# Agreement on the Processing of Personal Data

pursuant to Art. 26 General Data Protection Regulation – GDPR

between

AIRAdoc GmbH
Am Biopark 13
93053 Regensburg
(Processor)

and

**Controller – Name / Company**

**Controller – Address / Contact details**

(Controller)

## § 1 Subject Matter and Duration of the Processing (Art. 28(3) sentence 1 GDPR)

(1) The subject matter of the processing is the Processor's remote access to the AIRAdoc software made available to the Controller for the purposes of maintenance and product personalisation.

(2) The processing shall continue for the duration of the underlying main agreement for the provision of the AIRAdoc software. Termination of the main agreement shall also terminate this agreement.

(3) The Processor shall process personal data exclusively on the instructions of and on behalf of the Controller and in accordance with documented instructions (Art. 28(3)(a) GDPR), including with regard to transfers to third countries, unless the Processor is required to process the data under Union law or the law of a Member State. In such a case, the Processor shall inform the Controller of those legal requirements before processing.

| Specification | Content |
|---|---|
| Type of processing | Reading, deleting and modifying settings for the personalisation of AIRAdoc |
| Purpose | Improving product functionalities |
| Categories of data subjects | The Controller and members of the Controller's organisation in AIRAdoc. The processing does not include access to the Controller's patient data. |
| Categories of personal data | User settings |
| Special categories (Art. 9 GDPR) | none |
| Transfer to third countries | none |

## § 2 Nature, Purpose and Scope of the Processing

Particularly important for persons bound by professional secrecy: If service providers are engaged who gain access to secrets protected under § 203 of the German Criminal Code (StGB) (e.g. IT maintenance in a medical practice or law firm), they must be expressly bound to confidentiality under § 203(4) StGB and instructed about the criminal liability of a breach of secrecy (see § 5(2)).

## § 3 Obligations of the Processor

The Processor shall in particular undertake to:

- Confidentiality (lit. b): ensure that the persons authorised to process the data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality;
- Security (lit. c): implement all measures required under Art. 32 GDPR;
- Sub-processing (lit. d): comply with the requirements of § 4;
- Assistance with data subject rights (lit. e): assist the Controller, through appropriate technical and organisational measures, in responding to requests from data subjects under Chapter III GDPR; the Processor shall forward data subject requests to the Controller without undue delay and shall not answer them itself;
- Assistance under Arts. 32–36 (lit. f): assist the Controller in complying with obligations relating to data security, notification of personal data breaches, communication with data subjects, data protection impact assessments and prior consultation;
- Return or deletion (lit. g): after completion of the services, return or delete all personal data at the Controller's choice and destroy existing copies, unless a statutory retention obligation applies (see § 7 for details);
- Evidence and audits (lit. h): make available to the Controller all information necessary to demonstrate compliance and allow for and contribute to audits, including inspections;
- Duty to notify: inform the Controller without undue delay if the Processor believes that an instruction infringes the GDPR or other data protection provisions (Art. 28(3), sentence 3 GDPR).

## § 4 Sub-processors (Art. 28(2) and (4) GDPR)

(1) The Controller hereby grants a general authorisation for the engagement of further processors. The sub-processors engaged at the time of conclusion of the agreement are set out in the information provided by the Processor.

(2) In the event of intended changes (addition or replacement), the Processor shall inform the Controller at least seven days in advance in text form. The Controller may object within fourteen days; in the event of a justified objection, the Controller shall have a special right of termination.

(3) The Processor shall contractually impose on each sub-processor the same data protection obligations as those set out in this agreement. The Processor shall be liable to the Controller for the sub-processor's compliance with these obligations.

## § 5 Instructions, Confidentiality and Training

(1) Instructions shall generally be issued in text form. Oral instructions must be confirmed in text form without undue delay. All AIRAdoc users are authorised to issue instructions.

(2) The Processor shall oblige the persons involved in the processing to maintain confidentiality. Where secrets within the meaning of § 203 StGB are concerned, an additional express obligation under § 203(4) StGB shall be imposed, including instruction on the criminal liability for a breach of secrecy.

(3) The persons involved shall receive regular training on data protection and data security, at least once a year. The training shall be documented.

## § 6 Notification of Personal Data Breaches

The Processor shall notify the Controller of any personal data breach without undue delay after becoming aware of it, and no later than within 24 hours (Art. 33(2) GDPR). The notification shall contain at least: the nature of the breach, the categories of data affected and the approximate number of data subjects, the likely consequences, and the measures taken or proposed.

The 72-hour period under Art. 33(1) GDPR for notification to the supervisory authority applies to the Controller and begins when the Controller becomes aware of the breach. A short notification period for the Processor is therefore essential in practice.

## § 7 Termination: Return and Deletion

(1) Upon termination of the processing, the Processor shall, at the Controller's choice, return all personal data or delete it in a data protection-compliant manner; the same shall apply to copies and backup copies.

(2) Deletion shall be completed within thirty days and confirmed in writing upon request.

(3) Documentation that serves to demonstrate proper data processing may be retained beyond the end of the agreement in accordance with the applicable retention periods.

## § 8 Liability and Final Provisions

(1) Liability shall be governed by Art. 82 GDPR.

(2) Amendments and supplements must be made in text form. This shall also apply to any waiver of this formal requirement.

(3) If any provision is or becomes invalid, the validity of the remaining provisions shall remain unaffected.

(4) The law of the Federal Republic of Germany shall apply.