Technical & Organizational Measures (TOMs)

The following is a list of the specific technical and organizational measures taken for commissioned processing pursuant to Art. 24(1) of the EU General Data Protection Regulation (GDPR).

heylogin GmbH complies with the obligation laid down in the GDPR to protect the processing of personal data by appropriate technical and organizational measures and, as far as possible, to anonymize or pseudonymize personal data. All measures taken must take into account the risk of the respective data processing operation and correspond to the state of the art. In particular, the effectiveness of the measure should take into account the protection goals of confidentiality, integrity, availability and resilience.

Definition of protection goals:

- **Confidentiality**: Protection of data, information and programs from unauthorized access.
- **Integrity**: Factual and technical accuracy and completeness of all information and data during processing.
- **Availability**: Information, data, applications, IT systems and IT networks are accessible for processing.
- **Resilience**: Refers to an aspect of availability and thus the ability of information, data, applications, IT systems and IT networks to function in the event of disruptions, failures or heavy use.

1 Ensuring confidentiality

1.1 Physical access control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

Measures:

- No unauthorized access to data processing systems.
- The office buildings are secured with a locking system. The entrance area is under video surveillance.
- All data processing systems on which customer data is stored is located at subcontracted processors.

1.2 Data access control

Measures suitable for preventing data processing systems from being used by unauthorized persons.

Measures:

- No unauthorized system use.
- All own IT systems are secured with secure passwords.
- When leaving the workstation, the desktop is locked.
- The system enforces a minimum length of 16 characters, which must include numbers and letters.
- The assignment of rights when new employees join and leave the company is regulated in the information security management system.
- Suppliers of hosting infrastructure are ISO 27001 certified.

1.3 Data usage control

Measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use, or after storage.

Measures:

- Data is secured by software against unauthorized reading, copying, modification, or removal.
- Logins are logged.
- Logins on production systems generate notifications.
- The access control policy in the information security management system defines a binding process and rules for access control to internal and external systems.

1.4 Segregation control

Measures that ensure that data collected for different purposes is processed separately. This can be ensured, for example, by logical and physical separation of data.

Measures:

- Separate processing of data collected for different purposes.
- The production system is multi-client capable and ensures separation of data for individual customers on the software side.

- Each customer can be identified by his login to access only the data managed by him.
- The production system is strictly separated from test and development systems.

1.5 Measures for Mobile Work / Home Office

Measures that ensure the processing of personal data during mobile work is carried out in accordance with existing security policies and that a level of protection equivalent to that of the office workplace is guaranteed.

Mobile work is limited to the customer data defined in the Data Processing Agreement: account email addresses, log and metadata, as well as support and device data. All other data (e.g., usernames, passwords) are end-to-end encrypted and therefore technically not accessible to employees (cf. Data Processing Agreement 1.1).

Measures:

- Mobile work and home office workplaces are subject to the applicable policies within the ISO 27001-certified information security management system. All employees are contractually obliged to comply.
- All endpoint devices are protected with full-disk encryption or an equivalent mechanism and are regularly updated with the latest security patches.
- Access to endpoint devices is only possible with local user accounts protected by passwords in accordance with the password policy.
- All endpoint devices are locked in accordance with existing policies as soon as users leave their workplace.
- Workplaces are, in accordance with existing policies, free of unsecured sensitive information; documents, cabinets, drawers, and screens are always secured.

2 Ensuring integrity

2.1 Transfer control

Measures to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or while being transported or stored on data media, and that it is possible to verify and determine to which entities personal data is intended to be transmitted by data transmission equipment.

Measures:

- All data transfers between heylogin and external systems take place exclusively via encrypted connections. The protocol used is TLS in version 1.2 or higher.
- Data in paper form is disposed of using a document shredder in accordance with ISO/IEC 21964 with destruction level P4 in compliance with data protection regulations. Electronic media are collected and disposed of in accordance with ISO/IEC 21964 with destruction levels E4, H4.

2.2 Input control

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered into data processing systems, changed or removed.

Measures:

- Data processing is carried out directly by the customer.

3 Pseudonymization and Encryption

3.1 Pseudonymization

Measures that ensure the pseudonymization of data.

Measures:

- Personal data is pseudonymized after 30 days for longer-term storage. Pseudonymization is performed by assigning UUID identifiers.

3.2 Encryption

Measures that ensure encryption of data.

Measures:

- Encryption procedures are used in accordance with the current state of the art.
- Data is transmitted in encrypted form during electronic transmission or while in transit. The protocol used is TLS in version 1.2 or higher.
- Content-related customer data is stored exclusively in end-to-end encrypted form. The algorithms used are XSalsa20+Poly1305 and X25519.
- Backups of content-related customer data are additionally encrypted. The tool used is “age.

4 Guarantee of availability, resilience and recoverability

4.1 Availability (of data)

Measures to ensure that personal data is protected against accidental destruction or loss - ensuring availability of data.

Measures:

- All customer data is backed up hourly to at least one external system.
- The systems of the subcontracted processors used are secured against power failure by UPS.
- A firewall protects external access to all systems.
- All production systems are geo-redundant so that if one component fails, another component can immediately take over.

4.2 Resilience (of systems)

Measures to ensure that personal data is protected against accidental destruction or loss - ensure resilience of systems.

Measures:

- Monitoring of productive systems.
- Alerting in case of unexpected deviations in monitoring.

4.3 Recoverability (of data / systems).

Measures to ensure that personal data is protected against accidental destruction or loss - ensuring recoverability of data and systems.

Measures:

- Complete restoration of operations from a current backup within approximately two hours.

5 Procedures for periodic review, assessment and evaluation

5.1 Order control

Measures to ensure that personal data processed on behalf of a client can only be processed in accordance with the client's instructions.

Measures:

- Conclusion of the necessary commissioned data agreements.
- Conclusion of the necessary standard contractual clauses.
- Selection of the contractor under due diligence aspects.
- Obligation of the contractor's employees to maintain data secrecy.
- Ensuring the destruction of data after completion of an order.

5.2 Data protection management

Measures to ensure that methods have been evaluated to systematically plan, organize, manage and control the legal and operational requirements of data protection.

Measures:

- Regular review of the effectiveness of technical and organizational measures according to the PDCA cycle (Plan-Do-Check-Act).
- Compliance with the information requirements pursuant to Art. 13 DSGVO.
- Compliance with the information requirements pursuant to Art. 14 DSGVO.
- Documentation of all data protection procedures and regulations.
- Implementation of data protection impact assessments (if required).
- Regular sensitization of employees to data protection.
- Review of the effectiveness of the TOMs (conducted at least annually).
- Commitment of employees to data secrecy.

5.3 Incident response management

Measures to ensure that security incidents can be prevented or, in the case of security incidents that have already occurred, that data and systems can be protected and that rapid analysis and remediation of the security incident can be carried out.

Measures:

- Documentation of security incidents.
- Use of firewall and its regular updating.
- Use of spam filters and their regular updating.
- Use of virus scanners and their regular updating.
- Use of continuous vulnerability scanning on both codebase and infrastructure.

5.4 Data protection-friendly default settings

Measures that ensure that a certain level of data protection already exists in advance through the appropriate technical design (privacy by design) and factory settings (privacy by default) of a software.

Measures:

- Personal data is only collected if it is required for a specific purpose.