



heylogin ist Cybersecurity Made In Europe

Wie heylogin das europäische
Cybersicherheits-Qualitätslabel erhalten hat und wie unser
Produkt die ENISA-Basisanforderungen erfüllt

heylogin GmbH

06.10.2026

Inhaltsverzeichnis

1	Das Label	3
2	Was das Label voraussetzt	4
3	Die ENISA-Basissicherheitsanforderungen	5
1.	Security by Design	6
2.	Least Privilege	6
3.	Strong Authentication	7
4.	Asset Protection	8
5.	Supply Chain Security	8
6.	Documentation Transparency	9
7.	Quality Management	9
8.	Service Continuity	10
9.	EU Jurisdiction	10
10.	Data Usage Restriction	11



Abbildung 1: Zertifikat Cybersecurity Made In Europe

1 Das Label

heylogin wurde mit dem Label **Cybersecurity Made In Europe** ausgezeichnet. Das Label ist ein europäisches Qualitätszeichen, das von der European Cyber Security Organisation (ECSO) betrieben und über ein Netzwerk qualifizierter nationaler Partner vergeben wird. Es soll europäische Cybersicherheitsunternehmen fördern und Kunden ein klares, wiedererkennbares Signal für europäische Herkunft und vertrauenswürdige Sicherheitspraxis geben.



Initiated by ECSO. Issued by eurobits e.V.

Abbildung 2: heylogin ist Cybersecurity Made In Europe

Über das Label hinaus ist heylogin selbst Mitglied der ECSO, der gemeinnützigen Organisation, die europäische Akteure der Cybersicherheit vereint und sich für die Stärkung des europäischen Cybersicherheits-Ökosystems und der technologischen Unabhängigkeit Europas einsetzt. Unsere Mitgliedschaft steht für ein aktives Engagement in der europäischen Cybersicherheits-Community, nicht nur für das Abhaken einer Checkliste.



Abbildung 3: heylogin ist Mitglied der European Cyber Security Organisation (ECSO)

Das Label wird Unternehmen verliehen, die ihre Konformität mit einem definierten Kriterienkatalog erklären, was von einem qualifizierten Vergabepartner geprüft wird. Es ist zwölf Monate gültig und wird danach erneuert. heylogin hat das Label über eurobits e.V. erhalten, das Europäische Kompetenzzentrum für Sicherheit in der Informationstechnologie und den qualifizierten deutschen Vergabepartner des Programms. Für heylogin fasst das Label in einem Zeichen zusammen, worauf Kunden und Einkaufsabteilungen bei uns vertrauen sollen: dass wir ein echtes

europäisches Unternehmen sind, das die Konformität seines Produkts mit einer anerkannten europäischen Sicherheits-Baseline erklärt hat.

2 Was das Label voraussetzt

Um das Label Cybersecurity Made In Europe zu tragen, muss ein Unternehmen Kriterien erfüllen, die sowohl das Unternehmen selbst als auch die Entwicklung seines Produkts betreffen. Zusammengefasst gilt für ein ausgezeichnetes Unternehmen:

- Es hat seinen Hauptsitz in Europa (EU27, EFTA, EWR oder Vereinigtes Königreich); gehört es zu einer Unternehmensgruppe, liegt auch der Hauptsitz der Gruppe in Europa;
- es unterliegt keiner wesentlichen Beteiligung oder Kontrolle von außerhalb Europas;
- Europa ist sein Hauptgeschäftsort, und mehr als die Hälfte seiner Forschungs- und Entwicklungsaktivitäten und seines Personals im Bereich Cybersicherheit befindet sich in Europa;
- es bietet vertrauenswürdige Cybersicherheitslösungen im Sinne der Publikation *Indispensable baseline security requirements for the procurement of secure ICT products and services* der Agentur der Europäischen Union für Cybersicherheit (ENISA); und
- es hält die europäischen Datenschutzanforderungen gemäß DSGVO ein.

heylogin erfüllt jedes dieser Kriterien. Wir sind ein deutsches Unternehmen mit Sitz in Braunschweig, werden innerhalb Europas kontrolliert, und unser gesamtes Team sowie die gesamte Produktentwicklung befinden sich in Deutschland. Mozilla Ventures hält eine nicht beherrschende Minderheitsbeteiligung an heylogin; als Investmentarm der Mozilla Foundation teilt Mozilla Ventures unsere Vision eines freien und offenen Internets, und diese Beteiligung stellt keine wesentliche Beteiligung oder Kontrolle von außerhalb Europas dar. Unser Dienst wird ausschließlich aus europäischen, nach ISO/IEC 27001 zertifizierten Rechenzentren betrieben, und wir verarbeiten personenbezogene Daten streng nach der DSGVO.

