heylogin

Compliance
Whitepaper

of **heylogin GmbH**, Sophienstraße 40, 38118 Braunschweig
for the product heylogin

Date of Change: 6. April 2022
Version: 1.5

Inhalt

1 | Contract agreements....3
1.1 Availability....3
1.2 Capacity....3
1.3 Cancellation....3
2 | Operation....4
2.1 Server locations....4
2.2 Failure safety....4
2.3 Monitoring....5
2.4 Security incident response....5
3 | Cryptography....6
3.1 Transport encryption....6
3.2 Encryption of server backups....6
3.3 End-to-end encryption....6
3.4 End-to-end authentication....7
4 | Software development....8
4.1 Quality assurance....8
4.2 Error handling....9
4.3 Documentation....9
5 | Sustainability....9
5.1 Sustainable use of resources....9
6 | Standards, certifications, laws....10
6.1 Preface....10
6.2 GDPR....10
6.3 ISO 27001....11
6.4 TISAX....12

1 | Contract agreements

1.1 Availability

heylogin GmbH guarantees an availability of 99.9% on annual average. We can ensure this availability through our hosting provider Hetzner and our architecture.

1.2 Capacity

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

1.3 Cancellation

Depending on the contract period, the contract can be terminated as of the next month or annually. After the end of the contract period, logins stored in teams can be exported for at least 30 days. All team functions are deactivated after the end of the contract period. Teams can no longer be created, edited or deleted. Furthermore, logins in teams can no longer be used, created or edited. All login data can be deleted at any time.

2 | Operation

2.1 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 1: ISO 27001-certified data centre information security management system

2.2 Failure safety

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.

Encrypted backups of the server-side database are automatically created every hour. 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 system at an alternative hosting provider. In this case, the heylogin client applications will synchronize login data that is still locally available with the server, so that the probability of data loss is low. In the worst case, there may be a data loss of changes that have happened since the last hourly backup.

2.3 Monitoring

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

2.4 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.

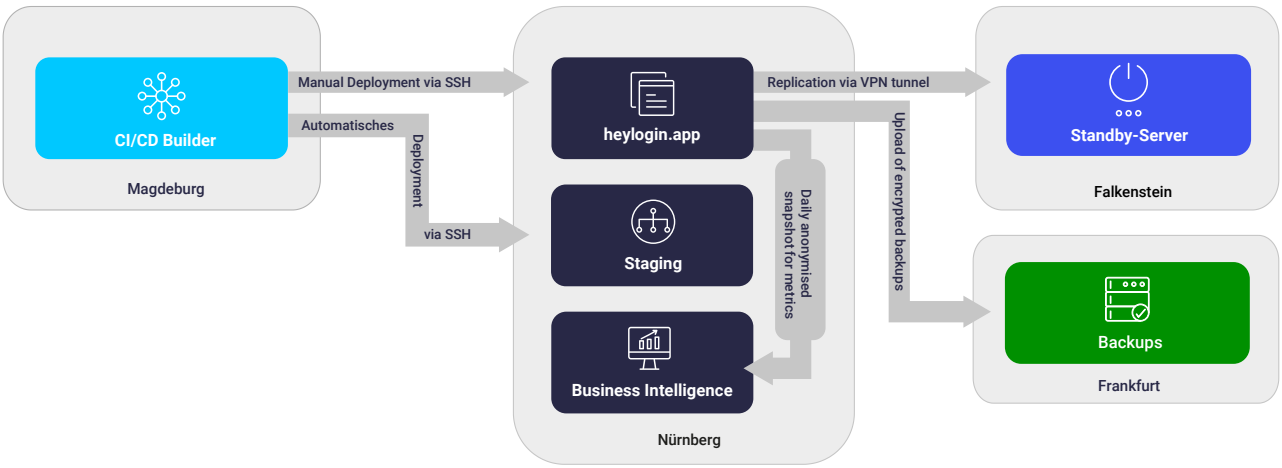

Figure 2: Development environment with Continuous Deployment (CI), production environment and backup systems are logically and physically separated from each other.

3 | Cryptography

3.1 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.

3.2 Encryption of server backups

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

3.3 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.

3.4 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.

