

Technical and organisational measures to ensure data security

Introductory remarks

This document describes the technical and organisational measures implemented by AIRAdoc GmbH to protect personal data under the joint controller agreement with its customers. These measures serve to comply with the requirements of Article 25(1) and (2), Article 32(1), (2) and (4), and Article 5 GDPR. For the technical context, reference should be made to the functional description of the AIRAdoc software in the General Terms and Conditions.

1. Principles of data processing

Under its joint controllership with the customer, AIRAdoc processes personal data, including special categories of personal data.

Taking into account the state of the art, implementation costs and the nature, scope, context and purposes of processing, AIRAdoc assesses the risks to the rights and freedoms of natural persons. In particular, AIRAdoc considers the likelihood and severity of these risks and implements appropriate technical and organisational measures both when determining the means of processing and during processing. These measures are intended to implement data protection principles effectively, provide the necessary safeguards and protect the rights of data subjects.

Despite these analyses and security measures, complete security in the processing of personal data cannot be guaranteed.

The AIRAdoc software is hosted by a processor of AIRAdoc GmbH. Under the processing agreement between AIRAdoc GmbH and the hosting provider, the hosting provider is responsible for meeting certain requirements mentioned above. The specific allocation of responsibilities is set out in the following sections of this document. High security standards were considered when selecting the hosting provider. Its Information Security Management System complies with the internationally recognised ISO 27001 certification.

2. Compliance with the principles relating to processing of personal data under Article 5 GDPR

a. Lawfulness, fairness and transparency under Article 5(1)(a) GDPR

By virtue of its technical design, the AIRAdoc software can only support processing of personal data to which the customer agreed in the General Terms and Conditions when the software was provided, or which follows directly from that processing from a technical perspective.

b. Purpose limitation under Article 5(1)(b) GDPR

By virtue of its technical design, the AIRAdoc software can only support processing of personal data to which the controller agreed in the General Terms and Conditions when the software was provided, or which follows directly from that processing from a technical perspective.

c. Data minimisation under Article 5(1)(c) GDPR

AIRAdoc processes only personal data provided by the customer. By transmitting text data, the customer is assumed to consider that data necessary for AIRAdoc to perform its tasks. This also applies in principle to audio recordings transmitted. However, these may also contain personal data that is not relevant to AIRAdoc's tasks. To avoid loss of information that could restrict functionality, AIRAdoc processes audio recordings in full, prioritising accuracy and, in particular, completeness of the data.

d. Accuracy under Article 5(1)(d) GDPR

The customer controls the personal data transmitted to AIRAdoc and is responsible for its accuracy. New representations of personal data generated by AIRAdoc are saved permanently only after manual review by the customer. All technically necessary representations of this data before manual confirmation are clearly identified as such both internally and to the customer.

e. Storage limitation under Article 5(1)(e) GDPR

Personal data processed by AIRAdoc under its joint controllership with the customer is completely deleted from the system no later than 90 days after it is first processed. This period is based on experience. The aim is to delete data as early as possible, but not while it can realistically be assumed that the customer still needs access to it. The customer can also manually initiate the deletion of selected data at any time. Upon expiry or termination of the software provision contract, all personal data processed by AIRAdoc under its joint controllership with the customer is deleted.

f. Integrity and confidentiality under Article 5(1)(f) GDPR

The measures described in section 4 of this document ensure the integrity and confidentiality of AIRAdoc's processing of personal data.

3. Data protection by default under Article 25(2) GDPR**a. Minimising the amount of personal data collected under Article 25(2), first and second subparagraphs, GDPR**

See 2.c.

b. Minimising the extent of processing of personal data under Article 25(2), first and second subparagraphs, GDPR

In accordance with section 2.b, AIRAdoc's processing of personal data is strictly limited to its purposes. All processing serves to ensure the software's functionality in performing the tasks agreed between AIRAdoc and the customer and meeting the necessary quality standards, as well as the required security and data protection standards.

c. Minimising the storage period of personal data under Article 25(2), first and second subparagraphs, GDPR

See 2.e.

d. Minimising the accessibility of personal data under Article 25(2), first to third subparagraphs, GDPR

For the accessibility of personal data to AIRAdoc, see section 4.a. AIRAdoc does not enable the dissemination of personal data beyond the respective customer's user account. Use of the software requires that personal data can be exported quickly via the user interface. The handling of exported personal data is solely the customer's responsibility.