Der weitere Teil dieses Whitepapers konzentriert sich auf das Produktkriterium: wie heylogin jede der zehn ENISA-Basisicherheitsanforderungen erfüllt, die den technischen Kern des Labels bilden.

3 Die ENISA-Basissicherheitsanforderungen

Die ENISA ist die Agentur der Europäischen Union für Cybersicherheit. Sie wurde 2004 gegründet und erhielt 2019 mit dem EU-Rechtsakt zur Cybersicherheit (Cybersecurity Act) ein dauerhaftes Mandat. Sie unterstützt die EU-Institutionen und Mitgliedstaaten dabei, in ganz Europa ein hohes gemeinsames Cybersicherheitsniveau zu erreichen, unter anderem durch Leitfäden und europäische Zertifizierungsschemata für Cybersicherheit. Die ENISA-Baseline ist ein technologieutraler Satz von Mindestanforderungen, der auf den Prinzipien Secure by Design, Secure by Default, Least Privilege und Überprüfbarkeit beruht. Das Originaldokument ist verfügbar unter:

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

Für jedes der zehn Prinzipien geben wir zunächst die Anforderung wieder und erläutern dann, wie heylogin sie erfüllt. Dabei gehen wir, wo zutreffend, auf die detaillierten Unterpunkte aus Abschnitt 3 des Originaldokuments ein. Wo sich ein Unterpunkt nicht direkt auf einen Zero-Knowledge-Passwortmanager übertragen lässt, sagen wir das und beschreiben die gleichwertige Maßnahme. "Wir", "unser" und "uns" bezeichnen durchgehend die heylogin GmbH als Anbieter. Funktionale Details sind in unserem Help Center unter <https://help.heylogin.com> dokumentiert; Sicherheits- und Architekturdetails sind in unserem Security Whitepaper und unserem Compliance Whitepaper dokumentiert, die über unser Trust Center unter <https://www.heylogin.com/de/trust-center> verfügbar sind.

Die folgende Tabelle fasst unsere Konformität mit den zehn ENISA-Basisprinzipien zusammen.

ENISA-Prinzip	Erfüllt
Security by Design	Ja
Least Privilege	Ja
Strong Authentication	Ja
Asset Protection	Ja
Supply Chain Security	Ja
Documentation Transparency	Ja
Quality Management	Ja
Service Continuity	Ja

ENISA-Prinzip	Erfüllt
EU Jurisdiction	Ja
Data Usage Restriction	Ja

1. Security by Design

Anforderung. Der Anbieter muss das gelieferte Produkt so gestalten und vorkonfigurieren, dass die Funktionen auf bewährten Sicherheitspraktiken beruhen und auf das für den Systembetrieb unbedingt erforderliche Minimum reduziert sind.

heylogin basiert auf einer Zero-Knowledge-Architektur. Alle Inhaltsdaten (Login-Titel, Benutzernamen, Websites, Teamnamen, Passwörter, TOTP-Secrets und benutzerdefinierte Felder) werden auf dem Endgerät Ende-zu-Ende-verschlüsselt. Unsere Server dienen nur als Synchronisations-Relay für bereits verschlüsselte Datenpakete und können diese nicht entschlüsseln. Die Verschlüsselung beruht auf bewährten kryptografischen Verfahren nach dem Stand der Technik und etablierten Kryptografie-Bibliotheken statt auf proprietären Verfahren.

Statt eines Master-Passworts bindet heylogin den Zugang standardmäßig an den Hardware-Sicherheitschip (Secure Enclave / TPM) des Geräts. Diese Standardkonfiguration reduziert die Angriffsfläche auf das notwendige Minimum und schließt Brute-Force-Angriffe auf ein Master-Passwort konstruktionsbedingt aus.

Im Detail: heylogin wird ohne unnötige Funktionen ausgeliefert, und der Client enthält keine undokumentierten Datenweiterleitungen oder Hintertüren. Sicherheitsrelevante administrative und Zugriffseignisse werden im Audit-Log der Organisation protokolliert, das Admins einsehen können. Wir setzen keine veralteten oder unsicheren Protokolle ein. Produkt und Abhängigkeiten werden durch kontinuierliches, automatisiertes Scannen von Abhängigkeiten und Schwachstellen in der Lage gehalten, bekannte Schwachstellen zu beheben.

2. Least Privilege

Anforderung. Der Anbieter muss das Produkt nach dem Prinzip der minimalen Rechte gestalten und vorkonfigurieren, sodass Admin-Rechte nur genutzt werden, wenn es unbedingt erforderlich ist, Sitzungen technisch getrennt sind und alle Konten verwaltbar sind.

