Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Version: 1.19

Stand: 15. November 2026

Auftragsverarbeiter: Simpliant Technologies GmbH, Fasanenstraße 12, 10623 Berlin

Diese Anlage beschreibt die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO nach Schutzzielen und Maßnahmenkategorien. Einzelheiten der technischen Umsetzung sind Betriebs- und Geschäftsgeheimnis und werden nicht offengelegt. Die Maßnahmen werden fortgeschrieben, ohne das vereinbarte Schutzniveau zu unterschreiten (§ 5 Abs. 2 des Vertrages).

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

- Der Auftragsverarbeiter unterhält keine eigenen Server- oder Rechenzentrumsräume; die Verarbeitung findet in den Rechenzentren der in Anlage 2 beschriebenen Unterauftragsverarbeiter statt. Die physischen Zutrittsmaßnahmen obliegen deren Betreibern und sind Gegenstand der mit ihnen geschlossenen Verträge nach Art. 28 DSGVO; ihre Nachweise werden auf Anfrage weitergereicht (§ 9 Abs. 4 des Vertrages).
- Datenträger mit personenbezogenen Daten aus dem Auftragsverhältnis werden weder versendet noch außerhalb dieser Rechenzentren aufbewahrt.

Zugangskontrolle

- Zugang zu den Systemen nur nach Authentifizierung. Administrative Zugänge sind zusätzlich auf ein gesondertes, nicht öffentlich erreichbares Verwaltungsnetz beschränkt und an ein persönlich zugeordnetes kryptografisches Berechtigungsmerkmal gebunden; eine Anmeldung allein mit einem Passwort ist dort nicht möglich.
- Schutz vor unbefugten Anmeldeversuchen durch automatische Sperren und Begrenzung der Zugriffshäufigkeit; Passwortregeln werden erzwungen.
- Sitzungen und Zugangsberechtigungen sind zeitlich befristet und können jederzeit einzeln entzogen werden.

Zugriffskontrolle

- Rollenbasiertes Berechtigungskonzept; Berechtigungen werden nur vergeben, soweit sie für die Aufgabe erforderlich sind. Der Kreis der Personen mit administrativem Zugriff ist auf das notwendige Minimum begrenzt und dokumentiert; Berechtigungen werden bei Ausscheiden oder Aufgabenwechsel unverzüglich entzogen.
- Protokollierung administrativer Zugriffe und sicherheitsrelevanter Ereignisse.
- Zugangsgeheimnisse werden getrennt von der Anwendung und mit beschränktem Zugriff vorgehalten; ihre Ablage im Quellcode ist ausgeschlossen und wird automatisiert geprüft.

Trennungskontrolle

- Mandantentrennung auf Anwendungsebene: Zugriffe sind technisch auf die Daten des jeweils berechtigten Nutzers beschränkt; ein Zugriff auf Daten anderer Kunden ist über die Schnittstellen nicht vorgesehen.
- Trennung von Produktiv-, Vorschau- und Entwicklungsumgebung; für Entwicklung und Test werden keine produktiven Diktatinhalte verwendet.
- Funktionale Trennung der Verarbeitungsbereiche (Anwendung, Datenhaltung, Verarbeitung der Diktate) in voneinander abgeschotteten Ausführungsumgebungen mit getrennten internen Netzen.

Pseudonymisierung

- Im Bereich der Transkription werden Nutzerinnen und Nutzer ausschließlich unter einer pseudonymen Kennung geführt; Klarnamen und E-Mail-Adressen werden dort nicht vorgehalten, die

Zuordnung der Kennung zum Konto findet getrennt hiervon statt.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Verschlüsselte Übertragung auch bei der Übermittlung an Unterauftragsverarbeiter (Abschnitt 4); unverschlüsselte Verbindungen werden abgewiesen.
- Der Transkriptionsdienst ist technisch auf den regionalen EU-Endpunkt des Anbieters festgelegt; das gilt für die Umwandlung in Text und für die KI-Korrektur gleichermaßen. Bei abweichender Endpunktkonfiguration nimmt der Dienst den Betrieb nicht auf. Die Verarbeitung über diesen Endpunkt findet nach Bestätigung des Anbieters in der EU statt (Anlage 2 Abschnitt B). Diese technische Endpunktbindung garantiert keinen regionalen Speicherort sämtlicher Anbieter-Konto-, Abrechnungs- und Betriebsmetadaten. Die ausgehenden Verbindungen sind auf einen dokumentierten, engen Kreis von Zielen begrenzt.
- Diktatinhalte werden nur für die Dauer der Verarbeitung vorgehalten und danach unverzüglich gelöscht, auch bei Fehler oder Abbruch; Transkripte werden nicht dauerhaft gespeichert, sondern an die Anwendung des Verantwortlichen zurückgegeben. Zur KI-Korrektur übermittelte Texte werden beim Auftragsverarbeiter nur für die Dauer der Korrektur verarbeitet und nicht gespeichert; für die Aufbewahrung beim Unterauftragsverarbeiter gilt Anlage 2 des Vertrags.

