heylogin

heylogin is Cybersecurity Made In Europe

How heylogin earned the European cybersecurity quality label, and how our product meets the ENISA baseline security requirements

heylogin GmbH

Public | 2026-10-06

Contents

1 The label **3**

2 What the label requires **4**

3 The ENISA baseline security requirements **4**

1. Security by Design . . . 5
2. Least Privilege . . . 6
3. Strong Authentication . . . 7
4. Asset Protection . . . 7
5. Supply Chain Security . . . 8
6. Documentation Transparency . . . 8
7. Quality Management . . . 9
8. Service Continuity . . . 9
9. EU Jurisdiction . . . 10
10. Data Usage Restriction . . . 10

CYBERSECURITY MADE IN EUROPE

Date of Issue:
01 – 10 – 2026

CERTIFICATE

eurobits e.V. - European Competence Centre for Information Technology Security approves that:

heylogin GmbH
Sophienstr. 40
38118 Braunschweig
GERMANY

heylogin

IS ENTITLED TO CARRY THE LABEL

'CYBERSECURITY MADE IN EUROPE'

Issuance Number: DE-EBS-2026-10-0081

Certificate Valid Until:
30 – 09 – 2027

Approved Signature:

Issuer:
eurobits

Figure 1: Cybersecurity Made In Europe certificate

1 The label

heylogin has been awarded the **Cybersecurity Made In Europe** label. The label is a European quality mark operated by the European Cyber Security Organisation (ECSO) and issued through a network of qualified national partners. It is designed to promote European cybersecurity companies and to give customers a clear, recognisable signal of European origin and trustworthy security practice.

Figure 2: heylogin is Cybersecurity Made In Europe

Beyond carrying the label, heylogin is itself a member of ECSO, the non-profit organisation that unites European cybersecurity stakeholders and works to strengthen Europe's cybersecurity ecosystem and technological independence. Our membership reflects an active commitment to the European cybersecurity community, not merely compliance with a checklist.

Figure 3: heylogin is member of the European Cyber Security Organisation (ECSO)

The label is granted to companies that declare conformity with a defined set of criteria, verified by a qualified issuing partner, and it is valid for twelve months, after which it is renewed. heylogin received the label through eurobits e.V., the European Competence Centre for Information Technology Security and the qualified German issuing partner of the scheme. For heylogin, the label expresses in a single mark what we ask customers and procurement teams to trust us on: that we are a genuinely European company that has declared conformity of its product with a recognised European security baseline.

2 What the label requires

To carry the Cybersecurity Made In Europe label, a company must satisfy criteria covering both who we are and how our product is built. In summary, a labelled company:

- is headquartered in Europe (EU27, EFTA, EEA or the UK), and where part of a group, the group headquarters are in Europe;
- has no major ownership or control from outside Europe;
- has Europe as its primary place of business, with more than half of its cybersecurity research and development activity and staff located in Europe;
- provides trustworthy cybersecurity solutions as defined by the European Union Agency for Cybersecurity (ENISA) in its *Indispensable baseline security requirements for the procurement of secure ICT products and services*; and
- respects European data and privacy requirements as defined by the GDPR.

heylogin meets each of these criteria. We are a German company based in Braunschweig, controlled within Europe, with our entire team and all product development located in Germany. Mozilla Ventures holds a minority, non-controlling stake in heylogin; as the investment arm of the Mozilla Foundation, it shares our vision of a free and open internet, and its involvement does not constitute major ownership or control from outside Europe. Our service runs exclusively from European, ISO/IEC 27001-certified data centres, and we process personal data strictly under the GDPR.

The remainder of this whitepaper focuses on the product criterion in detail: how heylogin meets each of the ten ENISA baseline security requirements that form the technical heart of the label.

3 The ENISA baseline security requirements

ENISA is the European Union Agency for Cybersecurity. Established in 2004 and given a permanent mandate by the EU Cybersecurity Act in 2019, it supports EU institutions and Member States in achieving a high common level of cybersecurity across Europe, among other things by publishing guidance and developing European cybersecurity certification schemes. The ENISA baseline is a technologically neutral set of minimum requirements built on the principles of secure by design, secure by default, least privilege, and verifiability. The original document is available at:

https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services

For each of the ten principles we restate the requirement, then explain how heylogin fulfils it, addressing the detailed sub-points from Section 3 of the original document where they apply. Where a sub-point does not map directly onto a zero-knowledge password manager, we say so and describe the equivalent control. Throughout, "we", "our" and "us" refer to heylogin GmbH as the provider. Functional details are documented in our Help Center at https://help.heylogin.com; security and architecture details are documented in our Security Whitepaper and Compliance Whitepaper, available through our Trust Center at https://www.heylogin.com/en/trust-center.

