AVV Anlage 2k -- Managed Service Password Management

Produktspezifische Anlage zum Rahmen-Auftragsverarbeitungsvertrag

1. Bezeichnung des Services

Managed Service Password Management

2. Gegenstand der Verarbeitung

Bereitstellung, Lizenzierung und Betrieb des Zero-Knowledge-Passwortmanagers heylogin (heylogin GmbH, Braunschweig) für die Beschäftigten des Auftraggebers. Der Auftragnehmer betreibt die Kundenorganisation auf der heylogin-Plattform als delegierter Administrator, verwaltet im vereinbarten Umfang Benutzer, Teams und Berechtigungen und ist zentraler Ansprechpartner für den Service.

Die in den Tresoren gespeicherten Zugangsdaten werden durch heylogin Ende-zu-Ende auf den Endgeräten der Nutzer verschlüsselt (ohne Master-Passwort, gebunden an die Sicherheitschips der Geräte). Weder der Auftragnehmer noch heylogin haben Zugriff auf diese Zugangsdaten im Klartext. Gegenstand der Verarbeitung durch den Auftragnehmer sind die zur Verwaltung der Organisation erforderlichen Konto- und Organisationsdaten sowie Zugriffs- und Audit-Protokolle.

3. Zweck der Verarbeitung

Sichere, zentrale Verwaltung und kontrollierte Bereitstellung von Zugangsdaten für die Beschäftigten des Auftraggebers. Durchführung von Benutzer- und Berechtigungsverwaltung, Zugriffskontrolle und Audit-Logging zur Erfüllung der Sicherheitsanforderungen des Auftraggebers.

4. Kategorien personenbezogener Daten

- Benutzerkennungen und Login-Identitäten (direkt oder indirekt personenbezogen)

- Namen und E-Mail-Adressen der Benutzer
- Organisations- und Berechtigungsdaten (Teams, Rollen, Gruppen- und Teamzugehörigkeit)
- Geräte- und Browserinformationen (registrierte Anmeldegeräte, Gerätekennungen)
- Zugriffs- und Audit-Logs (Anmelde- und Verwaltungsvorgänge), IP-Adressen

Hinweis zu den gespeicherten Zugangsdaten: Die in den Tresoren abgelegten Zugangsdaten (Benutzernamen, Passwörter, Schlüssel, TOTP-Secrets) werden Ende-zu-Ende verschlüsselt und sind für den Auftragnehmer und für heylogin **nicht im Klartext zugänglich**.

Besondere Kategorien (Art. 9 DSGVO): werden durch den Auftragnehmer nicht gezielt verarbeitet. Inhalte, die der Auftraggeber bzw. dessen Nutzer eigenständig als Zugangsdaten/Notizen in den Tresoren ablegen, unterliegen der Ende-zu-Ende-Verschlüsselung; die Verantwortung für deren Zulässigkeit liegt beim Auftraggeber.

5. Kategorien betroffener Personen

- Beschäftigte des Auftraggebers (Administratoren und sonstige berechtigte Nutzer)
- Externe Dienstleister des Auftraggebers, sofern ihnen Zugriffsrechte eingeräumt werden

6. Art der Verarbeitung

Erheben (Benutzer- und Organisationsdaten), Erfassen, Speichern, Auslesen, Abfragen, Verwenden (Benutzer- und Berechtigungsverwaltung), Verändern (Aktualisierung von Konten, Teams und Berechtigungen), Löschen (bei Offboarding, Beendigung der Beauftragung oder Entkopplung).

Bei Beauftragung des optionalen **On-Premise-Backups** kommt zusätzlich das **Übermitteln/Exportieren** hinzu: Die Organisations-Logins werden als verschlüsselte Datei auf einen Server des Auftraggebers exportiert (siehe Abschnitt 10).

7. Ort der Verarbeitung

Die Verarbeitung erfolgt ausschließlich in der Europäischen Union (Deutschland).

Standort	Anbieter	Zweck
Nürnberg (Deutschland)	heylogin GmbH (über Hetzner)	Produktivsystem der Passwortmanager-Plattform (Speicherung der verschlüsselten Tresore, Konto- und Organisationsdaten, Audit-Logs)
Falkenstein (Deutschland)	heylogin GmbH (über Hetzner)	Standby-/Failover-System
Frankfurt am Main (Deutschland)	heylogin GmbH (über IONOS)	Verschlüsselte Datensicherung (Backups)
Hannover (Deutschland)	EXT IT GmbH	Administration der Organisation als delegierter Administrator (Benutzer-, Team- und Berechtigungsverwaltung)

Bei Beauftragung des optionalen On-Premise-Backups erfolgt eine zusätzliche Verarbeitung am Standort des vom Auftraggeber bereitgestellten Servers (siehe Abschnitt 10).

8. Aufbewahrungsdauer / Löschfristen

Datenkategorie	Aufbewahrungsdauer	Löschverfahren
Konto- und Organisationsdaten (Benutzer, Teams, Berechtigungen)	Dauer der Beauftragung	Löschung bei Offboarding einzelner Nutzer bzw. bei Beendigung der Beauftragung; bei Entkopplung verbleiben die Daten in der dann unabhängigen Kundenorganisation
Verschlüsselte Tresor-Inhalte	Dauer der Beauftragung	Löschung mit dem jeweiligen Konto bzw. bei Beendigung; ein Klartext-Zugriff zur Löschung einzelner Inhalte durch den Auftragnehmer ist technisch ausgeschlossen (Ende-zu-Ende-Verschlüsselung)
Zugriffs- und Audit-Logs	gemäß Vorgabe der heylogin-Plattform	Automatische Rotation in der Plattform
Verschlüsselte Datenbank-Backups (heylogin)	rollierend (RPO 60 Minuten)	Automatisches Auslaufen der Backup-Stände gemäß heylogin-Backup-Logik

Nach Beendigung des Vertragsverhältnisses wird der administrative Zugriff von EXT IT entfernt. Auf Wunsch des Auftraggebers wird die Organisation in eine unabhängige Organisation umgewandelt (Fortführung durch den Auftraggeber) oder die

Organisation gelöscht. Etwaige beim Auftraggeber abgelegte On-Premise-Backup-Dateien unterliegen der Verfügungsgewalt des Auftraggebers.

