Projekt 29
Datenschutz | Informationssicherheit

member of
P29 GROUP

REVIEW

Subject of the audit: Data protection classification of the enterprise password manager ‘heylogin’ by Projekt 29 GmbH & Co. KG (external data protection officer of heylogin GmbH), in particular with regard to privacy by design.
Target group: Data protection officers (DPOs), CISOs, works councils and IT purchasing departments

heylogin

heylogin GmbH
Sophienstraße 40
38118 Braunschweig

As the appointed external data protection officer for heylogin GmbH, the Projekt 29 GmbH & Co. KG confirms that the enterprise password management solution ‘heylogin’ is suitable for use in highly regulated environments (GDPR area, KRITIS, professional secrecy).
Our review of the technical and organisational measures as well as the legal basis has come to the following conclusion:

- Data sovereignty: The processing of sensitive content data (passwords) takes place exclusively in Germany.
- High level of protection: heylogin GmbH is certified according to ISO/IEC 27001:2022 (TÜV Rheinland, ID: 9000032416).
- Legal compliance: The solution enables GDPR-compliant use. A certified data processing agreement (DPA) is available.

Regensburg, 14.01.2026

Nico Becker, external Data Protection Officer
Projekt 29 GmbH & Co. KG

Projekt 29
Datenschutz | Informationssicherheit
member of P29 GROUP
PRIVACY BY DESIGN
VERIFIED
DATA PROTECTION
issued 2026
P29
verified

ASSESSMENT

1. Assessment of the security architecture (privacy by design)

According to our assessment, the system architecture effectively implements the requirements for privacy by design (Art. 25 GDPR) and security of processing (Art. 32 GDPR) through technical access restrictions.

1.1 Zero-knowledge & end-to-end encryption

heylogin implements a technical zero-knowledge principle.

- Finding: The provider (heylogin GmbH) has no technical means of accessing the stored content data of its customers. The servers merely act as a synchronisation relay for encrypted data packets.
- Cryptography: Encryption takes place on the client side on the end devices. Modern methods (XSalsa20, Poly1305, Curve25519) are used, which correspond to the current state of the art.

1.2 Hardware-based security

The absence of a master password is compensated for by a hardware binding that minimises the risk of classic attack vectors (phishing, brute force).

- Security anchor: The cryptographic seed is generated in the security chip (Secure Enclave/TPM) of the end device and never leaves it unencrypted.
- 2-factor compulsion: Every decryption requires the possession factor (device) and the knowledge/being factor (PIN/biometrics).
- Local processing of biometrics/PIN: We explicitly confirm that biometric features (fingerprint, FaceID) or device PINs are processed exclusively locally on the end device in order to activate the security chip. This sensitive data is never transferred to the heylogin servers or processed there. The provider only receives the cryptographic result of the release ('token'), but never the raw biometric data.

ASSESSMENT

1.3 App data protection & third-party modules

A common risk with mobile applications is the unnoticed data leakage through analysis frameworks (SDKs).

- Tracker freedom: We confirm that the heylogin mobile apps (iOS/Android) are free of trackers for advertising purposes or comprehensive profiling. No usage data is transmitted to third parties (such as Facebook or Google Ads).
- Crash reporting: Where technical crash reports are necessary for troubleshooting, these are pseudonymised, opt-in-based and strictly purpose-bound.
- Permissions: The apps only request the permissions that are technically necessary (camera for QR login, biometrics for unlocking).

1.4 Overview of technical and organisational measures (TOMs)

The detailed measures in accordance with Art. 32 GDPR are documented as an appendix to the data processing agreement (DPA). In summary, the following protection categories are guaranteed:

- Access control: Physical security through ISO 27001-certified data centres with biometric access systems and 24/7 monitoring.
- Access control: Securing internal systems through hardware security keys and a strict 'need-to-know' principle for employees.
- Access control: Cryptographically enforced impossibility of data access to content data by the provider (zero knowledge).
- Transfer control: Encrypted transmission channels (TLS 1.2+) and no unencrypted backups.
- Separation requirement: Logical client separation and strict separation of production and test environments.