The table below summarises our conformity with the ten ENISA baseline principles.

ENISA principle	Fulfilled
Security by Design	Yes
Least Privilege	Yes
Strong Authentication	Yes
Asset Protection	Yes
Supply Chain Security	Yes
Documentation Transparency	Yes
Quality Management	Yes
Service Continuity	Yes
EU Jurisdiction	Yes
Data Usage Restriction	Yes

1. Security by Design

Requirement. The provider shall design and pre-configure the delivered product such that functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations.

heylogin is built around a zero-knowledge architecture. All content data (login titles, usernames, websites, team names, passwords, TOTP secrets and custom fields) is encrypted end-to-end on the client device. Our servers act only as a synchronisation relay for already-encrypted data

packets and cannot decrypt them. Encryption relies on well-established, state-of-the-art cryptographic methods and established cryptographic libraries rather than proprietary schemes.

Instead of a master password, heylogin binds access to the hardware security chip (Secure Enclave / TPM) of the user's device by default. This default configuration reduces the attack surface to the necessary minimum and removes brute-force attacks against a master password by design.

In detail: heylogin ships without unnecessary functionality, and the client contains no undocumented data-forwarding or backdoors. Security-relevant administrative and access events are recorded in an organization audit log that administrators can review. We do not rely on outdated or insecure protocols. The product and its dependencies are kept ready to mitigate known vulnerabilities through continuous automated dependency and vulnerability scanning.

2. Least Privilege

Requirement. The provider shall design and pre-configure the product according to the least privilege principle, whereby administrative rights are only used when absolutely necessary, sessions are technically separated and all accounts will be manageable.

Access in heylogin is distributed deliberately and granularly. A login is only visible and decryptable to the individuals or teams it has been explicitly shared with, because sharing is enforced cryptographically on a per-user and per-device basis. Within an organization, administrators manage access through roles and targeted login sharing, so each user receives only the credentials required for their work.

In detail: administrators manage all organization users and their access independently, without requiring our involvement, through the management interface. Every user has their own individual account bound to their own devices; accounts are not shared. Administrative functions are separated from ordinary user functions and restricted to admin roles, and sensitive operations such as unlocking a paired device, pairing another device or showing the backup code require local re-authentication on the device's security chip (PIN or biometrics), independent of the phone's screen unlock, which technically separates them from a general unlocked session. For credentials stored in heylogin, organizations can enforce a password policy, and stored passwords remain fully under the operator's control and can be changed at any time. Because heylogin replaces a memorized master password with hardware-bound authentication, classic master-password complexity rules do not map onto the unlock mechanism itself; the equivalent protection is delivered by the device security chip and its enforced brute-force limits.

3. Strong Authentication

Requirement. The product shall provide and support strong authentication mechanisms for all accounts. If authentication is unsuccessful the product shall not allow any user specific activities to be performed.

Every unlock and decryption in heylogin requires two factors: the possession factor (a registered device with a security chip) and the knowledge/inherence factor (PIN or biometrics). Biometrics and PINs are processed exclusively on the local device and are never transmitted to heylogin; the server only ever receives the cryptographic result of the release, never the raw data.

In detail: supported login devices include smartphone security chips (iOS/Android), Windows Hello, Touch ID, and FIDO2 security keys. Brute-force protection is enforced by the platforms' security chips (escalating timeouts or device lockout on iOS/Android, an 8-attempt limit on FIDO2 keys). Access to data is only granted after successful authentication; an unsuccessful authentication grants no access and allows no user-specific activity.

4. Asset Protection

Requirement. The product shall provide adequate level of protection for critical information assets during storage and transmission.

Critical logical assets in heylogin are protected continuously. All content data (login titles, usernames, websites, team names, passwords, TOTP secrets and custom fields) is end-to-end encrypted and can only be decrypted on the user's paired devices. Only operational metadata required to run the service, such as organization names and account emails, is not end-to-end encrypted. All data is additionally protected in transit by TLS. Server backups receive an additional layer of encryption at rest, so that no access is possible even if backup storage were compromised. Cryptographic keys never leave the device's security chip in clear text.

In detail: sensitive data such as credentials is stored and transmitted only in encrypted form. We use only established, well-known encryption algorithms and key lengths considered safe according to the state of the art, implemented on top of established cryptographic libraries to avoid implementation weaknesses; no proprietary encryption algorithms are used. Key generation produces secure keys, and keys are stored securely within the device security chip.

