Compliance Whitepaper

How heylogin meets compliance requirements

heylogin GmbH

February 18, 2025, Version: 3.0

Contents

1 Legal

1.1 Terms of Use

The Terms of Use apply to all users of heylogin, i.e. the free private accounts, but also to employees in a company who use heylogin. The current terms of use can be found at https://www.heylogin.com/en/terms-of-use.

1.2 Terms & Conditions

If you have purchased heylogin through our sales team, the terms and conditions you received in this process apply. If no special requirements have been contractually agreed upon, the terms and conditions apply, which can be found at https://www.heylogin.com/en/terms.

Our order process via credit card or PayPal is handled by our online reseller & "Merchant of Record", Paddle.com, who also handles order-related inquiries and returns. For information about the Paddle order process and your rights as a customer, please read Paddle's Terms & Conditions and Privacy Policy at https://www.heylogin.com/en/terms-paddle.

1.3 Privacy Policy & GDPR

The European General Data Protection Regulation (GDPR) is one of the most important achievements for a self-determined digital identity. The protection of personal data has always been an important concern for us. When using our software and the associated information, we always take care not to collect any data and to process all necessary data in accordance with the DSGVO.

There is a strict separation between the marketing website heylogin.com and the product on heylogin.app. On heylogin.app sensitive personal data is processed which is end-to-end encrypted and only available to the respective users. The use of external services on heylogin.app is therefore reduced to a minimum.

The most important rights and their implementation at heylogin are summarized below. Further details can be found in the privacy policy for our product at https://www.heylogin.com/en/privacy.

GDPR	heylogin
Art. 5 Principles relating to processing of personal data	When using external software, we make sure that data protection is our top priority. We only use providers with extended data protection settings to guarantee maximum data security for the user.
Art. 17 Right to erasure	We implement the right to deletion organizationally. Contact our support and we will delete your data as soon as possible.
Art. 20 Right to data portability	We allow the export of data by the user.
Art. 32 Security of processing	We collect personal data only in special cases and encrypt everything that is personally identifiable information.

1.4 Data Processing Agreement (DPA)

The data processing agreement, available at https://www.heylogin.com/en/dpa, automatically becomes effective on the day the contract is signed and remains effective until the contract is terminated.

If desired, it can also be signed by both parties. A request for this can be made via our partner Yousign. After verification, we will send you a signature request. This enables the contractor (heylogin GmbH) and client (you) to digitally sign the DPA in a legally valid manner: Submit request via Yousign: https://yousign.app/workflows/forms/7da62424-a88c-421e-b416-3668905572fa

If you have any questions, please contact us by e-mail at legal@heylogin.com.

2 ISO 27001:2022 certification

heylogin GmbH operates an information security management system (ISMS) that complies with the ISO 27001:2022 standard and meets the highest security standards. The ISMS is certified by TÜV Rheinland under the test mark number 9000032416: https://www.certipedia.com/quality_marks/9000032416?locale=en

Figure 1: Our ISMS is ISO 27001:2022 certified.

All assurances mentioned in this chapter are mapped by corresponding technical and organizational measures within the ISMS.

3 Operation

3.1 Server locations

The heylogin production environment is located in Nürnberg, the standby server in Falkenstein. Backups are stored separately in Frankfurt (all mentioned cities are located in Germany). All data centers are ISO 27001 certified (Hetzner certification).

