Information on Data Protection according to GDPR

- Customer and their employees -

As controller in the meaning of GDPR, we take the protection of personal data seriously and process it according to the legal regulations.

1. Data processing controller according to GDPR

The Aareon company with which the client agreement has been concluded is controller for fulfilling the agreement and initiating further business relations. The Aareon Group companies are also joint controllers for marketing measures (e.g. invitations to events, surveys).

- Aareon Sverige AB, Flöjelbergsgatan 10, 431 37 Mölndal, e-mail: info@aareon.se
- Aareon Norge AS - c/o Spaces Kvadraturen, Tollbugata 8, 0152 Oslo, Norge, e-mail: info@aareon.se

The joint controllers have concluded an agreement according to which the data of interested parties will be used by Aareon Sverige AB for marketing measures (e.g. invitations to events, surveys). For customers and their employees of both the above companies is the main office for determining the lead supervisory authority.

2. Contact with the Data Protection Officer

- For both companies: dataskyddsombud@aareon.com

3. Purpose and Lawfulness of Processing

Execution of the customer relationship and fulfillment of contract according to Art. 6 Abs. 1 b) GDPR. Business initiation as well as marketing with a legitimate interest according to Art. 6 para. 1 f) for business initiation as well as marketing and/or consent according to Art. 6 para. 1 a) GDPR. Data subjects may oppose to the legitimate interest and revoke consent at any time.

4. Data and Categories of Data

Customers (as far as natural persons)	Name + name affixes (Mr/Mrs, academic title)
	Address
	Contact details (phone, fax, email)
	Costumer number
	Bank account
	Contract data
	Creditworthiness data
	Support information, incl. customer development and previous contacts
	Product or contractual interest (for upselling)

	Data on opt-in or opt-out for marketing measures (declared consent to advertising notifications and other advertising measures, registration for newsletters, advertising objections)
	Photographic picture
	Billing and payment data
	Data for identification of economic beneficiaries according to the Money Laundering Act, if applicable
	Videos (recorded at events)
Employees of Customers	Name + name affixes (Mr/Mrs, academic title)
	Address
	Contact details (phone, fax, email)
	Bank account (travel expenses)
	Date of birth
	Contents (participation in workshops and training courses, substantive statements e.g. error messages, acceptances, instructions, concretizations)
	Data on opt-in or opt-out for marketing measures (declared consent to advertising notifications and other advertising measures, registration for newsletters, advertising objections)
	Photographic picture
	Videos (recorded at events)

5. Recipient and Categories of Recipients

Relevant employees of involved departments and associated companies, processors. Aareon uses Microsoft® Office applications (e.g. Word®, Outlook®), where support can be provided with possible access to data from outside the EU/EEA. Microsoft support is governed by the standard EU contractual clauses, which are available in the Microsoft Trust Center.

For a customer solution with Microsoft® Office 365, the following applies: If the data is hosted in the Microsoft Azure Cloud or Microsoft Support is provided, it may be possible to access data from outside the EU/EEA. For this purpose, EU standard contractual clauses apply via the Microsoft Customer Agreement and are available in the Microsoft Trust Center.

Aareon is obliged to cooperate in the fight against terrorism and carries out a data comparison with EU/US anti-terror lists and in UK also the UK anti-terror lists (sanction screening). The comparison is performed regarding the customer, not its employees. Aareon uses the AEB system for this purpose, for which support can be provided from outside the EU/EEA (UK, Singapore) if required. The UK is considered a safe third country in accordance with the EU Commission's adequacy decision, and EU standard contractual clauses apply to support from Singapore. In the case of international data transfer to or access from outside the EU, there are special risks for personal data (e.g. access by foreign intelligence agencies).

6. Storage Period

The data will be stored in compliance with the legal retention periods up to 10 years after termination of the customer relationship or performance of the sanction screening. Data that is no longer needed will be deleted. Data based on a consent will be stored until revocation. Data based on a legitimate interest will be stored for as long as the legitimate interest exists, until objection or at the latest until 6 years after the last contact with the company or the data subject.

7. Data Subject Rights

The data subject has the right of access from the controller about the personal data, rectification, erasure, restriction of processing, revocation or objection for the future, data portability and appeal to a supervisory authority.

Status 17 February 2022