Der Zugriff in heylogin wird gezielt und granular vergeben. Ein Login ist nur für die Personen oder Teams sichtbar und entschlüsselbar, mit denen er ausdrücklich geteilt wurde, da das Teilen kryptografisch pro Nutzer und pro Gerät durchgesetzt wird. Innerhalb einer Organisation steuern Admins den Zugriff über Rollen und gezieltes Teilen von Logins, sodass jeder Nutzer nur die Zugangsdaten erhält, die er für seine Arbeit benötigt.

Im Detail: Admins verwalten alle Nutzer der Organisation und deren Zugriffe selbstständig über die Verwaltungsoberfläche, ohne dass wir beteiligt sein müssen. Jeder Nutzer hat ein eigenes, an seine eigenen Geräte gebundenes Konto; Konten werden nicht geteilt. Administrative Funktionen sind von normalen Nutzerfunktionen getrennt und auf Admin-Rollen beschränkt. Sensible Vorgänge wie das Entsperren eines gekoppelten Geräts, das Koppeln eines weiteren Geräts oder das Anzeigen des Backup-Codes erfordern unabhängig von der Bildschirmsperre des Telefons eine lokale erneute Authentisierung am Sicherheitschip des Geräts (PIN oder Biometrie), wodurch sie technisch von einer allgemein entsperrten Sitzung getrennt sind. Für in heylogin gespeicherte Zugangsdaten können Organisationen eine Passwortrichtlinie durchsetzen; gespeicherte Passwörter bleiben vollständig unter der Kontrolle des Betreibers und können jederzeit geändert werden. Da heylogin ein auswendig gelerntes Master-Passwort durch hardwaregebundene Authentisierung ersetzt, lassen sich klassische Komplexitätsregeln für Master-Passwörter nicht auf den Entsperrmechanismus selbst übertragen; den gleichwertigen Schutz liefern der Sicherheitschip des Geräts und seine durchgesetzten Brute-Force-Limits.

3. Strong Authentication

Anforderung. Das Produkt muss starke Authentisierungsmechanismen für alle Konten bereitstellen und unterstützen. Ist die Authentisierung nicht erfolgreich, darf das Produkt keine nutzerspezifischen Aktivitäten zulassen.

Jedes Entsperren und jede Entschlüsselung in heylogin erfordert zwei Faktoren: den Besitzfaktor (ein registriertes Gerät mit Sicherheitschip) und den Wissens- bzw. Inhärenzfaktor (PIN oder Biometrie). Biometrie und PINs werden ausschließlich lokal auf dem Gerät verarbeitet und nie an heylogin übertragen; der Server erhält immer nur das kryptografische Ergebnis der Freigabe, niemals die Rohdaten.

Im Detail: Unterstützte Login-Geräte sind unter anderem Smartphone-Sicherheitschips (iOS/Android), Windows Hello, Touch ID und FIDO2-Sicherheitsschlüssel. Der Brute-Force-Schutz wird durch die Sicherheitschips der Plattformen durchgesetzt (eskalierende Wartezeiten oder Gerätesperre unter iOS/Android, ein Limit von 8 Versuchen bei FIDO2-Schlüsseln). Zugriff auf Daten wird nur nach erfolgreicher Authentisierung gewährt; eine fehlgeschlagene Authentisierung gewährt keinen Zugriff und lässt keine nutzerspezifischen Aktivitäten zu.

4. Asset Protection

Anforderung. Das Produkt muss kritische Informationswerte bei Speicherung und Übertragung angemessen schützen.

Kritische logische Werte sind in heylogin durchgehend geschützt. Alle Inhaltsdaten (Login-Titel, Benutzernamen, Websites, Teamnamen, Passwörter, TOTP-Secrets und benutzerdefinierte Felder) werden Ende-zu-Ende-verschlüsselt und können nur auf den gekoppelten Geräten des Nutzers entschlüsselt werden. Lediglich für den Betrieb des Dienstes erforderliche Metadaten wie Organisationsnamen und E-Mail-Adressen der Konten sind nicht Ende-zu-Ende-verschlüsselt. Alle Daten sind bei der Übertragung zusätzlich durch TLS geschützt. Server-Backups erhalten eine zusätzliche Verschlüsselungsebene im Ruhezustand, sodass selbst bei einer Kompromittierung des Backup-Speichers kein Zugriff möglich ist. Kryptografische Schlüssel verlassen den Sicherheitschip des Geräts nie im Klartext.

