General description of the technical and organizational measures according to Art. 32 GDPR (applying as from Mars 16, 2018)

Aareon has taken several measures which ensure *confidentiality*, *integrity*, *availability* and *resilience* of the systems and services related to the processing of **Personally identifiable information (PII)** for the client. *Pseudonymization* or *encryption* of PII was considered by these measures as well. The technical and organizational measures mitigate the risk at a reasonable level of protection according to the state of the art. The protection needs of at Aareon usually processed PII was considered appropriately.

These measures are related to those implemented at Aareon and at Aareon's affiliated companies part of the at Aareon established Internal Control System (ICS). Key measures are listed below.

To implement the measures described there are detailed internal concepts and rules for IT security, system security, network security, telecommunications security, security on mobile devices, cryptography and further technical and organizational measures in place. Aareon carries out regular internal controls regarding implementation and adherence to these concepts and rules.

In case of further processors acting under control of Aareon, Aareon will commit them to implement and comply with technical and organizational measures to ensure a level of protection according to the risks for affected individuals. Technical and organisational measures implemented within those further processors may differ from those listed in this document.

Confidentiality

Technical measures

1. Access to the structurally separated and electronically monitored security zones of the data center is only allowed to persons performing necessary activities in these zones. Visitors can only enter these zones under supervision of authorized persons.
2. Access to Aareon's premises is controlled through an access control system (access card to the premises and, depending on the authorization, to various security areas). Any use of a card reader is logged.
3. Outside normal working hours, video cameras coupled with motion detectors monitor access routes to parts of the building which are in need of protection.
4. Access to the applications is only possible after authentication via a user account with password that must be changed by the user after a specified interval according to the password policy. The access is restricted to each client-independent instance.
5. Logon processes are logged.
6. The applications are set up in this way that they can only be accessed by authorized users after entering a password.

7. Aareon's server systems are protected against unauthorized access from the Internet through a multi-level firewall system. Access to applications over the Internet is controlled by the firewall system and secured by additional authentication mechanisms. Access to applications over the Internet is encrypted.

Organizational measures

1. All employees dealing with personal data are sworn to secrecy.
2. There are regular training sessions on data protection and data protection.
3. Passing on passwords is prohibited.
4. The data processing areas by Aareon are divided into several security areas with differentiated access authorizations.
5. The access authorizations are controlled according to an access authorization concept.
6. The access authorizations within the applications are managed by differentiated, function-specific authorization systems.
7. The range of privileged support user accounts is limited restrictively to the necessary extent and is subject to additional protocol mechanisms.
8. By the existing authorization concept and the existing user permissions a logical separation of data which are collected for different purposes and separately processed is appropriately performed.
9. The principle of segregation of duties is adequately realized within the organizational units. Data in need of protection will only be provided to employees to the necessary extend which is determined by the assigned lawful performance of the task. To ensure this, rights profiles for the various functional areas are assigned and administered centrally.
10. Disposal items that contain sensitive content are regularly destroyed in sealed special containers, which are not accessible from the outside, by a company that is certified for such activities and subject to the statutory data protection regulations.
11. Media (tape cartridges, optical media, etc.) are kept in special security areas.
12. Transfers of personal data to third parties, state institutions and authorities, will only be performed according to law or on behalf of the client.

Integrity

Technical measures

1. Data changes are recorded including the time of entry.
2. Altering and authentication mechanisms within Aareon's network components protect Aareon-operated systems from unauthorized remote data communications.

Organizational measures

1. Procedures to ensure data security and appropriate order execution are regularly reviewed. Compliance with these operating procedures is regularly audited according to the ICS set up by Aareon.
2. Data carriers and processing results are sent in suitable containers.
3. Lines, connections and distributors for remote data transmission in the Aareon facilities are located in non-public accessible security areas.

Availability and resilience

Technical measures

1. Appropriate fire protection, loss prevention and civil protection measures have been implemented. These include the security of datacentre rooms by early fire detection, active fire prevention and extinguishing systems and a self-sufficient emergency power supply for the uninterrupted bridging of power failures.
2. A backup of application data is created at least on working days and stored in appropriate data security rooms.
3. Incoming volumes are scanned for viruses. Incoming e-mails and attachments are scanned for viruses before being transferred to the general office communication network (LAN). In addition, virus scanning programs are deployed both at the workstations of the employees and on the central servers.

Organizational measures

1. Emergency concepts for data protection and security incidents are regularly tested and improved.

Pseudonymization

Aareon did not implement any general pseudononymization measures when processing data on behalf of the client.

Encryption

Technical measures

1. Aareon uses state-of-the-art cryptographic techniques and products for encryption procedures. This applies to encryption during the transmission and storage of data as well as to the transport routes of transmitted data.

Organizational measures

1. General guidelines for the use of encryption methods are regulated in a guideline for cryptography.
2. Aareon performs a periodic review of encryption methods.

Procedures for periodic review, evaluation and evaluation of effectiveness

All systems operated by Aareon for customers themselves are subject to the ICS established at Aareon, which covers all aspects of IT and data security during operation.

Compliance as well as effectiveness of the rules defined in the ICS are regularly audited both internally and externally.

Furthermore, the Aareon Information Security Management System ISMS is regularly external audited regarding standard conformity.

In addition, Aareon is externally evaluated on a regular basis regarding privacy and audited in terms of effectiveness.

A list of current Certificates is published within our website: www.aareon.de.