

TOMs

Technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit

Einleitende Bemerkungen

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen, die die AIRAdoc GmbH im Rahmen der Vereinbarung über gemeinsame Verantwortlichkeit mit ihren Kunden zum Schutz personenbezogener Daten umsetzt. Sie dienen der Einhaltung der Anforderungen aus Art. 25 Abs. 1 und 2, Art. 32 Abs. 1, 2 und 4 sowie Art. 5 DSGVO. Für den technischen Kontext ist die Funktionsbeschreibung der Software AIRAdoc in den Allgemeinen Geschäftsbedingungen heranzuziehen.

1. Grundlagen der Datenverarbeitung

AIRAdoc verarbeitet im Rahmen der gemeinsamen Verantwortlichkeit mit dem Kunden personenbezogene Daten, darunter auch besondere Kategorien personenbezogener Daten.

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung bewertet AIRAdoc die Risiken für die Rechte und Freiheiten natürlicher Personen. Dabei berücksichtigt AIRAdoc insbesondere die Wahrscheinlichkeit und Schwere dieser Risiken und trifft sowohl bei der Festlegung der Verarbeitungsmittel als auch während der Verarbeitung geeignete technische und organisatorische Maßnahmen. Diese Maßnahmen sollen die Datenschutzgrundsätze wirksam umsetzen, die erforderlichen Garantien schaffen und die Rechte der betroffenen Personen schützen.

Trotz dieser Analysen und Sicherheitsmaßnahmen kann eine vollständige Sicherheit der Verarbeitung personenbezogener Daten nicht garantiert werden.

Die Software AIRAdoc wird von einem Auftragsverarbeiter der AIRAdoc GmbH gehostet. Im Rahmen des zwischen der AIRAdoc GmbH und dem Hoster geschlossenen Auftragsverarbeitungsvertrags ist der Hoster für die Erfüllung bestimmter der zuvor genannten Anforderungen verantwortlich. Die konkrete Aufgabenteilung ergibt sich aus den weiteren Abschnitten dieses Dokuments. Bei der Auswahl des Hosters wurden hohe Sicherheitsstandards berücksichtigt. Das Information Security Management System des Hosters entspricht der international anerkannten ISO 27001-Zertifizierung.

2. Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten nach Art. 5 DSGVO

a. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz nach Art. 5 Abs. 1 lit. a DSGVO

Aufgrund ihrer technischen Ausgestaltung kann die Software AIRAdoc nur solche Verarbeitungen personenbezogener Daten unterstützen, denen der Kunde im Rahmen der Allgemeinen Geschäftsbedingungen bei Bereitstellung der Software zugestimmt hat oder die sich aus technischer Sicht unmittelbar daraus ergeben.

b. Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO

Aufgrund ihrer technischen Ausgestaltung kann die Software AIRAdoc nur solche Verarbeitungen personenbezogener Daten unterstützen, denen der Verantwortliche im Rahmen der Allgemeinen Geschäftsbedingungen bei Bereitstellung der Software zugestimmt hat oder die sich aus technischer Sicht unmittelbar daraus ergeben.

c. Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO

AIRAdoc verarbeitet ausschließlich vom Kunden bereitgestellte personenbezogene Daten. Durch die Übermittlung von Textdaten ist anzunehmen, dass der Kunde diese als für die Erfüllung der Aufgaben von AIRAdoc erforderlich ansieht. Gleiches gilt grundsätzlich für übermittelte Audioaufnahmen. Diese können jedoch auch für die Erfüllung der Aufgaben von AIRAdoc nicht relevante personenbezogene Daten enthalten. Um einen möglicherweise funktionseinschränkenden Informationsverlust zu vermeiden, verarbeitet AIRAdoc die Audioaufnahmen vollständig und priorisiert dabei die Richtigkeit und insbesondere die Vollständigkeit der Daten.

d. Richtigkeit nach Art. 5 Abs. 1 lit. d DSGVO

Der Kunde hat die Kontrolle über die von ihm an AIRAdoc übermittelten personenbezogenen Daten und ist für deren Richtigkeit verantwortlich. Neue Darstellungen personenbezogener Daten, die von AIRAdoc erzeugt werden, werden erst nach manueller Kontrolle durch den Kunden endgültig abgespeichert. Alle aus technischer Sicht notwendigen Darstellungen dieser Daten vor der manuellen Bestätigung sind intern und dem Kunden gegenüber eindeutig als solche gekennzeichnet.

e. Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO

Von AIRAdoc im Rahmen der gemeinsamen Verantwortlichkeit mit dem Kunden verarbeitete personenbezogene Daten werden spätestens 90 Tage nach der ersten Verarbeitung vollständig aus dem System gelöscht. Diese Frist basiert auf Erfahrungswerten. Ziel ist es, die Daten so früh wie möglich zu löschen, jedoch nicht so lange, wie realistischerweise davon auszugehen ist, dass der Kunde noch Zugang zu den Daten benötigt. Ferner hat der Kunde jederzeit die Möglichkeit, die Löschung ausgewählter Daten manuell zu veranlassen. Bei Ablauf oder Kündigung des Vertrags über die Bereitstellung der Software werden alle personenbezogenen Daten gelöscht, die AIRAdoc im Rahmen der gemeinsamen Verantwortlichkeit mit dem Kunden verarbeitet hat.

f. Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f DSGVO

Die unter Punkt 4. dieses Dokuments beschriebenen Maßnahmen stellen die Integrität und Vertraulichkeit der Verarbeitung personenbezogener Daten durch AIRAdoc sicher.

3. Datenschutzfreundliche Voreinstellungen nach Art. 25 Abs. 2 DSGVO

a. Minimierung der Menge der erhobenen personenbezogenen Daten nach Art. 25 Abs. 2 Unterabsätzen 1 und 2 DSGVO

Siehe 2.c.

b. Minimierung des Umfangs der Verarbeitung von personenbezogenen Daten nach Art. 25 Abs. 2 Unterabsätzen 1 und 2 DSGVO

Entsprechend Abschnitt 2.b ist die Verarbeitung der personenbezogenen Daten durch AIRAdoc streng zweckgebunden. Jegliche Verarbeitung der Daten dient der Sicherstellung der Funktionalität der Software zur Erfüllung der zwischen AIRAdoc und dem Kunden vereinbarten Aufgaben und der dafür erforderlichen Qualitätsstandards sowie der Erfüllung der nötigen Sicherheits- und Datenschutzstandards.

c. Minimierung der Speicherfrist der personenbezogenen Daten nach Art. 25 Abs. 2 Unterabsätzen 1 und 2 DSGVO

Siehe 2.e.

d. Minimierung der Zugänglichkeit der personenbezogenen Daten entsprechend Art. 25 Abs. 2 Unterabsätze 1 bis 3 DSGVO

Für die Zugänglichkeit der personenbezogenen Daten für AIRAdoc siehe Abschnitt 4.a. AIRAdoc ermöglicht keine Verbreitung personenbezogener Daten über das Nutzerkonto des jeweiligen Kunden hinaus. Für die Nutzung der Software müssen personenbezogene Daten schnell über die Benutzeroberfläche exportiert werden können. Der Umgang mit den exportierten personenbezogenen Daten liegt allein in der Verantwortung des Kunden.

4. Sicherheit der Verarbeitung nach Art. 32 DSGVO

a. Pseudonymisierung und Verschlüsselung nach Art. 32 Abs. 1 lit. a DSGVO

Da eine Zuordnung personenbezogener Daten zu konkreten Patienten ein wichtiger Bestandteil der Funktionalität von AIRAdoc ist, wird für den Nutzer keine Pseudonymisierung der angezeigten Daten vorgenommen. Bei der Datenspeicherung werden die Daten jedoch pseudonymisiert, um im Rahmen des technisch Möglichen eine Zuordnung zur betroffenen Person zu verhindern. Alle personenbezogenen Daten sind im Ruhezustand mit RSA und nutzerspezifischen Schlüsseln verschlüsselt. Die gesamte Infrastruktur kommuniziert über ein privates Subnetz, das nur über einen Port für das Frontend zugänglich ist. Der Datenfluss über diese Verbindung ist mit TLS verschlüsselt. Innerhalb des Subnetzes ist der Fluss personenbezogener Daten ebenfalls mit TLS verschlüsselt.

b. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit nach Art. 32 Abs. 1 lit. b DSGVO

i. Vertraulichkeit

- Zutrittskontrolle: Der Hoster stellt nach höchsten Standards entsprechend DSGVO eine Zutrittskontrolle auf Hardware-Ebene sicher.
- Zugangskontrolle: Der Hoster stellt nach höchsten Standards entsprechend DSGVO eine Zugangskontrolle auf Hardware-Ebene sicher. Die Software AIRAdoc selbst ist durch eine Nutzeridentifikation mit Benutzerkennung und Passwort gesichert, wobei Anforderungen an die Mindestkomplexität des Passworts gestellt sind. Jeglicher Datenverkehr zwischen Nutzer und Servern ist dabei mit TLS verschlüsselt.
- Zugriffskontrolle: Der Hoster stellt nach höchsten Standards entsprechend DSGVO eine Zugriffskontrolle auf Hardware-Ebene sicher. Innerhalb von AIRAdoc ist durch Nutzerberechtigungen und eine klare Trennung von Datenstrukturen eindeutig gewährleistet, dass nur der ursprüngliche Verantwortliche für die Verarbeitung der personenbezogenen Daten auch Zugriff auf diese hat. Seitens AIRAdocs haben im Rahmen des technisch Möglichen keine Personen Zugriff auf die unverschlüsselten und nicht-pseudonymisierten personenbezogenen Daten.
- Trennungskontrolle: Zu keinem Zeitpunkt findet eine Aggregation der Daten verschiedener Organisationen statt. Innerhalb einer Organisation hat deren Administrator die Möglichkeit, Metadaten über die Nutzung der Software durch die Mitglieder seiner Organisation einzusehen. Hierbei werden jedoch keinerlei personenbezogene Daten geteilt. Diese bleiben durch eindeutige Zugangskontrolle nur dem jeweils verantwortlichen Nutzer zugänglich.