Im Detail: Sensible Daten wie Zugangsdaten werden ausschließlich verschlüsselt gespeichert und übertragen. Wir verwenden nur etablierte, bekannte Verschlüsselungsalgorithmen und Schlüssellängen, die nach dem Stand der Technik als sicher gelten, umgesetzt auf Basis etablierter Kryptografie-Bibliotheken, um Implementierungsschwächen zu vermeiden; proprietäre Verschlüsselungsalgorithmen kommen nicht zum Einsatz. Die Schlüsselerzeugung liefert sichere Schlüssel, und Schlüssel werden sicher im Sicherheitschip des Geräts gespeichert.

5. Supply Chain Security

Anforderung. Der Anbieter muss Mittel bereitstellen, die sicherstellen, dass das Produkt echt ist, im Betrieb nicht manipuliert werden kann und seine Integrität über den gesamten Produktlebenszyklus gewährleistet ist.

heylogin wird über die offiziellen Plattform-Stores (App Store, Google Play, Browser-Web-Stores) und signierte Vertriebskanäle verteilt, die für Nutzer Authentizität und Integrität der Software sicherstellen und eine Rückverfolgung der Komponenten zu ihrer echten Quelle ermöglichen. Da das Produkt ausschließlich clientseitig verschlüsselt, kann der Betreiber des Dienstes zu keinem Zeitpunkt serverseitig auf Inhalte zugreifen oder sie manipulieren.

Im Detail: Integritäts- und Abhängigkeitsanforderungen werden durch automatisierte Prüfungen im gesamten Build-Prozess überprüft, und gemäß unserer internen Secure Development Policy durchläuft jede wesentliche Änderung vor der Veröffentlichung ein verpflichtendes Code-Review durch einen zweiten Entwickler sowie eine automatisierte CI-Pipeline. Kontinuierliches, automatisiertes Scannen von Abhängigkeiten und Schwachstellen erkennt Probleme über den

gesamten Lebenszyklus. Die unterstützende Infrastruktur wird ausschließlich von nach ISO/IEC 27001 zertifizierten Unterauftragsverarbeitern mit Sitz in Europa bereitgestellt.

6. Documentation Transparency

Anforderung. Der Anbieter muss eine umfassende und verständliche Dokumentation über das Gesamtdesign des Produkts bereitstellen, die dessen Architektur, Funktionen und Protokolle, deren Umsetzung in Hardware- oder Softwarekomponenten sowie die Schnittstellen und Interaktionen der Komponenten beschreibt, damit das Produkt so sicher wie möglich implementiert und genutzt werden kann.

Wir stellen über unser Trust Center unter <https://www.heylogin.com/de/trust-center> eine umfassende, verständliche Dokumentation bereit: ein ausführliches Security Whitepaper (Architektur, kryptografisches Design, unterstützte Geräte und Protokolle sowie ein dokumentiertes Bedrohungsmodell einschließlich seiner Grenzen), ein Compliance Whitepaper, den Auftragsverarbeitungsvertrag, die technischen und organisatorischen Maßnahmen sowie eine öffentliche Liste der Unterauftragsverarbeiter. Die funktionale und Nutzungsdokumentation aller Funktionen ist öffentlich unter <https://www.heylogin.com> und im Help Center unter <https://help.heylogin.com> verfügbar.

Im Detail: Die Dokumentation wird über unsere eigenen Kanäle bereitgestellt und aktualisiert und ist nicht von dauerhaften Verweisen auf Server Dritter abhängig. Sie wird bei wesentlichen Änderungen an Design oder Funktionalität aktualisiert, und Nutzer werden über unsere Release Notes auf relevante Änderungen hingewiesen.

7. Quality Management

Anforderung. Der Anbieter muss nachweisen können, dass ein gesteuerter Security-by-Design-Ansatz verfolgt wird, einschließlich dokumentierter Prozesse für sichere Softwareentwicklung, Qualitätsmanagement und Informationssicherheitsmanagement.

Die heylogin GmbH ist nach ISO/IEC 27001:2022 (TÜV Rheinland) zertifiziert und betreibt ein entsprechend zertifiziertes Informationssicherheitsmanagementsystem. Unser Entwicklungsprozess, festgelegt in unserer internen Secure Development Policy, umfasst eine verbindliche Definition of Done, Code-Reviews durch einen zweiten Entwickler, automatisierte Tests und eine

CI-Pipeline sowie kontinuierliches, automatisiertes Schwachstellen-Scanning der Abhängigkeiten. Sicherheitsrelevante Änderungen werden geprüft, um die kryptografischen Ende-zu-Ende-Eigenschaften des Produkts zu erhalten. Das Produkt wurde zusätzlich von einem unabhängigen Penetrationstester, der secuvera GmbH, geprüft; der Bericht ist über unser Trust Center unter <https://www.heylogin.com/de/trust-center> verfügbar.

