daten des Mandanten betreffen könnten?	Es existiert ein Prozess, welcher eine Information des Kunden bei Sicherheitsvorfällen mit Datenschutzrelevanz vorsieht.
1.24	Existiert ein Datenschutz- bzw. Sicherheitskonzept für die Anwendung?	Die hier vorliegende Dokumentation zu den technischen und organisatorischen Maßnahmen beinhaltet die Ausführungen hinsichtlich Datenschutzes und Datensicherheit.

2. Zutrittskontrolle

Definition: Maßnahmen, die dazu geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

2.1	Existiert ein schriftlich dokumentiertes Zutrittsberechtigungssystem für Mitarbeiter des Unternehmens bzw. nicht zutrittsberechtigte Personen (z. B. Geschäftskunden/ Besucher, Reinigungsfirmen, Wartungsfirmen etc.)?	<p>Nur autorisiertes AWS-Personal erhält Zugang zu den physischen Rechenzentren. Alle Mitarbeiter, die Zugang zu einem Rechenzentrum benötigen, müssen zunächst einen Antrag auf Zugang stellen und eine gültige geschäftliche Begründung vorlegen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Die Anfrage wird geprüft und von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt.</p> <p>Der Zugang von Dritten muss von autorisierten AWS-Mitarbeitern beantragt werden, die auch eine gültige geschäftliche Begründung für diesen Zugang vorlegen müssen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Diese Anfragen werden von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt. Personen mit einem Besucherausweis müssen diesen bei Ankunft am Standort vorlegen und werden von autorisiertem Personal angemeldet und begleitet.</p>
2.2	Gibt es einen Sicherheitsdienst? Welche Verantwortungsbereiche/ Aufgaben übernimmt dieser?	Der physische Zugang wird durch professionelles Sicherheitspersonal an den Gebäudeeingängen kontrolliert. Dabei werden Überwachung, Meldeanlagen und andere elektronische Vorrichtungen eingesetzt. Autorisiertes Personal erlangt über Multi-Faktor-Authentifizierungsmechanismen Zugang zu den Rechenzentren. Die Eingänge zu den Serverräumen sind mit Geräten abgesichert, die Alarm auslösen, wenn die Tür aufgebrochen oder offengehalten wird.
2.3	Findet eine Videoüberwachung statt? Wie lange werden die Videos gespeichert?	Physische Zugangspunkte zu Serverräumen werden von CCTV-Kameras mit Aufzeichnungsfunktion überwacht. Die Aufnahmen werden gemäß behördlichen und Compliance-Anforderungen aufbewahrt.

2. Zutrittskontrolle

Definition: Maßnahmen, die dazu geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

2.4	Gibt es ein Alarmsystem? Wer wird über dieses alarmiert?	In der Datenebene sind elektronische Einbruchmeldesysteme installiert, die sicherheitsrelevante Ereignisse erkennen und automatisch die zuständigen Mitarbeiter alarmieren. Die Ein- und Ausgänge zu den Serverräumen sind mit Geräten gesichert, die von jeder Person eine Multi-Faktor-Authentifizierung verlangen, bevor sie Zutritt erhält, und einen Ausweis, bevor sie den Raum verlässt. Diese Geräte lösen einen Alarm aus, wenn die Tür ohne Authentifizierung gewaltsam geöffnet, offengehalten oder während eines Notfalls zum Verlassen der Wohnung geöffnet wird. Türalarmanlagen sind auch so konfiguriert, dass sie Situationen erkennen, in denen eine Person eine Datenebene ohne Multi-Faktor-Authentifizierung betritt oder ohne ordnungsgemäßes Badging verlässt. In diesem Fall wird umgehend ein Alarm ausgelöst und an die AWS Security Operations Center zur Protokollierung, Analyse und Reaktion gesendet.
-----	---	--

3. Zugangskontrolle

Definition: Maßnahmen, die dazu geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