ii. Integrität

- Aufbewahrung, Vernichtung und Weitergabe: Der Hoster stellt nach höchsten Standards entsprechend DSGVO angemessene Maßnahmen zur Aufbewahrung, Vernichtung und Weitergabe personenbezogener Daten auf Hardware-Ebene sicher. Bei AIRAdoc beruht die Datenweitergabe alleine auf der bewussten Entscheidung des Kunden durch Export der Daten. Eine automatische Verbreitung ist nicht möglich. Alle personenbezogenen Daten werden für die kürzestmögliche Zeit gespeichert und anschließend gelöscht.

- Eingabekontrolle: Der Hoster stellt nach höchsten Standards entsprechend DSGVO eine Eingabekontrolle auf Hardware-Ebene sicher. Bei AIRAdoc wird jede Eingabe durch Nutzerauthentifizierung gesichert und über TLS verschlüsselt.

c. Verfügbarkeit

Der Hoster stellt nach höchsten Standards entsprechend DSGVO eine Verfügbarkeitskontrolle auf Hardware-Ebene sicher. Die Verfügbarkeit von AIRAdoc wird regelmäßig durch manuelle Tests sichergestellt und es existiert eine automatische Überwachung der Systemfunktionalität.

d. Belastbarkeit

Der Hoster stellt nach höchsten Standards entsprechend DSGVO eine angemessene Belastbarkeit auf Hardware-Ebene sicher. AIRAdoc führt regelmäßig Tests unter der anzunehmenden realen Systembelastung durch.

e. Wiederherstellbarkeit nach Art. 32 Abs. 1 lit. c DSGVO

Der Hoster stellt nach höchsten Standards entsprechend DSGVO die Wiederherstellbarkeit auf Hardware-Ebene sicher. Es finden tägliche Backups aller Datenbanken statt, die zyklisch für sieben Tage aufbewahrt werden und jederzeit schnell abgerufen werden können. Des Weiteren führt AIRAdoc regelmäßig Tests zur Wiederherstellbarkeit durch und hat Notfallpläne für den Ausfall verschiedener Systemkomponenten.

f. Prüfverfahren nach Art. 32 Abs. 1 lit. d DSGVO

AIRAdoc führt regelmäßig technische Prüfverfahren wie Verschlüsselungskontrollen und Penetrationstests durch. Zur organisatorischen Kontrolle setzen wir Audit-Logs, Zugriffskontrollen, regelmäßige interne Audits und ein kontinuierliches Monitoring sicherheitsrelevanter Ereignisse ein. Externe Prüfungen und Zertifizierungen des Hosters gewährleisten darüber hinaus die Einhaltung der DSGVO und hoher Sicherheitsstandards.

g. Auftragskontrolle

Für die von AIRAdoc eingesetzten Auftragsverarbeiter wird gewährleistet, dass sie personenbezogene Daten im Auftrag der AIRAdoc GmbH nur nach deren Weisungen verarbeiten. Die Auswahl der Unterauftragsverarbeiter erfolgt nach

sorgfältiger Prüfung. Vor Auftragserteilung prüfen wir deren Dokumentation und Sicherheitsmaßnahmen.

AIRAdoc schließt mit dem Auftragsverarbeiter notwendige Vereinbarungen zur Auftragsverarbeitung unter Einbeziehung der Standard-Vertragsklauseln der Europäischen Union ab.

AIRAdoc erteilt dem Auftragsverarbeiter schriftliche Weisungen und vereinbart mit ihm Kontrollrechte. Außerdem stellt AIRAdoc sicher, dass der Auftragsverarbeiter die Daten nach Beendigung des Auftrags löscht.

h. Weisungsbindung nach Art. 32 Abs. 4 DSGVO

Alle Mitarbeitenden der AIRAdoc GmbH werden zur Einhaltung der Vorschriften der DSGVO und zur Wahrung der Vertraulichkeit verpflichtet. Die entsprechenden Regelungen werden regelmäßig überprüft.