4. Security of processing under Article 32 GDPR

a. Pseudonymisation and encryption under Article 32(1)(a) GDPR

As linking personal data to specific patients is an important part of AIRAdoc's functionality, the data displayed to the user is not pseudonymised. During storage, however, data is pseudonymised to prevent attribution to the data subject as far as technically possible. All personal data is encrypted at rest using RSA and user-specific keys. The entire infrastructure communicates via a private subnet accessible only through one port for the frontend. The data flow over this connection is encrypted using TLS. The flow of personal data within the subnet is also encrypted using TLS.

b. Confidentiality, integrity, availability and resilience under Article 32(1)(b) GDPR

i. Confidentiality

Physical access control: The hosting provider ensures physical access control at hardware level in accordance with the highest standards under the GDPR.

System access control: The hosting provider ensures system access control at hardware level in accordance with the highest standards under the GDPR. The AIRAdoc software itself is protected by user identification with a username and password, with minimum password complexity requirements. All data traffic between users and servers is encrypted using TLS.

Data access control: The hosting provider ensures data access control at hardware level in accordance with the highest standards under the GDPR. Within AIRAdoc, user permissions and clear separation of data structures ensure that only the original controller responsible for processing the personal data has access to it. As far as technically possible, no persons at AIRAdoc have access to unencrypted and non-pseudonymised personal data.

Separation control: Data from different organisations is never aggregated. Within an organisation, its administrator can view metadata about the use of the software by members of that organisation. No personal data is shared in this process. Clear access controls ensure that such data remains accessible only to the respective responsible user.

ii. Integrity

Retention, destruction and disclosure: The hosting provider ensures appropriate measures for the retention, destruction and disclosure of personal data at hardware level in accordance with the highest standards under the GDPR. At AIRAdoc, disclosure of data is based solely on the customer's deliberate decision to export it. Automatic dissemination is not possible. All personal data is stored for the shortest possible period and then deleted.

Input control: The hosting provider ensures input control at hardware level in accordance with the highest standards under the GDPR. At AIRAdoc, every input is secured through user authentication and encrypted using TLS.

c. Availability

The hosting provider ensures availability control at hardware level in accordance with the highest standards under the GDPR. AIRAdoc's availability is regularly checked through manual tests, and system functionality is monitored automatically.

d. Resilience

The hosting provider ensures appropriate resilience at hardware level in accordance with the highest standards under the GDPR. AIRAdoc regularly performs tests under the real system load that can reasonably be expected.

e. Ability to restore under Article 32(1)(c) GDPR

The hosting provider ensures the ability to restore at hardware level in accordance with the highest standards under the GDPR. All databases are backed up daily. Backups are retained on a rolling basis for seven days and can be retrieved quickly at any time. AIRAdoc also regularly performs restoration tests and has contingency plans for failures of different system components.

f. Testing procedures under Article 32(1)(d) GDPR

AIRAdoc regularly performs technical testing procedures such as encryption checks and penetration tests. For organisational control, we use audit logs, access controls, regular internal audits and continuous monitoring of security-related events. External audits and certifications of the hosting provider also ensure compliance with the GDPR and high security standards.

g. Control of processing on behalf of AIRAdoc

AIRAdoc ensures that the processors it uses process personal data on behalf of AIRAdoc GmbH only in accordance with its instructions. Subprocessors are selected after careful review. Before commissioning them, we examine their documentation and security measures.

AIRAdoc concludes the necessary data processing agreements with the processor, incorporating the European Union's Standard Contractual Clauses.

AIRAdoc issues written instructions to the processor and agrees rights of inspection with it. AIRAdoc also ensures that the processor deletes the data after the engagement ends.

h. Processing under instructions under Article 32(4) GDPR

All employees of AIRAdoc GmbH are required to comply with the GDPR and maintain confidentiality. The relevant provisions are reviewed regularly.