3.1	Gibt es Regelungen zu Vergabe, Entzug und zyklischen Reviews (auf die Notwendigkeit) von Zugangsberechtigungen?	Entsprechendes wird über den Starter-Changer-Leaver-Prozess realisiert. Weiterhin finden zyklische Reviews auf die Notwendigkeit der Berechtigungen statt. Diese finden mindestens einmal pro Jahr statt.
3.2	Werden sämtliche Berechtigungen lediglich auf Basis der minimalen Rechte (Need-to-Know) vergeben?	Es werden für die einzelnen Ebenen unterschiedliche Teams eingesetzt, die lediglich Zugriff auf die von diesen Mitarbeitern verantworteten Komponenten haben.
3.3	Existieren Maßnahmen zum Schutz von Passwortdateien und Passwörtern auf der Applikationsebene?	Die Passwörter der Applikation werden im PBKDF2WithHmacSHA256-Verfahren auf einem zentralen Authentifizierungssystem bei der noris network AG gespeichert.

3. Zugangskontrolle

Definition: Maßnahmen, die dazu geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- | | | |
|-----|---|--|
| 3.4 | Gibt es eine Begrenzung der Anmeldeversuche bei wiederholten Fehlversuchen (Anzahl/Konfigurierbarkeit)? | Eine Zurücksetzung erfolgt erst nach einer eindeutigen Identifikation des Mitarbeiters. Auf Seiten des zentralen Authentifizierungs- und Autorisierungssystems der Applikation kann ein Brute-Force-Schutz konfiguriert werden. Dieser erlaubt die Sperrung eines Accounts nach einer konfigurierbaren Anzahl von Fehlversuchen in Kombination mit einer automatischen Entsperrung nach einer gewissen Zeitspanne oder lediglich nach manueller Freischaltung. |
| 3.5 | Wie erfolgt der Zugriff im Rahmen z. B. von Telearbeit/ Homeoffice bzw. mobile Computing? Welche Vorgaben existieren? | Telearbeit ist lediglich unter Verwendung eines VPNs mit einer Zwei-Faktor-Authentifizierung (Zertifikat/Secure-App) in Kombination von einem Benutzernamen und Passwort) möglich. Die Dateisysteme der Notebooks sind verschlüsselt. |
| 3.6 | Existieren Regelungen bei Verlassen des Arbeitsplatzes (z.B. Sperren des Rechners)? | Die Rechner werden automatisch nach 15 Minuten Inaktivität gesperrt. |
| 3.7 | Werden Intrusion Detection/ Prevention Systeme eingesetzt? | Ja. |
| 3.8 | Wird ein Virenschanner auf allen Server-Systemen eingesetzt? Wenn ja, in welchem Intervall werden die Signaturen geupdatet? | Für Daten innerhalb der Anwendung wird ein Clam-AV eingesetzt. Dieser wird einmal täglich mit den neusten Anti-Viren-Signaturen versehen. |



4. Zugriffskontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- | | | |
|-------|---|--|
| 4.1 | Existiert ein Berechtigungskonzept für die Applikation zur bedarfsorientierten Ausgestaltung der Zugriffsrechte (differenzierte Berechtigungen für Profile, Rollen, Transaktionen und Objekte)? | Es existiert ein Rollen- und Berechtigungskonzept, welches den Zugriff beschränkt, siehe Seite 7. |
| <hr/> | | |
| 4.2 | Einsatz von Verschlüsselungstechnik bei Notebooks? | Eine Festplattenverschlüsselung wird eingesetzt. Diesbezüglich kommen unterschiedliche Lösungen wie z.B. Truecrypt, Bitlocker oder die Festplattenverschlüsselung von Apple zum Einsatz. |

5. Trennungskontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- | | | |
|-------|---|--|
| 5.1 | Wie und wo erfolgt die Trennung der Daten von Daten anderer Kunden/Mandanten (z.B. physisch getrennte Serversysteme je Kunden)? | Die Daten verschiedener Kunden liegen in einer zentralen Datenbank; getrennt über die Mandantenummer. Es gibt nicht für jeden Kunden einen eigenen Datenbankserver oder ein eigenes Datenbankschema. |
| <hr/> | | |
| 5.2 | Erfolgt eine logische und physikalische Trennung der Produktions-, Integrations- und Entwicklungssysteme voneinander? | Neben der produktiven Umgebung existiert eine Staging-Umgebung für Tests sowie Entwicklungsumgebungen. |
| <hr/> | | |
| 5.3 | Werden produktive Daten des Mandanten auf anderen Systemen als dem Produktivsystem (z.B. Verwendung der Echtdaten auf den Testsystemen zu Testzwecken) gespeichert? | Auf den Testsystemen (Staging) werden nur anonymisierte Daten verwendet, bei denen sämtliche schützenswerten personenbezogene Daten anonymisiert sind. |

6. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Definition: Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

6.1 Wie werden sensible personenbezogene Daten im Haufe Zeugnis Manager pseudonymisiert?

Der Haufe Zeugnis Manager Premium pseudonymisiert die Daten durch Verschlüsselung der Daten:

- sowohl bei der Übermittlung (https)
- als auch im Rahmen der Speicherung sensibler personenbezogener Zeugnisdaten auf Datenbankebene (256 Bit AES).

6.2 Einsatz von Verschlüsselungstechnik in Datenbanken?

Es kommt eine 256 Bit AES Verschlüsselung für die folgenden Zeugnisdaten zum Einsatz:

- Bewertung bzw. Zeugnisnoten
- Zeugnistext inkl. Tätigkeitsbeschreibung
- Werdegangtext
- Zeugnisdokument (PDF)
- Kommentare (Text)

Der Schlüssel wird individuell für den Lizenznehmer erzeugt und separiert von den sonstigen personenbezogenen Daten gespeichert.



7. Weitergabekontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- | | | |
|------------|---|--|
| 7.1 | Werden personenbezogene Daten an weitere Anwendungen/ Systeme übertragen (z. B. durch Schnittstellen/Web-Services)? Nennung der entsprechenden Schnittstellen inklusive der übertragenen Datenkategorien. Wie werden entsprechende Übertragungen protokolliert? | Es findet keine Übertragung von personenbezogenen Daten aus der HZM Applikation an weitere Systeme statt. Lediglich die Authentifizierung und Autorisierung erfolgt an einem zentralen Authentifizierungs- und Autorisierungssystem, welches von der Noris Network AG in Nürnberg betrieben wird.

Optional kann eine Schnittstelle zum Import von Mitarbeiterstammdaten eingerichtet werden. Dies geschieht jedoch nur auf Wunsch des Kunden und ist standardmäßig nicht aktiviert. |
| 7.2 | Ist der Zugriff auf die Applikation lediglich verschlüsselt möglich? Das Verfahren (z. B. TLS) inklusive der verwendeten Algorithmen angeben (z. B. RSA 2048 in Kombination mit AES 256). | Ja, wir unterstützen TLS 1.2 und TLS 1.3 unter Verwendung von RSA 4096 bits. |
| 7.3 | Werden Datenträger (z. B. Backups) an eine zusätzliche Lokalität (z. B. Katastrophenarchiv, Tresor, Bankschließfach) transportiert? | Nein, es erfolgt keine Sicherung außerhalb der AWS Rechenzentren (EU-central-1). |



8. Eingabekontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

8.1 Was wird in der Anwendung protokolliert (z. B. Eingabe, Veränderung, Löschung ... von Daten, Berechtigungen etc.)?

In der Anwendung selbst werden die Daten in dem Prozess der Zeugniserstellung bei Übergabe von HR an einen Vorgesetzten und bei Übergabe vom Vorgesetzten an HR protokolliert.

Hierbei werden folgende Daten zwischengespeichert:

- Tätigkeitsbeschreibung
- Kompetenzen
- Besondere Arbeitserfolge
- Benotung der Kriterien
- Vom Vorgesetzten empfohlener Textbaustein
- Kommentare zu den Bewertungen
- Datum und Uhrzeit der Übergabe an die nächste Instanz im Prozess

Der Administrator der Anwendung kann einstellen, dass diese Dokumentation beim Archivieren des Zeugnisses automatisch gelöscht wird.