Eingabekontrolle und Nachvollziehbarkeit

- Protokollierung der Zugriffe auf die Verarbeitungssysteme; Inhalte von Diktaten, Transkripten und zur KI-Korrektur übermittelten Texten werden nicht protokolliert, Geheimnisse in Protokollen unkenntlich gemacht.
- Änderungen an der Produktivumgebung werden ausschließlich über ein versioniertes, dokumentiertes Änderungsverfahren mit Autor, Prüfer und Zeitpunkt eingebracht; jeder Stand ist einem konkreten Änderungsvorgang zugeordnet. Eingehende Daten werden vor der Verarbeitung geprüft und begrenzt.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Regelmäßige, automatisierte Sicherungen des Konto- und Abonnementportals werden verschlüsselt auf einem von der Produktivumgebung getrennten System abgelegt. Für die kurzfristige Wiederherstellung werden zusätzlich täglich und vor jeder Änderung der Produktivumgebung lokale Sicherungen auf dem Produktivsystem vorgehalten; sie sind nur der Administration zugänglich, werden verschlüsselt abgelegt (Abschnitt 4) und nach 7 Tagen gelöscht. Auf dem getrennten System werden Datenbankstände nach spätestens 7 Tagen gelöscht, Sicherungen der Systemkonfiguration und der Betriebsprotokolle nach einer gestaffelten Regel bis zu sechs Monate aufbewahrt. Die Sicherungsläufe werden protokolliert.
- Dokumentiertes Wiederherstellungs- und Rückrollverfahren; die Wiederherstellbarkeit wird erprobt.
- Überwachung der Erreichbarkeit und des Betriebszustands durch ein von der Produktivumgebung unabhängiges Verfahren mit Alarmierung an einen gesonderten Meldeweg. Die Fehlerüberwachung wird in eigener Verantwortung betrieben und erhält keine personenbezogenen Daten.
- Automatischer Wiederanlauf der Dienste nach Störungen; Schutz vor Überlastung durch Begrenzung von Zugriffshäufigkeit, gleichzeitiger Verarbeitung und Datenmenge. Sicherheitsrelevante Aktualisierungen werden zeitnah eingespielt.

4. Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Verschlüsselte Übertragung nach dem Stand der Technik für sämtliche von außen erreichbaren Verbindungen und für den Versand von Nachrichten an Vertragspartner. Die lokalen Sicherungen nach Abschnitt 3 werden asymmetrisch verschlüsselt abgelegt; der zur Entschlüsselung erforderliche Schlüssel wird nicht auf dem Produktivsystem, sondern getrennt davon verwahrt. Die Sicherungen auf dem getrennten System werden ebenfalls verschlüsselt abgelegt.

- Passwörter, Zugangs- und Aktivierungsmerkmale werden ausschließlich in nicht rückrechenbarer Form nach dem Stand der Technik gespeichert, Klartextwerte nicht vorgehalten. Für ihre Erzeugung werden kryptografisch sichere Zufallswerte verwendet.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Jede Änderung an der Produktivumgebung durchläuft vor der Übernahme ein automatisiertes Prüfverfahren, das sicherheitsrelevante Vorgaben und die Wirksamkeit der Löschroutinen abdeckt; Herkunft und Unverändertheit der eingesetzten Software-Bestandteile sind nachvollziehbar.
- Die Löschläufe weisen die Zahl der gelöschten Datensätze je Kategorie aus und sind damit überprüfbar.
- Verzeichnis der Verarbeitungstätigkeiten, Datenschutzerklärung, Auftragsverarbeitungsvertrag und diese Anlage werden geführt und bei Änderungen fortgeschrieben.
- Beschäftigte und mitwirkende Personen sind zur Vertraulichkeit verpflichtet und über die für sie geltenden Datenschutzanforderungen unterrichtet. Anlaufstelle für Datenschutzanliegen, Nachweisanfragen und Meldungen: support@simpliant.eu.

6. Auftragskontrolle (Art. 28 DSGVO)

- Unterauftragsverarbeiter werden nach den in Anlage 2 festgelegten Standorten und Transfermechanismen ausgewählt (EU/EWR, Anlage 2 Abschnitt B); mit allen bestehen Verträge nach Art. 28 DSGVO. Anlage 2 beschreibt sie nach Leistung, Sitz und Ort der Verarbeitung; die Liste mit Name und Anschrift erhält der Verantwortliche auf Anfrage (Anlage 2 Abschnitt D). Änderungen werden vorab in Textform mitgeteilt (§ 6 des Vertrages).
- Die von den Unterauftragsverarbeitern eingesetzten weiteren Dienstleister werden beobachtet.
- Weisungen des Verantwortlichen werden dokumentiert und ihre Umsetzung nachgehalten.

7. Datenminimierung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

- Die Funktion zur dauerhaften Ablage von Aufnahmen und Transkripten ist im Produktivbetrieb nicht aktiv (Abschnitt 2).
- Nutzungsdaten werden pseudonym geführt und nach Ablauf der in § 11 des Vertrages genannten Fristen automatisiert gelöscht; abgelaufene Zugangs- und Aktivierungsmerkmale werden im selben Lauf entfernt.
- Es werden ausschließlich technisch notwendige Cookies und lokale Speicher verwendet. Die Reichweitenmessung erfolgt ohne Einbindung Dritter, ohne Cookies, ohne geräteübergreifende Wiedererkennung und ohne Profilbildung; Marketing- und Werbenetzwerke werden nicht eingesetzt. Zahlungsmittel- und Kartendaten werden nicht beim Auftragsverarbeiter erhoben.

8. Vorgehen bei Verletzungen des Schutzes personenbezogener Daten

- Verletzungen, die die im Auftrag verarbeiteten Daten betreffen, werden dem Verantwortlichen unverzüglich, spätestens innerhalb von **24 Stunden** nach Kenntniserlangung, in Textform gemeldet (§ 8 des Vertrages).
- Vorfall, Sofortmaßnahmen und Verlauf werden dokumentiert; der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Pflichten nach Art. 33 und 34 DSGVO.