ASSESSMENT

1.5 Measures for mobile working/home office (internal regulation)

heylogin GmbH has implemented specific security requirements for mobile working and home office for its employees within the framework of ISO 27001 ISMS in order to ensure the security of the data processed at all times:

- Device security: All company-owned end devices used by employees are required to be secured with full disk encryption and are subject to centralised patch management.
- Access protection: Access to work devices is secured by strong passwords in accordance with the internal password policy. Automatic screen locks are activated when the workstation is left unattended.
- Data minimisation: Mobile working is limited to access to necessary metadata (e.g. for support purposes). Employees do not have technical access to customers' end-to-end encrypted content data, even when working from home.
- Guidelines: Binding ‘clean desk’ policies and contractual obligations to maintain information security in the home environment apply.

ASSESSMENT

2. Infrastructure & Data Transfers

2.1 Sub-Service Providers & Hosting

Our audit of subcontractors confirms a supply chain focused on data sovereignty. No US hyperscalers are used for the core service (storage of password vaults). Audited hosting environment:

- Location: Physical hosting and backups of content data are located in Germany.
- Quality: The contracted data centres (currently including Hetzner Online GmbH and IONOS SE) are ISO/IEC 27001 certified.
- Transparency: The list of sub-service providers is publicly documented.

2.2 Assessment of third country transfers (Schrems II)

- Core product: Encrypted password vaults are not transferred to third countries.
- Risk assessment Cloud Act: Due to the zero-knowledge architecture, any data disclosed would be unreadable to third parties (including foreign authorities). We consider this to be an effective technical measure ('Supplementary Measure') within the meaning of the Schrems II ruling of the ECJ.
- Optional services: Where US service providers are used for commercial processes (e.g. billing), these are secured by adequacy decisions (EU-US Data Privacy Framework) or standard contractual clauses.

BEWERTUNG

3. Availability & Business Continuity

The measures to ensure availability (Art. 32(1)(b) GDPR) were assessed as adequate:

- Redundancy: Physical separation of production and backup systems at different locations in Germany.
- Recovery: Defined RTO (< 2 hours) and RPO (60 minutes) ensure business continuity.
- Offline capability: Local cache in the clients ensures that work can continue even in the event of server failures.

Incident management & reporting processes (Art. 33 GDPR): heylogin GmbH maintains a defined process for handling security incidents.

- Response time: The security team monitors the infrastructure 24/7. In the event of a detected breach of personal data protection, we inform the affected customers immediately (usually < 24 hours after becoming aware of it) to enable them to comply with the statutory reporting deadlines (72 hours according to Art. 33 GDPR).
- Support: In an emergency, all necessary information for risk assessment and documentation is provided.

ASSESSMENT

4. Works council & employee data protection

From the perspective of employee data protection and co-determination, we assess the solution as follows:

4.1 No performance and behaviour monitoring

The audit logs are used exclusively for IT security and compliance purposes.

- Purpose limitation: Use for performance or behaviour monitoring is contractually excluded.
- Data minimisation: Only technically necessary metadata is collected.

4.2 Restricted admin view of personal company logins

Protective mechanisms also apply to personalised accounts that are clearly assigned to an employee and belong to the organisation ('personal vault'):

- Visibility: For compliance reasons, administrators can see which logins exist and whether they comply with security guidelines (e.g. password strength).
- Protection of content data: However, administrators cannot technically display the passwords themselves in plain text. Passwords are treated by the system as particularly sensitive personal data, even within a business context.

4.3 Strict separation from private accounts ('Private Vault')

In addition to the organisational level, the architecture allows the use of a completely private area.

- Privacy protection: Administrators and supervisors have no technical access to or insight into (including metadata) the vault of an employee's private account ('Private Vault'). This effectively protects the privacy of employees even when using the app on company devices.