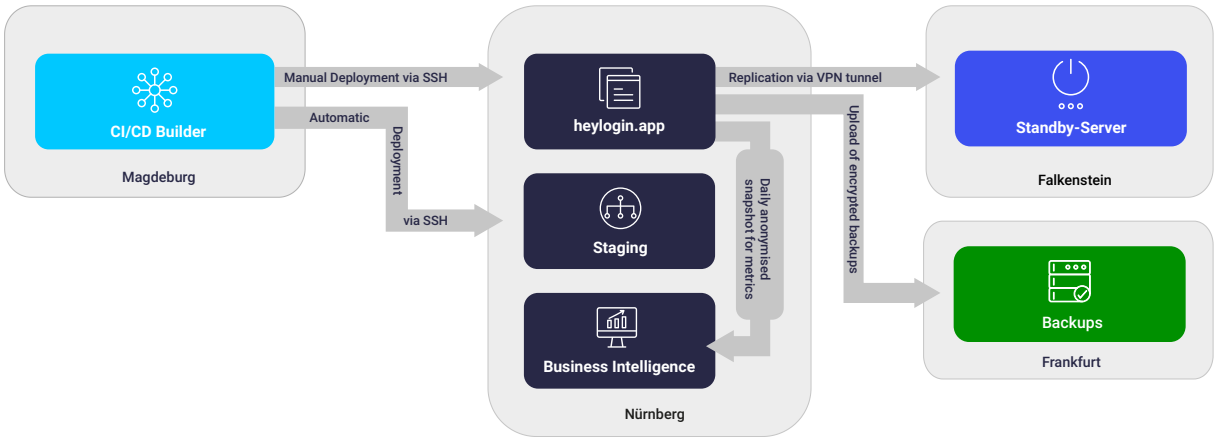

Figure 2: Development environment with Continuous Deployment (CI), production environment and backup systems are logically and physically separated from each other.

3.2 Failure safety

The defined Recovery Time Objective (RTO) of the heylogin service is 8 hours. The measured Recovery Time Actual (RTA) is less than 2 hours. The architecture of heylogin allows us to

start a replacement instance of our productive environment within a short time. If the data center used by our hosting provider is no longer available, there is a standby server that can be converted into a functioning productive environment within a restart time of no more than 30 minutes. No data loss occurs in this case.

The defined Recovery Point Objective (RPO) is 60 minutes. Encrypted backups of the server-side database are automatically created every hour. The backups are stored for 90 days. This database continues to be actively replicated to the previously mentioned standby server in another data center. With this backup, we protect ourselves against a complete failure of our hosting provider. Within a recovery time of maximum 60 minutes we can start up a new productive environment at an alternative hosting provider. In this case, the heylogin client applications will synchronize login data that is still locally available with the server to reduce the probability of data loss even more.

3.3 Monitoring

The heylogin production environment is monitored by a system every minute. In case of failures and anomalies, notifications are sent and logged.

3.4 Security incident response

All administrative logins to the production environment and the standy server are logged and must be justified. There is always an employee on standby to intervene in case of anomalies.

3.5 Availability

We strive for an availability of 99.9% on annual average. Through our architecture and technical measures for fail-safety, we have achieved an availability of ~99.95% on annual average in 2022, for example. Contractually, we guarantee an availability of 99% on annual average. For a contractually guaranteed higher availability, please contact our sales team.

3.6 Support

We aim to answer general support requests within 2 working days (Mon-Fri). Errors that affect the operation will be handled within 8 hours on working days. Critical errors, such as failures of the productive environment, are processed within 8 hours on all weekdays (Mon-Sun).

3.7 Capacity

heylogin has no limits on the amount of logins and teams stored. We reserve at least 500MB of storage per organization.

4 Cryptography

This compliance whitepaper only briefly introduces the most important cryptographic procedures. Details can be found in our Security Whitepaper.

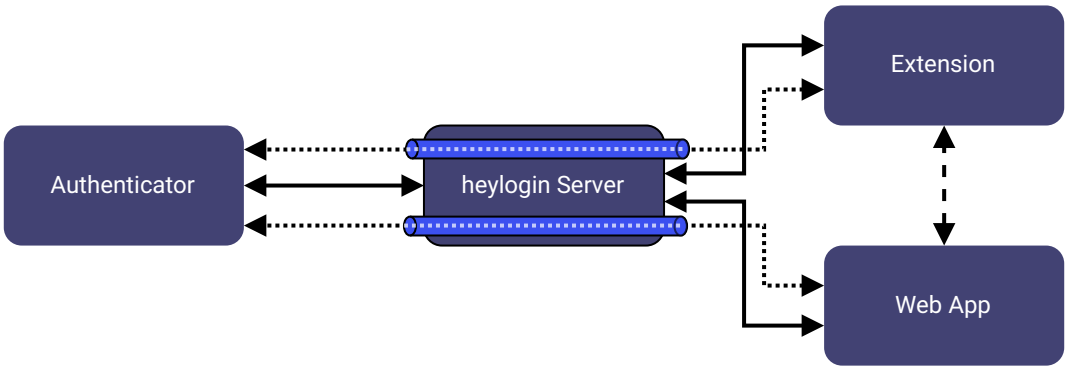

Figure 3: Only the user's authenticator, such as smartphone or security key, can decrypt the logins. End-to-end encryption & authentication between smartphone and browser extension ensure that no third party can read logins. Even the heylogin server cannot access content data and forwards it only in encrypted form.

