Projekt 29
Datenschutz | Informationssicherheit

member of
P29 GROUP

TESTAT

Gegenstand der Prüfung: Datenschutzrechtliche Einordnung des Enterprise-Password-Managers „heylogin“ durch die Projekt 29 GmbH & Co. KG (Externer Datenschutzbeauftragter der heylogin GmbH) insbesondere bzgl. Privacy by Design.

Zielgruppe: Datenschutzbeauftragte (DSB), CISO, Betriebsräte und IT-Einkauf

heylogin

heylogin GmbH
Sophienstraße 40
38118 Braunschweig

Als bestellter externer Datenschutzbeauftragter der heylogin GmbH bestätigen wir, die Projekt 29 GmbH & Co. KG, dass die Enterprise-Password-Management-Lösung „heylogin“ für den Einsatz in hochregulierten Umfeldern (DSGVO-Raum, KRITIS, Berufsgeheimnisträger) geeignet ist.

Unsere Prüfung der technischen und organisatorischen Maßnahmen sowie der Rechtsgrundlagen kommt zu folgendem Ergebnis:

- Datensouveränität: Die Verarbeitung sensibler Inhaltsdaten (Passwörter) erfolgt ausschließlich in Deutschland.
- Hohes Schutzniveau: Die heylogin GmbH ist nach ISO/IEC 27001:2022 zertifiziert (TÜV Rheinland, ID: 9000032416).
- Rechtskonformität: Die Lösung ermöglicht einen DSGVO-konformen Einsatz. Ein geprüfter Auftragsverarbeitungsvertrag (AVV/DPA) liegt vor.

Regensburg, 14.01.2026

Nico Becker, externer Datenschutzbeauftragter
Projekt 29 GmbH & Co. KG

Projekt 29 Datenschutz | Informationssicherheit — member of P29 GROUP

PRIVACY BY DESIGN

GEPRÜFTE DATENSCHUTZ-ARCHITEKTUR

Ausgestellt 2026

P29 geprüft

BEWERTUNG

1. Bewertung der Sicherheitsarchitektur (Privacy by Design)

Die Systemarchitektur setzt nach unserer Bewertung die Anforderungen an „Privacy by Design“ (Art. 25 DSGVO) und die Sicherheit der Verarbeitung (Art. 32 DSGVO) durch eine technische Zugriffsbeschränkung effektiv um.

1.1 Zero-Knowledge & End-to-End-Verschlüsselung

heylogin realisiert ein technisches Zero-Knowledge-Prinzip.

- Befund: Der Anbieter (heylogin GmbH) besitzt technisch keine Möglichkeit, auf die gespeicherten Inhaltsdaten der Kunden zuzugreifen. Die Server fungieren lediglich als Synchronisations-Relay für verschlüsselte Datenpakete.
- Kryptografie: Die Verschlüsselung erfolgt client-seitig auf den Endgeräten. Zum Einsatz kommen moderne Verfahren (XSalsa20, Poly1305, Curve25519), die dem aktuellen Stand der Technik entsprechen.

1.2 Hardware-basierte Sicherheit

Der Verzicht auf ein Master-Passwort wird durch eine Hardware-Bindung kompensiert, die das Risiko klassischer Angriffsvektoren (Phishing, Brute-Force) minimiert.

- Sicherheitsanker: Der kryptografische Seed wird im Sicherheitschip (Secure Enclave/TPM) des Endgeräts generiert und verlässt diesen nie unverschlüsselt.
- 2-Faktor-Zwang: Jede Entschlüsselung erfordert zwingend den Faktor Besitz (Gerät) und den Faktor Wissen/Sein (PIN/Biometrie).
- Lokale Verarbeitung von Biometrie/PIN: Wir bestätigen explizit, dass biometrische Merkmale (Fingerabdruck, FaceID) oder Geräte-PINs ausschließlich lokal auf dem Endgerät verarbeitet werden, um den Sicherheitschip freizuschalten. Diese sensiblen Daten werden zu keinem Zeitpunkt an die heylogin-Server übertragen oder dort verarbeitet. Der Anbieter erhält lediglich das kryptografische Resultat der Freigabe ("Token"), jedoch niemals die biometrischen Rohdaten.