9. Eingesetzte Unterauftragsverarbeiter

Für diesen Service werden die folgenden **produktspezifischen** Unterauftragsverarbeiter eingesetzt:

Nr.	Firma	Sitz	Verarbeitungszweck	Drittlandtransfer	Garantien
Z9	heylogin GmbH	Braunschweig, Deutschland (EU)	Zero-Knowledge-Passwortmanager-Plattform: Speicherung der verschlüsselten Tresore sowie der Konto-, Organisations- und Audit-Daten, Bereitstellung der Verwaltungs- und Synchronisationsfunktionen	Nein (EU)	Siehe Anlage 3
Z10	Hetzner Online GmbH	Gunzenhausen, Deutschland (EU); Rechenzentren Nürnberg und Falkenstein	Hosting des Produktiv- und Standby-Systems (Sub-Processor der heylogin GmbH)	Nein (EU)	Siehe Anlage 3
Z11	IONOS SE	Montabaur, Deutschland (EU); Rechenzentrum Frankfurt am Main	Hosting der verschlüsselten Datensicherung (Sub-Processor der heylogin GmbH)	Nein (EU)	Siehe Anlage 3

Die vollständigen DPA-Details, Zertifizierungen und Garantien zu den oben genannten Unterauftragsverarbeitern sind zentral in **Anlage 3** geführt. Die vollständige Unterauftragsverarbeiter-Liste der heylogin GmbH wird dem Auftraggeber auf Anfrage in ihrer jeweils aktuellen Fassung zur Verfügung gestellt.

Ergänzend kommen die in Abschnitt 3 der Anlage 3 gelisteten produktübergreifenden Unterauftragsverarbeiter zum Einsatz.

10. Besondere Hinweise

- **Zero-Knowledge-Architektur:** heylogin verschlüsselt die Tresor-Inhalte Ende-zu-Ende auf den Endgeräten der Nutzer (ohne Master-Passwort, gebunden an die Sicherheitschips der Geräte). Ein Klartext-Zugriff auf die gespeicherten Zugangsdaten ist weder durch heylogin noch durch den Auftragnehmer (auch nicht als delegierter Administrator) möglich. Die Verwaltung durch den Auftragnehmer beschränkt sich auf Konten, Teams und Berechtigungen. Geteilte Team-Tresore sind nur für die jeweils berechtigten Mitglieder auf deren Geräten entschlüsselbar.
- **Datenverlust bei fehlendem Wiederherstellungscode (Art. 17 / Verfügbarkeit):** Gehen alle Anmeldegeräte eines Nutzers verloren und liegt kein gültiger Backup-/Wiederherstellungscode vor, ist eine Wiederherstellung der betroffenen Zugangsdaten technisch ausgeschlossen -- auch durch den Auftragnehmer oder heylogin. Der Auftraggeber als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO stellt sicher, dass seine Nutzer Wiederherstellungscodes sicher verwahren und mindestens ein interner Administrator vorhanden ist. Eine Haftung des Auftragnehmers für einen derart bedingten Datenverlust ist im Rahmen des §7 AGB und des §12 des Rahmen-AVV ausgeschlossen.
- **Jederzeitige Entkopplung:** Der Auftraggeber kann den administrativen Zugriff des Auftragnehmers jederzeit entziehen (Entfernen der delegierten Administratoren und Umwandlung in eine unabhängige Organisation; Voraussetzung: mindestens ein interner Administrator). Der Auftragnehmer hat danach keinen administrativen Zugriff mehr auf die Organisation.
- **On-Premise-Backup (optional):** Bei Beauftragung exportiert eine Backup-Komponente die Organisations-Logins als verschlüsselte Datei (age-Verschlüsselung, `.csv.age`) auf einen vom Auftraggeber bereitgestellten Server. Hierbei verlassen die Daten die Zero-Knowledge-Sphäre als auf dem Kundenserver entschlüsselbarer Export. Verantwortung für den Backup-Server, die Schlüsselverwahrung und die Absicherung des Service-Zugangs liegen beim Auftraggeber; die konkrete Ausgestaltung wird im Einzelauftrag vereinbart.
- **Breach-Meldung:** heylogin meldet dem Auftragnehmer Verletzungen des Schutzes personenbezogener Daten gemäß den Bestimmungen des heylogin-Datenverarbeitungsvertrags; der Auftragnehmer informiert den Auftraggeber unverzüglich gemäß §7 des Rahmen-AVV.
- **Zertifizierung:** heylogin GmbH ist nach ISO 27001 zertifiziert; die Rechenzentren der eingesetzten Unterauftragsverarbeiter sind ebenfalls ISO-27001-zertifiziert.

Änderungshistorie

Version	Datum	Änderung	Verantwortlich
1.0	2026-06-01	Erstveröffentlichung	Geschäftsführung

Stand: 2026-06-01