4.1 Transport encryption

The production environment uses transport encryption according to current standards (TLS 1.3 or 1.2) for all connections. TLS is enforced by HSTS.

4.2 Encryption of server backups

Server backups are stored exclusively in encrypted form. ChaCha20 is used for symmetric encryption and Poly1305 for integrity protection.

4.3 End-to-end encryption

The confidentiality of the stored data is ensured with end-to-end encryption. XSalsa20 is used as the symmetric algorithm. The integrity of the stored data is ensured by Poly1305 and thus protected against modification. Curve25519 is used as the asymmetric encryption. heylogin uses the Secure Element embedded in the smartphone hardware for cryptographic operations.

4.4 End-to-end authentication

All of the user's connected devices are authenticated "out-of-band". This is usually done by scanning a QR code, which initiates a Diffie-Hellman key exchange. As an alternative for devices without a camera, a hash-commitment procedure with Short Authentication String is used.

5 Software development

5.1 Quality assurance

heylogin is backed by a comprehensive test suite that automatically checks every code change for correctness and compatibility. We also automatically check the compatibility of our server application with older versions of our client applications.

New features are first tested in internal review apps before they are integrated into the productive environment. In addition, there is a select group of users who always use the latest development version of the mobile app together with the productive environment in order to detect errors as early as possible.

The compatibility of the browser extension with websites is continuously tested automatically. If a faulty website is reported, the algorithm is adjusted and this website is added to the test suite.

5.2 Error handling

When an application error occurs in a heylogin component (Android, iOS, Web, Extension), a message is sent to an error tracking system. This contains necessary information for error diagnosis and a pseudonymized identification number, but never content data.

Based on the severity of the failure, actions are taken to prevent further failures or mitigation changes are developed.

5.3 Documentation

The architecture of heylogin is documented in the company's internal wiki and can be viewed by all employees. Details regarding heylogin's security architecture can be found in our Security Whitepaper.

6 Sustainability

heylogin GmbH attaches great importance to sustainability. Our hosting provider Hetzner runs its data centers 100% with electricity from renewable sources. Laptops that have been written off are donated to Hey Alter! and thus continue to be used by students.

7 Implementation of laws, standards and norms by heylogin

The use of heylogin can help your company meet requirements of certifications such as ISO 27001 and TISAX.

7.1 ISO 27001

The International Organization for Standardization (ISO) develops and publishes technical, industrial, and commercial standards worldwide. The ISO 27001 standard for Information Security Management Systems (ISMS) provides a framework for information security consisting of 114 controls. To achieve ISO 27001 certification, organizations must demonstrate compliance with most controls.

While each control contains important objectives related to organizational security and secure processes, organizations should pay particular attention to Annex A.9. heylogin can be used as a technical controls for sections A.9.4.2 and A.9.4.3.

ISO 27001	heylogin
A.9.4.2 Secure log-on procedures	This control is about using multi-factor authentication for secure login to systems.

ISO 27001	heylogin
	Our security architecture is always 2-factor secure without the disadvantages of traditional methods, since all logins are end-to-end encrypted with the smartphone's security chip. This security chip forms the 1st factor (possession) and must always be unlocked on the smartphone itself by a 2nd factor (biometrics or PIN). This means that every access to every website is stored and protected in a 2-factor secure manner. Since no master password is used, there is no need for employee training on how to use it securely.
A.9.4.3 Password management system	This control is about password management, including the ability to create strong passwords. Password sharing is discouraged in the ISO standard. heylogin stores passwords in an end-to-end encrypted automated manner and generates strong passwords for account registration. Passwords can be assigned to employees or organized into teams. Furthermore, heylogin can control the sharing of access by admins and thus prevents careless disclosure of passwords. By a policy it is possible to share accounts without giving out the corresponding passwords.

7.2 ISO 27002

ISO/IEC 27002 is a standard of the ISO 27000 family that contains best practices and can therefore be interpreted and applied individually by organizations according to the respective information security risks. On the one hand, this flexibility gives users a lot of leeway to select and implement the appropriate measures; on the other hand, it makes ISO 27002 unsuitable for

compliance testing. The measures in Annex A of ISO 27001 are derived from and aligned with ISO 27002.