BEWERTUNG

1.3 App-Datenschutz & Drittanbieter-Module

Ein häufiges Risiko bei mobilen Anwendungen ist der unbemerkte Datenabfluss durch Analyse-Frameworks (SDKs).

- Tracker-Freiheit: Wir bestätigen, dass die heylogin Mobile-Apps (iOS/Android) frei von Trackern zu Werbezwecken oder übergreifendem Profiling sind. Es werden keine Nutzungsdaten an Dritte (wie Facebook, Google Ads) übermittelt.
- Crash-Reporting: Soweit technische Crash-Reports zur Fehlerbehebung notwendig sind, erfolgen diese pseudonymisiert, opt-in-basiert und streng zweckgebunden.
- Berechtigungen: Die Apps fordern nur die technisch zwingend notwendigen Berechtigungen (Kamera für QR-Login, Biometrie für Entsperrung) an.

1.4 Übersicht der technisch-organisatorischen Maßnahmen (TOMs)

Die detaillierten Maßnahmen gemäß Art. 32 DSGVO sind als Anlage zum Auftragsverarbeitungsvertrag (AVV) dokumentiert. Zusammenfassend werden folgende Schutzkategorien gewährleistet:

- Zutrittskontrolle: Physische Sicherheit durch ISO-27001 zertifizierte Rechenzentren mit biometrischen Zutrittssystemen und 24/7-Überwachung.
- Zugangskontrolle: Absicherung interner Systeme durch Hardware-Security-Keys und striktes "Need-to-Know"-Prinzip für Mitarbeiter.
- Zugriffskontrolle: Kryptografisch erzwungene Unmöglichkeit des Datenzugriffs auf Inhaltsdaten durch den Anbieter (Zero-Knowledge).
- Weitergabekontrolle: Verschlüsselte Übertragungswege (TLS 1.2+) und Verzicht auf unverschlüsselte Backups.
- Trennungsgebot: Logische Mandantentrennung sowie strikte Trennung von Produktions- und Testumgebungen.

BEWERTUNG

1.5 Maßnahmen für mobiles Arbeiten / Homeoffice (Interne Regelung)

Die heylogin GmbH hat für ihre Mitarbeiter spezifische Sicherheitsvorgaben für mobiles Arbeiten und Homeoffice im Rahmen des ISO 27001 ISMS implementiert, um die Sicherheit der verarbeiteten Daten jederzeit zu gewährleisten:

- Gerätesicherheit: Alle firmeneigenen Endgeräte der Mitarbeiter sind verpflichtend mit Full-Disk-Encryption (Festplattenverschlüsselung) gesichert und unterliegen einem zentralen Patch-Management.
- Zugriffsschutz: Der Zugriff auf Arbeitsgeräte ist durch starke Passwörter gemäß der internen Passwortrichtlinie gesichert. Bei Verlassen des Arbeitsplatzes greifen automatische Bildschirmsperren.
- Datenminimierung: Mobiles Arbeiten beschränkt sich auf den Zugriff auf notwendige Metadaten (z.B. für Support-Zwecke). Auf die End-to-End verschlüsselten Inhaltsdaten der Kunden haben Mitarbeiter auch im Homeoffice technisch keinen Zugriff.
- Richtlinien: Es gelten verbindliche "Clean Desk"-Policies sowie vertragliche Verpflichtungen zur Einhaltung der Informationssicherheit im häuslichen Umfeld.

BEWERTUNG

2. Infrastruktur & Datentransfers

2.1 Sub-Dienstleister & Hosting

Unsere Prüfung der Unterauftragnehmer bestätigt eine auf Datensouveränität ausgerichtete Lieferkette. Für den Kern-Service (Speicherung der Passwort-Vaults) werden keine US-Hyperscaler eingesetzt. Geprüfte Hosting-Umgebung:

- Standort: Physisches Hosting und Backups der Inhaltsdaten befinden sich in Deutschland.
- Qualität: Die beauftragten Rechenzentren (aktuell u.a. Hetzner Online GmbH, IONOS SE) sind nach ISO/IEC 27001 zertifiziert.
- Transparenz: Die Liste der Sub-Dienstleister ist öffentlich dokumentiert.