5. Supply Chain Security

Requirement. The provider shall give means to ensure that the product is genuine, cannot be tainted during operation, and its integrity is warranted throughout the product's lifecycle.

heylogin is distributed through the official platform stores (App Store, Google Play, browser web stores) and signed distribution channels, which establish the authenticity and integrity of the software for the user and allow components to be traced back to their genuine source. Because the product encrypts purely on the client side, the operator of the service cannot access or tamper with content at any point server-side.

In detail: integrity and dependency requirements are verified through automated checks across the build, and as required by our internal Secure Development Policy, every significant change passes a mandatory code review by a second developer plus an automated CI pipeline before release. Ongoing automated dependency and vulnerability scanning detects issues across the lifecycle. The supporting infrastructure is provided exclusively by ISO/IEC 27001-certified subprocessors located in Europe.

6. Documentation Transparency

Requirement. The provider shall offer comprehensive and understandable documentation about the overall design of the product, describing its architecture, functionalities and protocols, their realisation in hardware or software components, and the interfaces and interactions of components, in order to implement and use the product in the most secure way possible.

We provide comprehensive, understandable documentation through our Trust Center at https://www.heylogin.com/en/trust-center: a detailed Security Whitepaper (architecture, cryptographic design, supported devices and protocols, and a documented threat model including its limits), a Compliance Whitepaper, the data processing agreement, the Technical and Organizational Measures, and a public subprocessor list. Functional and usage documentation for all features is publicly available at https://www.heylogin.com and in the Help Center at https://help.heylogin.com.

In detail: documentation is hosted and updated through our own channels and does not depend on permanent references to external servers, it is updated when there are major changes to design or functionality, and users are made aware of relevant changes through our release notes.

7. Quality Management

Requirement. The provider shall be able to provide evidence that a managed security-by-design approach has been adopted, including documented secure software development, quality management and information security management processes.

heylogin GmbH is certified to ISO/IEC 27001:2022 (TÜV Rheinland) and operates a correspondingly certified information security management system. Our development process, defined in our internal Secure Development Policy, includes a binding definition of done, code review by a second developer, automated testing and a CI pipeline, and continuous automated vulnerability scanning of dependencies. Security-relevant changes are reviewed to preserve the end-to-end cryptographic properties of the product. The product has additionally been tested by an external penetration-testing auditor, secuvera GmbH; the report is available through our Trust Center at https://www.heylogin.com/en/trust-center.

In detail: our valid ISO/IEC 27001 certification covers the relevant area, evidence of how requirements are met is available through that certification and our Trust Center documentation, and the ISMS scope and Statement of Applicability are covered by the certificate.

8. Service Continuity

Requirement. The provider shall guarantee support throughout the agreed lifetime of the product such that the system can work as agreed and is secure.

heylogin runs as a SaaS from German, ISO/IEC 27001-certified data centres with standby systems, supported by encrypted backups, monitoring and alerting to keep the service running. In the event of a lost device, the product offers established backup and recovery methods as well as administrator-assisted recovery of organization users, so that access can be continued securely. Support is provided through the agreed channels throughout the entire contract term; operational figures (availability, recovery objectives, response times) are set out in our Compliance Whitepaper and Terms and Conditions.

In detail: we continuously scan our codebase and infrastructure for vulnerabilities and operate a vulnerability disclosure policy, published at https://www.heylogin.com/security. Reported and newly known vulnerabilities are assessed and remediated under our internal Security Incident Management Procedure.

9. EU Jurisdiction

Requirement. The provider shall accept that all contracts refer to EU Member State law and only EU Member State law and a place of jurisdiction in an EU Member State, including those with subcontractors.

heylogin GmbH is a German company based in Braunschweig. Contracts are governed by German law (an EU Member State) with the place of jurisdiction in Germany. The entire core infrastructure and all subprocessors used for content data are located in Europe; no US hyperscalers are used for the core service. Data processing takes place exclusively in Germany, the EU or the EEA (see the data processing agreement), and engaged subprocessors are contractually bound by the same data protection obligations.

In detail: heylogin is not subject to non-EU legal regimes that would compel access to operator data, and the applicable law is set out in our Terms and Conditions and the data processing agreement.

10. Data Usage Restriction

Requirement. The provider shall explicitly declare, justify and document, context and purpose wise, all data collection and processing activities that take or may take place, including the relevant legal obligations stipulating them.

All data collection and processing is declared and justified by purpose and context in our privacy policy, the data processing agreement, and the public subprocessor list, including the respective legal bases under the GDPR. Because of the product's zero-knowledge architecture, heylogin GmbH has no technical access to stored content data (login titles, usernames, websites, passwords, TOTP secrets and custom fields). Processing on behalf of the customer takes place exclusively on the documented instructions of the controller on the basis of an Article 28 GDPR-compliant data processing agreement.

In detail: the place of processing and any third-country transfer are documented for each subprocessor in our public subprocessor list.