Technical and organizational measures, including those to ensure data security

Introductory remarks

This document describes the technical and organizational measures taken by the processor in the context of the DPA between AIRAdoc GmbH (processor) and its customers (controllers) to ensure the security of personal data in accordance with Art. 25 (1) and (2) GDPR and Art. 32 (1), (2), and (4) GDPR and to comply with the data protection principles in accordance with Art. 5 GDPR. For the technical context of this document, please refer to the functional description of the AIRAdoc software in the General Terms and Conditions.

1. Basics of data processing

The processor processes personal data on behalf of the controller, including special categories of personal data.

Taking into account the state of the art, the implementation costs, and the nature, scope, circumstances, and purposes of the processing, as well as the varying likelihood and severity of the risks associated with the processing for the rights and freedoms of natural persons, the processor shall implement appropriate technical and organizational measures, both at the time of determining the means for processing and at the time of the processing itself, designed to effectively implement data protection principles and incorporate the necessary safeguards into the processing to meet the requirements of the GDPR and protect the rights of data subjects.

Despite these analyses and the security measures derived from them, complete security of personal data processing can never be guaranteed.

The processor's AIRAdoc software is hosted by Microsoft Ireland Operations Limited (host). Under the data processing agreement concluded between the processor and the host as a sub-processor, the host is responsible for fulfilling some of the standards mentioned in the introduction. The specific division of tasks can be found in the rest of this document. The host was selected taking into account the highest security standards.

security standards. The host's information security management system complies with the internationally recognized ISO 27001 certification.

2. Compliance with the principles of personal data processing in accordance with Art. 5 GDPR

a. Lawfulness, processing in good faith, and transparency in accordance with Art. 5 (1) (a) GDPR

   The AIRAdoc software is designed to only support the processing of personal data that the controller has agreed to in the general terms and conditions when providing the software or that is necessary from a technical point of view directly resulting from this processing.

b. Purpose limitation in accordance with Art. 5 (1) (b) GDPR

   The AIRAdoc software is designed to only support the processing of personal data that the controller has agreed to in the general terms and conditions when providing the software or that is necessary from a technical perspective as a direct result of this processing.

c. Data minimization in accordance with Art. 5 (1) (c) GDPR

   The processor only processes personal data provided by the controller. By transmitting text data, it can be assumed that the controller considers this data to be necessary for the performance of the processor's tasks. The same applies in principle to transmitted audio data, although it cannot be ruled out that this may also contain personal data that is irrelevant to the performance of the processor's tasks. At this point, the processor prioritizes the accuracy and, in particular, the completeness of the data by processing the entirety of the audio data in order to prevent any loss of information that could potentially restrict functionality.

d. Accuracy in accordance with Art. 5 (1) (d) GDPR

   The controller has control over the personal data it passes on to the processor and is therefore responsible for ensuring its accuracy. New representations of personal data generated by the processor are only finally stored after manual verification by the controller. All representations of this data that are necessary from a technical point of view prior to manual confirmation are clearly marked as such internally and to the controller.

e. Storage limitation in accordance with Art. 5 (1) (e) GDPR

   Personal data processed by the processor on behalf of the controller will be completely deleted from the system no later than 90 days after the first processing.
   This period is based on experience and aims to delete the data as early as possible, but not while it can realistically be expected that the controller still needs access to the data. Furthermore, the controller has the option of manually initiating the deletion of selected data at any time. Upon expiry or termination of the contract for the provision of the software, all personal data processed by the processor on the instructions of the controller will be deleted.

f. Integrity and confidentiality in accordance with Art. 5 (1) (f) GDPR

   The measures described in section 4 of this document ensure the integrity and confidentiality of the processing of personal data by the processor.

3. Privacy-friendly default settings in accordance with Art. 25 (2) GDPR

a. Minimization of the amount of personal data collected in accordance with Art. 25 (2) subparagraphs 1 and 2 GDPR

   See 2.c.

b. Minimization of the scope of processing of personal data in accordance with Art. 25 para. 2 subparagraphs 1 and 2 GDPR

   In accordance with 2.b., the processing of personal data by the processor is strictly limited to the specified purpose. Any processing of the data serves to ensure the functionality of the software for the fulfillment of the tasks assigned to the processor by the controller and the quality standards required for this, as well as the fulfillment of the necessary security and data protection standards.

c. Minimization of the storage period for personal data in accordance with Art. 25 (2) subparagraphs 1 and 2 GDPR

   See 2.e.

d. Minimization of the accessibility of personal data in accordance with Art. 25 (2) subparagraphs 1-3 GDPR

   For the accessibility of personal data for the processor, see 4.a. AIRAdoc does not allow the dissemination of personal data beyond the

user account of the respective controller. In order to use the software, it is necessary to be able to quickly copy personal data from the user interface. However, the controller is solely responsible for the handling of the personal data exported in this way.