2.2 Bewertung Drittlandtransfers (Schrems II)

- Kern-Produkt: Es findet keine Übermittlung der verschlüsselten Passwort-Vaults in Drittländer statt.
- Risikoeinschätzung Cloud Act: Aufgrund der Zero-Knowledge-Architektur wären herausgegebene Daten für Dritte (inkl. ausländischer Behörden) unlesbar. Dies bewerten wir als wirksame technische Maßnahme ("Supplementary Measure") im Sinne der Schrems-II-Rechtsprechung des EuGH.
- Optionale Dienste: Soweit US-Dienstleister für kaufmännische Prozesse (z.B. Billing) eingesetzt werden, sind diese durch Angemessenheitsbeschlüsse (EU-US Data Privacy Framework) oder Standardvertragsklauseln abgesichert.

BEWERTUNG

3. Verfügbarkeit & Business Continuity

Die Maßnahmen zur Sicherstellung der Verfügbarkeit (Art. 32 Abs. 1 lit. b DSGVO) wurden als angemessen bewertet:

- Redundanz: Physische Trennung von Produktions- und Backup-Systemen an verschiedenen Standorten in Deutschland.
- Wiederherstellung: Definierte RTO (< 2 Stunden) und RPO (60 Minuten) gewährleisten die Betriebskontinuität.
- Offline-Fähigkeit: Durch lokalen Cache in den Clients ist die Arbeitsfähigkeit auch bei Server-Störungen gegeben.

Incident Management & Meldeprozesse (Art. 33 DSGVO): Die heylogin GmbH unterhält einen definierten Prozess zur Behandlung von Sicherheitsvorfällen.

- Reaktionszeit: Das Security-Team überwacht die Infrastruktur 24/7. Im Falle einer festgestellten Verletzung des Schutzes personenbezogener Daten informieren wir die betroffenen Kunden unverzüglich (in der Regel < 24 Stunden nach Bekanntwerden), um ihnen die Einhaltung der gesetzlichen Meldefristen (72 Stunden gem. Art. 33 DSGVO) zu ermöglichen.
- Support: Im Ernstfall werden alle notwendigen Informationen zur Risikoabwägung und Dokumentation bereitgestellt.

BEWERTUNG

4. Betriebsrat & Beschäftigtendatenschutz

Aus Sicht des Beschäftigtendatenschutzes (§ 26 BDSG) und der Mitbestimmung bewerten wir die Lösung wie folgt:

4.1 Keine Leistungs- und Verhaltenskontrolle

Die Protokollierung (Audit Logs) dient ausschließlich der IT-Sicherheit und Compliance.

- Zweckbindung: Eine Nutzung zur Leistungs- oder Verhaltenskontrolle ist vertraglich ausgeschlossen.
- Datenminimierung: Es werden nur technisch notwendige Metadaten erfasst.

4.2 Eingeschränkte Admin-Sicht auf persönliche Firmen-Logins

Auch bei personalisierten Accounts, die eindeutig einem Mitarbeiter zugeordnet sind und zur Organisation gehören ("Persönlicher Tresor"), greifen Schutzmechanismen:

- Sichtbarkeit: Administratoren können aus Compliance-Gründen einsehen, welche Logins existieren und ob diese den Sicherheitsrichtlinien (z.B. Passwortstärke) entsprechen.
- Schutz der Inhaltsdaten: Administratoren können jedoch technisch nicht die Passwörter selbst im Klartext anzeigen. Passwörter werden systemseitig als besonders schützenswerte persönliche Daten behandelt, auch innerhalb des geschäftlichen Kontextes.

4.3 Strikte Trennung zum Privaten Account ("Private Vault")

Zusätzlich zur Organisationsebene ermöglicht die Architektur die Nutzung eines komplett privaten Bereichs.

- Schutz der Privatsphäre: Administratoren und Vorgesetzte haben technisch keinen Zugriff und keine Einsicht (auch keine Metadaten) auf den Tresor des privaten Accounts ("Private Vault") eines Mitarbeiters. Dies schützt die Privatsphäre der Beschäftigten auch bei Nutzung der App auf Firmengeräten effektiv.