Appendix A4

Technical and Organizational Measures

1Measures to ensure confidentiality

1.1 Access control

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

General (documented) building security concept
Locking system (with security locks)
Alarm system
Video surveillance of the entrances
(Concrete) access authorization concept
Accompaniment of visitors by employees
Electronic access code cards/ access transponders
Key regulation (including key directory; separate locking of individual offices)
Careful selection of cleaning staff

1.2 Access control

Measures that are suitable for preventing data processing systems (computers) from being used by unauthorized persons.

Role concept
Authorization management
Creating user profiles
Functional and/or time-limited assignment of user authorizations
Documented process for assigning rights when new employees join the company
Use of individual passwords
Login with user name and password
Login with biometric data
Automatic password-protected locking of the screen after inactivity (screen saver)
Secure password" policy (with minimum requirements for password complexity):

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Vienna
hello@heylog.com;

• At least 8 characters
• At least 8 characters for local admin passwords
• Upper and lower case, special characters, number (of which at least 3 criteria)
Time delay between individual login attempts
Failed login attempts are displayed to users
Two-factor or multi-factor authentication for high-risk processing
Saving passwords in the browser only with master password
Encryption of notebooks / tablets
Encryption of networks
• Encryption algorithms used: WPA3
Preventing the execution of downloaded software whose sources are marked as unsafe
Use of VPN technology
Use of a software firewall
Default authentication information is changed after software installation/first login
Regulation on home office / teleworking

1.3 Access control

Measures that ensure that persons 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 and after storage.

Management of user rights by administrators
Use of an authorization concept
Minimal use of administrator accounts (minimum number of administrators)
Various administrative roles according to the least privilege concept (users, firewall, backups, etc.)
Superuser (e.g. root under Linux) not used as far as possible
Regular review of roles and authorizations
Regular evaluation of protocols (log files)
Time limitation of access options
Logging of file accesses
Logging of file deletions
Logging of file changes
SPAM filter
Encrypted data storage
Encryption algorithms used: AES (128/256 bit)

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Vienna
hello@heylog.com;

Hash function used: SHA3
Two-factor authentication for web server maintenance
SSL certificates only from trusted sources
Only use WLAN on current routers with effective access mechanisms
WLAN guest access without access to internal network
Scanning of incoming emails using anti-malware

2 Measures to ensure integrity

2. 1Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data are to be transmitted by data transmission equipment.

How is data transferred between the controller and third parties?
• VPN connection
E-mail encryption (SMIME)
Logging of accesses and retrievals
Provision via encrypted connections such as sftp, https
Data exchange via https connection (encryption protocol used: TLS 1.3)
For HTTPS: Use of client certificates
Regulation on the use of cloud services (incl. exit strategy)

2.2 Input control

Measures to ensure that it can be subsequently verified and established whether and by whom personal data has been entered into, modified or removed from data processing systems. The control can be carried out by using the logging functionalities

Technical logging of the entry, modification and deletion of data
Manual or automated evaluation of the logs
Differentiated user authorizations:
• Individual user names, no user groups
• Assignment of rights to enter, change and delete data on the basis of an authorization concept
Commitment to data secrecy
Traceability of data entry, modification and deletion through individual user names (not user groups)
Assignment of rights to enter, change and delete data on the basis of an authorization

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Vienna
hello@heylog.com;

concept. The user cannot delete or change any data in the application, he can send a request to GDPR@heylog.com and the data will be adjusted within 48 hours.

3 Measures to ensure availability & resilience

3.1 Availability control

Measures to ensure that personal data is protected against accidental destruction or loss.

Fire alarm systems in server rooms
Smoke detectors in server rooms
Fire doors
Waterless firefighting systems in server rooms
Water sensors in server rooms
Lightning/overvoltage protection
Air-conditioned server rooms
Server rooms in separate fire compartment
Storage of backup systems in separate rooms and in a separate fire compartment
Server rooms not under or next to sanitary facilities
Restrict access to server rooms to essential personnel only
Alarm message in the event of unauthorized access to server rooms
CO2 fire extinguishers in the immediate vicinity of the server rooms
UPS system (uninterruptible power supply)
Power generator
Documented data protection and backup concept
Regular data recovery tests
Ensuring the long-term technical readability of backup storage media
Regular data recovery tests and logging of the results: The recovery tests are carried out every last quarter of the year.
The backup process is checked daily by the Google Cloud admin and a notification is sent if a backup fails.
Backup & recovery concept (formulated): Heylog makes a nightly backup and is managed by Google Cloud.

3.2 Resilience (resistance and failure control)

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Vienna
hello@heylog.com;

Should enable systems to deal with risk-related changes and demonstrate tolerance and the ability to compensate for disruptions.

Redundant power supply
Redundant data connection
System hardening (deactivation of unnecessary components)
Immediate and regular activation of available software and firmware updates
Regular sensitization of employees (at least annually)
Taking out cyber insurance

4 Measures for regular review, assessment and evaluation

4. 1Control procedure

Measures to ensure the effectiveness of data security measures.

Processing records (Art. 30 I and II GDPR) are updated annually
Notification of new/changed data processing procedures to the data protection officer
Processes for reporting new/changed procedures are documented
Regular review and evaluation of the software used
Checking the effectiveness of security measures taken at least once a year
In the event of findings within the scope of the aforementioned. review, the safety measures are adapted in line with the risks
Process in place to respond to security breaches (attacks) and system malfunctions (incident response management)
Documentation of security incidents
Use of security intelligence (real-time analysis; log management, SIEMs, NBADs, network forensics)

4.2Order control

Is intended to ensure that data processed by service providers (subcontractors) on behalf of the client is only processed in accordance with the client's instructions.

Contract design in accordance with legal requirements (Art. 28 GDPR) *where possible*
Central recording of existing service providers (standardized contract management)
Review of existing IT security certificates of the contractors

4. 3Separation control

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Vienna
hello@heylog.com;

Measures to ensure that data collected for different purposes can be processed separately.

Separation of customers (multi-client capability of the system used)
Logical data separation (e.g. based on customer or client numbers)
Separation of development, test and production systems https://app-dev.heylog.com : **Development environment** https://staging.heylog.com/ : **Test environment** https://app.heylog.com/ : **Live environment**
Definition of database rights
Control via authorization concept

4.4 Data protection measures for the Heylog system and its development

Documented process for detecting and reporting security incidents/data breaches (also with regard to the obligation to report to the supervisory authority).
Documentation of security incidents and data breaches is sent to gdpr@heylog.com.
No more personal data is collected than is necessary for the respective purpose.
Simple exercise of the data subject's right of withdrawal by manual measures of the organization.
The effectiveness of the technical protective measures must be checked at least once a year.
Regular sensitization of employees

4.5Other data protection and security management

Appropriate organizational structure for information security with clearly defined roles
Use of data protection management software
Central documentation of all data protection procedures and regulations
Trained employees committed to confidentiality / data secrecy
General data protection and security policy
Documented process for dealing with IT security incidents
Clear responsibilities for handling data protection and security incidents
Documented process for safeguarding the rights of data subjects
Central storage of guidelines/ processes/ procedural instructions accessible to all employees
External service providers are obliged to maintain confidentiality where necessary
Regular training on the guidelines and security processes
Obligation to appoint a data protection officer by the contractor, if there is an obligation

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Vienna
hello@heylog.com;

to appoint one.

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Vienna
hello@heylog.com;