heyData

Technical and Organizational Measures

Table of Contents

1. Introduction

1.1 Controller

The controller according to Art. 4 No. 7 EU General Data Protection Regulation (GDPR) is replient.ai Software GmbH, Derflerstraße 27/1, Lichtenberg, Österreich, email: office@replient.ai. We are legally represented by Thomas Danninger, Markus Danninger.

1.2 Data Protection Officer

Our data protection officer is heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, email: datenschutz@heydata.eu.

1.3 Subject of the Document

This document summarizes the technical and organizational measures taken by the controller in accordance with Art. 32 para. 1 GDPR. These are measures that the controller uses to protect personal data. The purpose of the document is to support the controller in fulfilling their accountability obligation under Art. 5 para. 2 GDPR.

2. Confidentiality (Art. 32 para. 1 lit. b GDPR)

2.1 Entry Control

The following implemented measures prevent unauthorized entry to data processing facilities:

- Chip card/transponder locking system
- Careful selection of cleaning staff
- Instruction to employees not to work in publicly accessible spaces (e.g. cafés)

- Working from home: Instruction to employees, if possible, to work in workrooms separated from living areas

2.2 Admission control

The following implemented measures prevent unauthorized access to data processing systems:

- Authentication with username and password
- Automatic desktop lock
- General instruction to manually lock the desktop when leaving the workplace

2.3 Access control

The following implemented measures ensure that unauthorized persons do not have access to personal data:

- Logging of access to applications (especially for data entry, modification, and deletion)
- Number of administrators kept as small as possible
- Management of user rights by system administrators
- Instruction to employees that only absolutely necessary data should be printed
- Instruction to employees that data should only be deleted after consultation

2.4 Separation control

The following measures ensure that personal data collected for different purposes is processed separately:

- Separation of production and test system

Definition of database rights

3. Integrity (Art. 32 para. 1 lit. b GDPR)

3.1 Transfer control

It is ensured that personal data cannot be read, copied, altered, or removed without authorization during transmission or storage on data carriers and that it can be verified which persons or entities have received personal data. The following measures are implemented to ensure this:

- WLAN encryption (WPA2 with strong password)
- Logging of access and retrievals

3.2 Input control

The following measures ensure that it can be verified who processed personal data in data processing systems at what time:

- Logging of input, modification, and deletion of data
- Creation of an overview of which applications can enter, change, and delete which data
- Traceability of data input, modification, and deletion through individual usernames (not user groups)
- Instruction to employees to delete data only after consultation

4. Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client:

- Regular backups
- Separation of operating systems and data
- Hosting (at least the most important data) with a professional hoster

5. Procedures for regular review, assessment, and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

5.1 Data protection management

The following measures are intended to ensure that an organization meeting the basic requirements of data protection law is in place:

- Use of the heyData platform for data protection management
- Appointment of heyData as the data protection officer
- Obligation of employees to data secrecy
- Regular training of employees in data protection
- Keeping a record of processing activities (Art. 30 GDPR)

5.2 Incident-Response-Management

The following measures ensure that reporting processes are triggered in the event of data protection violations:

- Reporting process for data protection violations according to Art. 4 No. 12 GDPR to the supervisory authorities (Art. 33 GDPR)
- Reporting process for data protection violations according to Art. 4 No. 12 GDPR to the data subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches

5.3 Privacy-friendly default settings (Art. 25 para. 2 GDPR)

The following implemented measures take into account the principles of "Privacy by design" and "Privacy by default":

- Training of employees in "Privacy by design" and "Privacy by default"

- No more personal data is collected than necessary for the respective purpose.

5.4 Order control

By the following measures, it is ensured that personal data can only be processed according to instructions:

- Written instructions to the contractor or instructions in text form (e.g., via data processing agreement)
- Ensuring the destruction of data after the end of the contract, e.g., by requesting corresponding confirmations
- Confirmation from contractors that they obligate their own employees to data secrecy (typically in the data processing agreement)
- Careful selection of contractors (especially regarding data security)
- Ongoing review of contractors and their activities