Data Security Concept

Heidelberg Engineering GmbH
Max-Jarecki-Str. 8
69115 Heidelberg · Germany

Phone +49/62 21/64 63-0
Fax +49/62 21/64 63 62
www.HeidelbergEngineering.com

Technical and organizational measures

Heidelberg Engineering GmbH seeks to warrant the best possible protection of personal data at all times and has therefore taken extensive technical and organizational measures aimed at warranting a high level of data protection. An overview of these measures is provided in this document.

General information

Pursuant to Article 32 GDPR, appropriate technical and organizational measures must be implemented to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Heidelberg Engineering GmbH is guided in its technical and organizational measures by common standards such as the BSI (German abbreviation “Bundesamt für Sicherheit in der Informationstechnik”; German Federal Office for Information Technology Security) basic protection standard and ISO 27001 et seq..

The high level of protection afforded by the measures is regularly evaluated and adjusted to the current state of the art.

Employees are regularly trained in the handling of personal data and are obligated to maintain confidentiality and secrecy.

The handling of data and data processing systems is subject to written regulations (data protection policy, information security policy and work instructions) and is evaluated regularly.

Confidentiality (Article 32 para. 1 lit. b GDPR)

Entry control

Unauthorized persons must be prevented from entering premises housing data processing equipment used for the processing of personal data.

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Automatic entry control system
- Locking system with transponders
- Burglar alarm system with motion sensors and connection to a permanently manned guard service
- Key regulations
- Logging of visitors
- Regulations for external persons/visitors
- Subdivision into different security zones

Access control

Data processing systems must be prevented from being used by unauthorized persons.

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Design and implementation of an authorization concept for user devices and IT systems
- Authentication with user name and password
- Automatic enforcement of secure passwords (password policy)
- Determination and regular evaluation of access credentials
- Use of intrusion detection systems
- Encryption of mobile user devices and mobile data carriers
- Use of centrally administrated antivirus software
- Use of hardware firewall systems
- Use of VPN technology
- Monitoring of attempts to gain access
- Regulations for external persons/visitors

Data access control

It must be warranted that persons authorized to use a data processing system have access only to the personal data covered by their access authorization and that the personal data cannot be read, copied, modified or deleted by unauthorized persons during processing or after the data have been saved.

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Authorization concept for applications
- Management of credentials and user rights by system administrators with dedicated administration accounts
- Limiting the number of authorizations to what is necessary
- Logging of access to critical applications, in particular when entering, modifying and deleting data
- Secure storage of data carriers
- Physical deletion of data carriers prior to reuse
- Legally compliant destruction of data carriers (DIN 66399)
- Use of document shredders and/or certified service providers
- Written regulation governing the handling of digital storage media
- Functional limitations (in terms of time/functionality)

Data separation control

It must be warranted that personal data collected for different purposes can be processed separately.

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- For pseudonymized data (Article 32 para. 1 lit. a GDPR, Article 25 para. 1 GDPR) by separation of the mapping file and the data
- Separate storage on autonomous systems or data carriers
- Regular evaluation on conforming use of data and IT systems
- Separation of productive and test system

HEIDELBERG ENGINEERING

Heidelberg Engineering GmbH
Max-Jarecki-Str. 8
69115 Heidelberg · Germany

Phone +49/62 21/64 63-0
Fax +49/62 21/64 63 62
www.HeidelbergEngineering.com

Managing Directors
Arianna Schoess Vargas
Kfir Azoulay

Mannheim HRB 334163

Integrity (Article 32 para. 1 lit. b GDPR)

Disclosure control

It must be warranted that personal data cannot be read, copied, modified or deleted without authorization during electronic transmission or during their transport or storage on data carriers, and that it is possible to evaluate and determine to which parties a transfer of personal data is intended by means of data transmission equipment.

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Use of suitable encryption methods
- Use of VPN technology
- Disclosure of data in anonymized or pseudonymized form
- Documentation of the recipients of data, periods of intended disclosure and/or agreed deletion periods
- Measures aimed at preventing any uncontrolled information outflows

Data entry control

It must be warranted that it is possible to subsequently verify and assess whether and by whom personal data was entered, modified or deleted in data processing systems.

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Logging of data entry, modification and deletion operations
- Traceability of data entry, modification and deletion operations
- Assignment of rights to enter, modify and delete data on the basis of an authorization concept
- Preparation of an overview showing with which applications which data can be entered, changed and deleted
- Retention of forms from which data were imported into automated data processing operations

Availability and resilience (Article 32 para. 1 lit. b GDPR) and restorability in a timely manner (Article 32 para. 1 lit. c GDPR)

Availability control

It must be warranted that personal data are protected against accidental destruction or loss and that the system and services are adequately resilient.

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Uninterruptible power supply (UPS) for server rooms
- Equipment for monitoring temperature and humidity in server rooms
- Air-conditioning in server rooms
- Smoke detection systems
- Additional fire extinguishing equipment for server rooms
- Alarm signal in case of unauthorized access to server rooms
- Data backup and recovery plan
- Established incident plan
- Testing of data recovery
- Use of redundant IT systems

HEIDELBERG ENGINEERING

Heidelberg Engineering GmbH
Max-Jarecki-Str. 8
69115 Heidelberg · Germany

Phone +49/62 21/64 63-0
Fax +49/62 21/64 63 62
www.HeidelbergEngineering.com

Managing Directors
Arianna Schoess Vargas
Kfir Azoulay

Mannheim HRB 334163

Process for regularly testing, assessing and evaluating the effectiveness (Article 32 para. 1 lit. d GDPR; Article 25 para. 1 GDPR)

Data protection management

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Documentation of all data protection procedures and regulations
- Annual review of the effectiveness of technical and organizational measures
- Obligation of employees to maintain confidentiality/data secrecy and annual data protection training for employees
- External data protection officer and internal data protection coordinator in place
- Internal information security officer in place
- If required, performance of a data protection impact assessment
- Fulfillment of information obligations according to Art 13 and 14 GDPR
- Formalized processes are in place for processing requests in the context of asserting data subject rights, in particular the the right of access by the data subject

Incident response management

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Structured assessment and prioritization of reported and/or detected technical malfunctions and security incidents
- Defined internal and external communication and escalation processes

Data protection by design and by default (Article 25 GDPR)

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Systems and applications are configured and parameterized in compliance with data protection before use (“privacy by default”).
- Products are developed in adherence to the “privacy by design” principle
- Default settings of other manufacturers' products are checked and set in compliance with data protection before the first use

Contract data processing control

It must be warranted that personal data processed by a contract data processor can only be processed in accordance with the instructions of the principal.

Heidelberg Engineering GmbH ensures this by taking the following measures, among others:

- Selection of contractors under due diligence aspects (in particular with regard to data security)
- Written instructions issued to the contractors
- Agreement on effective control rights over the contractors
- Inspection and documentation of the security measures implemented at the contractor's premises
- Ensuring that the contractor's employees have been obligated to maintain data secrecy
- Ensuring the destruction of data after the completion of the contract
- Regular audit of the contractor and its activities

Heidelberg Engineering GmbH
Max-Jarecki-Str. 8
69115 Heidelberg · Germany

Phone +49/62 21/64 63-0
Fax +49/62 21/64 63 62
www.HeidelbergEngineering.com

Managing Directors
Arianna Schoess Vargas
Kfir Azoulay

Mannheim HRB 334163