Im Detail: Unsere gültige ISO/IEC-27001-Zertifizierung deckt den relevanten Bereich ab, Nachweise zur Erfüllung der Anforderungen sind über diese Zertifizierung und die Dokumentation in unserem Trust Center verfügbar, und der ISMS-Geltungsbereich sowie die Erklärung zur Anwendbarkeit (Statement of Applicability) sind durch das Zertifikat abgedeckt.

8. Service Continuity

Anforderung. Der Anbieter muss über die vereinbarte Lebensdauer des Produkts Support gewährleisten, sodass das System wie vereinbart und sicher funktioniert.

heylogin wird als SaaS aus deutschen, nach ISO/IEC 27001 zertifizierten Rechenzentren mit Standby-Systemen betrieben, unterstützt durch verschlüsselte Backups, Monitoring und Alarmierung. Bei Verlust eines Geräts bietet das Produkt etablierte Backup- und Wiederherstellungsmethoden sowie eine durch Admins unterstützte Wiederherstellung von Organisationsnutzern, sodass der Zugang sicher fortgesetzt werden kann. Support wird über die vereinbarten Kanäle während der gesamten Vertragslaufzeit geleistet; betriebliche Kennzahlen (Verfügbarkeit, Wiederherstellungsziele, Reaktionszeiten) sind in unserem Compliance Whitepaper und unseren Geschäftsbedingungen festgelegt.

Im Detail: Wir scannen unsere Codebasis und Infrastruktur kontinuierlich auf Schwachstellen und betreiben eine Vulnerability Disclosure Policy, veröffentlicht unter <https://www.heylogin.com/security>. Gemeldete und neu bekannt gewordene Schwachstellen werden gemäß unserer internen Security Incident Management Procedure bewertet und behoben.

9. EU Jurisdiction

Anforderung. Der Anbieter muss akzeptieren, dass sich alle Verträge, auch mit Unterauftragnehmern, ausschließlich auf das Recht eines EU-Mitgliedstaats beziehen und einen Gerichtsstand in einem EU-Mitgliedstaat vorsehen.

Die heylogin GmbH ist ein deutsches Unternehmen mit Sitz in Braunschweig. Verträge unterliegen deutschem Recht (Recht eines EU-Mitgliedstaats), Gerichtsstand ist Deutschland. Die

gesamte Kerninfrastruktur und alle für Inhaltsdaten eingesetzten Unterauftragsverarbeiter befinden sich in Europa; für den Kerndienst werden keine US-Hyperscaler eingesetzt. Die Datenverarbeitung erfolgt ausschließlich in Deutschland, der EU oder dem EWR (siehe Auftragsverarbeitungsvertrag), und eingesetzte Unterauftragsverarbeiter sind vertraglich an dieselben Datenschutzpflichten gebunden.

Im Detail: heylogin unterliegt keinen Rechtsordnungen außerhalb der EU, die einen Zugriff auf Daten des Betreibers erzwingen könnten; das anwendbare Recht ist in unseren Geschäftsbedingungen und im Auftragsverarbeitungsvertrag festgelegt.

10. Data Usage Restriction

Anforderung. Der Anbieter muss alle Datenerhebungen und -verarbeitungen, die stattfinden oder stattfinden können, nach Kontext und Zweck ausdrücklich angeben, begründen und dokumentieren, einschließlich der zugrunde liegenden rechtlichen Verpflichtungen.

Alle Datenerhebungen und -verarbeitungen sind in unserer Datenschutzerklärung, dem Auftragsverarbeitungsvertrag und der öffentlichen Liste der Unterauftragsverarbeiter nach Zweck und Kontext angegeben und begründet, einschließlich der jeweiligen Rechtsgrundlagen nach DSGVO. Aufgrund der Zero-Knowledge-Architektur hat die heylogin GmbH keinen technischen Zugriff auf gespeicherte Inhaltsdaten (Login-Titel, Benutzernamen, Websites, Passwörter, TOTP-Secrets und benutzerdefinierte Felder). Die Verarbeitung im Auftrag des Kunden erfolgt ausschließlich auf dokumentierte Weisung des Verantwortlichen auf Grundlage eines Auftragsverarbeitungsvertrags nach Art. 28 DSGVO.

Im Detail: Ort der Verarbeitung und etwaige Drittlandübermittlungen sind für jeden Unterauftragsverarbeiter in unserer öffentlichen Liste der Unterauftragsverarbeiter dokumentiert.