The use of heylogin supports companies in the implementation of ISO 27002 in the organizational measures (ISO 27002:2022, “organizational controls”, Clause 5) as well as the technical measures (ISO 27002:2022, “technological controls”, Clause 8).

ISO 27001-2022	heylogin
5.16 Identity management	This measure is about identity management in companies.
Guidance b)	With heylogin, decision-makers always have full control over which logins are used as “shared identities” by multiple employees. This fulfills approval and documentation requirements.
d)	Logins can be deleted or revoked from individual employees at any time. This fulfills the procedural requirements.
f)	heylogin’s audit log records all significant events concerning the use and management of logins.
5.17 Authentication information	This measure deals with the storage and management of authentication data.
Guidance „Allocation of authentication information“ a)	heylogin generates passwords for each login automatically during registration. Thus, they are unique for each website and cannot be guessed.
c)	As required, passwords are never transmitted in clear text, but are assigned end-to-end encrypted via heylogin or used in a team.
d)	A user confirmation is technically implemented in heylogin. Employees can confirm joining a heylogin team with a click.

ISO 27001-2022	heylogin
f)	In a future version of heylogin, better traceability will be mapped by an access history.
User responsibilities a)	With heylogin, passwords always remain encrypted and are only shared with authorized employees.
c)	heylogin generates passwords automatically and thus fulfills all requirements in this point.
d)	Password generation makes passwords unique.
Password management system b)	As also required in “User responsibilities” (c), strong passwords are generated according to the state of the art.
g)	Passwords are not displayed when logging in. heylogin replaces the login process on websites in the browser.
h)	Passwords are only exchanged end-to-end encrypted in heylogin.
Other information	heylogin can be classified as a “password vault”. It protects and simplifies the handling of passwords. As described in the standard, measures are thus effectively implemented.
6.3 Information security awareness, education and training	This measure is about the use of continuing education and training for employees in the context of information security. The use of heylogin eliminates the need for security awareness training on password security, as this is implemented technically.
8.5 Secure authentication	This measure is about the technology and processes of authentication to implement access controls.

ISO 27001-2022	heylogin
Guidance	With heylogin, accesses are automatically hardware-protected and “by default” 2-factor secure. This means that the required “multi-factor authentication” is implemented for all websites.
e)	Additional brute force protection on the part of the login mechanism is not necessary, as heylogin generates and uses strong and unique passwords.
i)	heylogin replaces the login process on websites in the browser. Thus, passwords are not visible to the employee.
k)	In heylogin, devices can be locked or unlocked at any time. Automatic locking takes place at the end of a working day.

7.3 TISAX

Trusted Information Security Assessment Exchange (TISAX) is a testing and exchange procedure of the automotive industry and allows to check the maturity level of information security at potential partners. The German Association of the Automotive Industry (VDA) publishes the Information Security Assessment (ISA) as a catalog of criteria for a TISAX audit.

heylogin is a possible control to achieve the desired protection requirement in the information security criteria catalog. This applies in particular to the area of Identity and Access Management (VDA ISA catalog v5.0 Section 4).

VDA ISA v5.0 catalog		heylogin
3.1.4	To what extent is the handling of mobile IT devices and mobile data storage devices managed?	heylogin requires the use of Android or iOS smartphones in the company. To ensure 2-factor security, the display lock with biometrics or PIN must be activated.
4.1.2	To what extent is the user access to network services, IT systems and IT applications secured?	We have integrated 2-factor authentication via smartphones into our software to ensure security when sharing sensitive and highly confidential data.
4.1.3	To what extent are user accounts and login information securely managed and applied?	heylogin itself uses unique personal accounts. Due to the end-to-end encryption, we as the provider cannot access the stored login data. heylogin implements easy offboarding of employees, allowing user accounts to be disabled quickly and easily. The team functions allow admins to always have full control over so-called “collective accounts”. Admins can assign personalized passwords to individual users inside heylogin to make sure that these are known to the assigned user only.
4.2.1	To what extent are access rights assigned and managed?	Passwords are only known to the user due to heylogin’s end-to-end encryption.

VDA ISA v5.0 catalog		heylogin
5.1.1	To what extent is the use of cryptographic procedures managed?	We encrypt the transmitted data several cryptographic methods and use XSalsa20+Poly1305 and Curve25519 as algorithms.
5.1.2	To what extent is information protected during transport?	End-to-end encryption means that only the sender and recipient can access the data.