Übergreifend wird ein Audit-Log generiert. Hier werden sämtliche Aktionen (keine Zeugnisdaten) mit der UserID und OrganisationsID protokolliert. Diese Protokollierung dient der Sicherheit und erfasst:

- Aufrufe des Zeugnismanagers
- Transaktionen (Zeugnis laden, Zeugnis editieren, Zeugnis an Vorgesetzte weiterleiten, Zeugnis archivieren, Zeugnis löschen, Zeugnis aus dem Archiv bearbeiten, Zeugnis wandeln) Die Protokollierungsdaten werden 90 Tage aufbewahrt:

8. Eingabekontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- | | | |
|-----|---|--|
| 8.2 | Was wird auf Datenbankebene (Transaktionsprotokoll/Audit-Log der Datenbank) protokolliert? Bitte entsprechende Log-Kategorien inklusive Log-Inhalte je Kategorie nennen. Wie lange werden diese Log-Daten aufbewahrt? | Es werden Transaktionsprotokolle erstellt, welche auf Stundenbasis als Backup verwendet werden. Aus diesen können Veränderungen an Inhalten entsprechend rekonstruiert werden. Diese Daten werden für 90 Tage gespeichert. |
| 8.3 | Wird sichergestellt, dass die Protokolldaten nicht verändert werden können? | Ja, durch die Übertragung der Protokolldaten an einen zentralen Syslog-Server. |

VERFÜGBARKEIT UND BELASTBARKEIT (Art. 32 Abs. 1 lit. b DS-GVO)

9. Verfügbarkeitskontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- | | | |
|-----|---|--|
| 9.1 | Existiert ein Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung (Notfallplan)? | Ja, gem. ISO 22301 |
| 9.2 | Werden zwei unabhängige Rechenzentren mit ausreichend Geo-Redundanz verwendet (zwei unterschiedliche Risikoumgebungen)? | Die Infrastruktur wird redundant über Rechenzentren verteilt, dementsprechend ist der Service auch bei Komplettausfall eines Rechenzentrums weiterhin verfügbar. |
| 9.3 | Existieren Tests und Freigabeverfahren (z. B. nach Patches, neuen Releases etc.)? Wenn ja, wie sehen diese aus? | Die Prozesse orientieren sich diesbezüglich an der IT Infrastructure Library (ITIL). |

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG
(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

10. Auftragskontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

10.1	Welche Subauftragnehmer/ Dienstleister haben Zugriff auf Daten des Auftraggebers?	<p>Zugriff auf die Zeugnisdaten haben nur ausgewählte Mitarbeiter bei Haufe. AWS hat keinen Zugriff.</p> <p>Zugriff auf die Authentifizierungsdaten hat die: noris Network AG in Nürnberg, welche das Authentifizierungs- und Autorisierungssystem und die zugrundeliegende Infrastruktur betreiben.</p>
10.2	Welche Subauftragnehmer außerhalb der EU haben Zugriff auf personenbezogene Daten des Auftraggebers?	Keine.
10.3	Liegt mit Subunternehmern ein schriftlicher Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO, ein NDA, eine Verpflichtung zur Vertraulichkeit vor?	Mit den oben genannten Dienstleistern besteht ein Vertrag gem. Art. 28 DSGVO; die Mitarbeiter, die Zugriff auf Daten des Auftraggebers haben, sind auf das Datengeheimnis/ Vertraulichkeit verpflichtet.
10.4	Ist eine Kontrolle der technischen und organisatorischen Maßnahmen bei vorheriger Anmeldung und Terminabstimmung vor Ort beim Subunternehmer möglich?	Nein.
10.5	Wie oft wird eine Kontrolle der technischen und organisatorischen Maßnahmen beim Subunternehmer durchgeführt?	Es erfolgen Kontrollen durch den Datenschutzbeauftragten bei den oben genannten Dienstleistern. Diese Prüfung erfolgt einmal jährlich.
10.6	Erfolgt bei Fehlern hinsichtlich der Datenverarbeitung oder Verstoß gegen den Datenschutz sowie IT-Sicherheitsvorfällen eine unverzügliche Information an den Auftraggeber? Wer erhält diese Information?	Ja, die Information erfolgt an die im Vertrag mit dem Auftraggeber benannte Stelle.