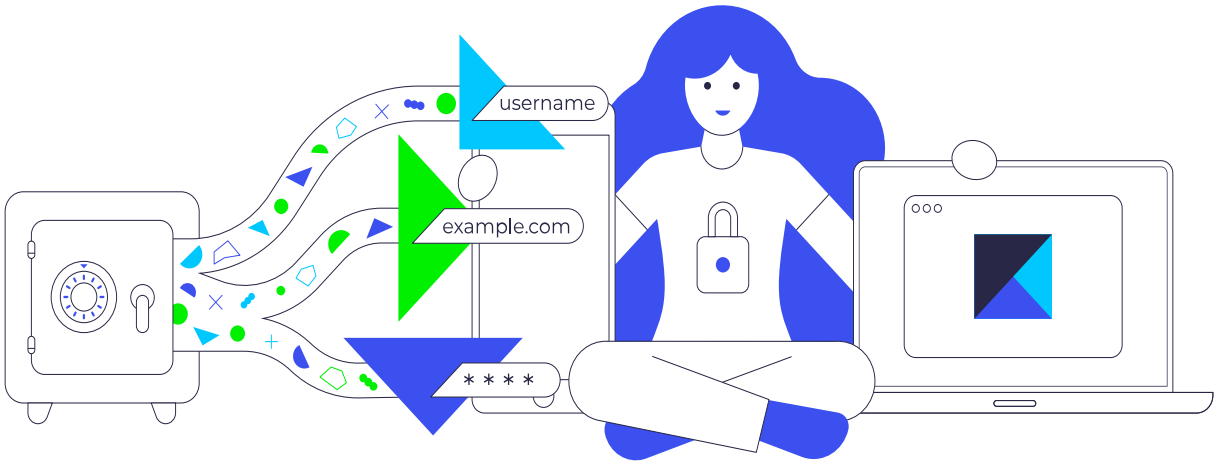

Figure 3: Only the user's smartphone can decrypt and pass on the logins. End-to-end encryption & authentication between smartphone and browser ensure that no third party can read logins.

4 | Software development

4.1 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.

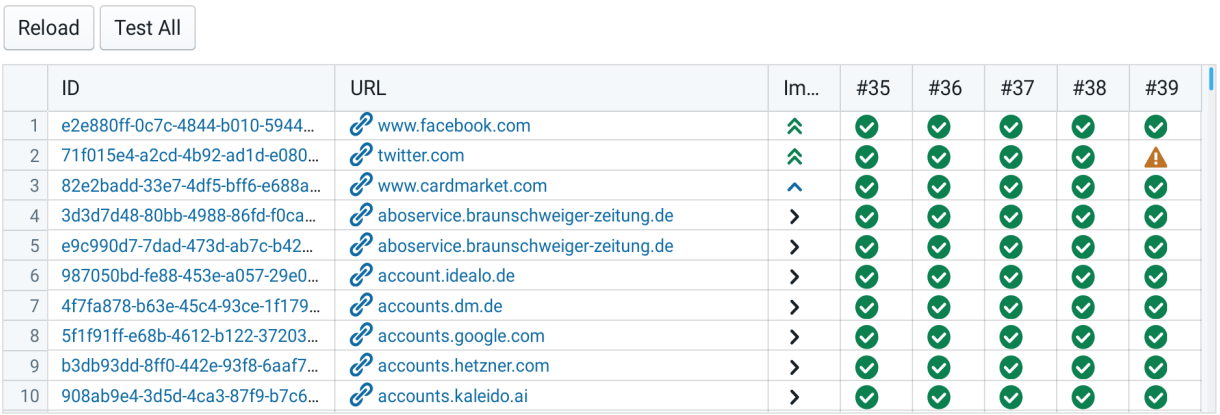

Figure 4: Automated compatibility tests for the browser extension

4.2 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.

4.3 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.

5 | Sustainability

5.1 Sustainable use of resources

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.

6 | Standards, certifications, laws

6.1 Preface

heylogin GmbH and the product heylogin use modern security standards and meet the legal requirements of the General Data Protection Regulation (GDPR). At the same time, the use of heylogin can help your company meet requirements of certifications such as ISO 27001 and TISAX.

6.2 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.

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.	✓

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

6.4 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, it is assumed that a display lock with biometrics or PIN is 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?	We have clearly personalized user accounts to which we have no access because of our encryption protocol.	✓
4.2.1	To what extent are access rights assigned and managed?	Passwords are only known to the user due to the encryption.	✓
5.1.1	To what extent is the use of cryptographic procedures managed?	We encrypt and hash the data to be transmitted with several cryptographic methods and use XSalsa20+Poly1305 and Curve 25519 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.	✓

Please note:

To meet the TISAX requirements, the heylogin team function must not be used. As proof, an organizational control is possible, e.g. in the form of written contract.