4. Security of processing in accordance with Art. 32 GDPR

a. Pseudonymization and encryption in accordance with Art. 32 (1) (a) GDPR

   Since the assignment of personal data to specific patients is an important part of AIRAdoc's functionality, the data displayed is not pseudonymized for the user. However, when the data is stored, it is pseudonymized in order to prevent assignment to the data subject as far as technically possible. All personal data is encrypted at rest using RSA with user-specific keys. The entire infrastructure communicates via a private subnet that is only open to the front end via one port. The data flow via this connection is encrypted with TLS. Within the subnet, the flow of personal data is also encrypted with TLS.

b. Confidentiality, integrity, availability, and resilience in accordance with Art. 32 (1) (b) GDPR
   i. Confidentiality
      - Access control: The host ensures access control at the hardware level in accordance with the highest standards under the GDPR.
      - Access control: The host ensures access control at the hardware level in accordance with the highest standards of the GDPR. The AIRAdoc software itself is secured by user identification with a user ID and password, with requirements for minimum password complexity. All data traffic between users and servers is encrypted with TLS.
      - Access control: The host ensures access control at the hardware level in accordance with the highest standards of the GDPR. Within AIRAdoc, user authorizations and a clear separation of data structures ensure that only the original controller responsible for processing personal data has access to it. On the part of the processor, no persons have access to unencrypted and non-pseudonymized personal data, as far as technically possible.
      - Separation control: At no time is data from different organizations aggregated. Within an organization, its administrator has the option of viewing metadata about the use of the software by the members of his or her organization. However, no

personal data is shared. This data remains accessible only to the responsible user through clear access control.

ii. Integrity
- Storage, destruction, and disclosure: The host ensures appropriate measures for the storage, destruction, and disclosure of personal data at the hardware level in accordance with the highest standards under the GDPR. At AIRAdoc, data disclosure is based solely on the conscious decision of the responsible person to copy the data. Automatic distribution is not possible. All personal data is stored for the shortest possible time and then deleted.
- Input control: The host ensures input control at the hardware level in accordance with the highest standards of the GDPR. At AIRAdoc, every input is secured by user authentication and encrypted via TLS.

iii. Availability

The host ensures availability control at the hardware level in accordance with the highest standards of the GDPR. The availability of AIRAdoc is regularly ensured through manual tests, and there is automatic monitoring of system functionality.

iv. Resilience

The host ensures adequate resilience at the hardware level in accordance with the highest standards under the GDPR. The processor regularly conducts tests under the assumed real system load.

c. Recoverability in accordance with Art. 32 (1) (c) GDPR

The host ensures recoverability at the hardware level in accordance with the highest standards under the GDPR. Daily backups of all databases are performed, which are stored cyclically for 7 days and can be quickly retrieved at any time. Furthermore, the processor regularly performs recoverability tests and has contingency plans in place for the failure of various system components.

d. Audit procedures in accordance with Art. 32 (1) (d) GDPR
   i. Control processes

The processor regularly performs technical testing procedures such as encryption checks and penetration tests. Audit logs, access controls, and regular internal audits are used for organizational control, as well as continuous monitoring of security-related events. External audits and certifications of the host also ensure compliance with the GDPR and high security standards.

ii. Order control

For subcontractors employed by the processor, it is ensured that the processing of personal data on behalf of the processor is carried out only in accordance with the processor's instructions as the client. Subcontractors are selected with due care. To this end, the subcontractor's documentation and security measures are checked before the order is placed.

The processor shall conclude the necessary agreements with the sub-processor for order processing, including the
standard contractual clauses of the European Union.

The processor provides written instructions to the sub-processor and agrees on control rights with them. Furthermore, they ensure that the data is deleted by the sub-processor after completion of the order.

e. Binding instructions in accordance with Art. 32 (4) GDPR

All employees of the processor are obliged to comply with the provisions of the GDPR and to maintain confidentiality. The applicable regulations for employees are monitored on an ongoing basis.