Auftragsverarbeitungsvertrag

Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO. Sie ist Bestandteil des Vertrags über die Nutzung von Diktiro und gilt für alle Kunden ohne Enterprise-Vertrag, ohne dass eine gesonderte Unterzeichnung erforderlich ist. Für Enterprise-Kunden gilt der Auftragsverarbeitungsvertrag, der Bestandteil des Enterprise-Vertrags ist.

Stand: 3. November 2026

1. Präambel und Gegenstand

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV“) ist Bestandteil des zwischen dem Kunden (nachfolgend „Verantwortlicher“) und der AI Union UG (haftungsbeschränkt), Weidenweg 29, 75382 Althengstett, Deutschland (nachfolgend „Diktiro“) geschlossenen Vertrags über die Nutzung der Diktiro-Dienste (nachfolgend „Hauptvertrag“).

Der AVV konkretisiert die datenschutzrechtlichen Pflichten der Parteien für den Fall, dass Diktiro im Rahmen der Erbringung der Dienste personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Er regelt Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen sowie die Rechte und Pflichten der Parteien gemäß Art. 28 Abs. 3 DSGVO.

Der AVV bedarf keiner gesonderten Unterzeichnung. Mit Abschluss des Hauptvertrags gilt er zwischen den Parteien als vereinbart. Auf Wunsch stellt Diktiro eine unterzeichnete Ausfertigung zur Verfügung; eine Anfrage genügt an info@diktiro.ai.

Datenschutzbeauftragter von Diktiro ist die heyData GmbH, Schützenstraße 5, 10117 Berlin. Anfragen an den Datenschutzbeauftragten nimmt Diktiro unter der oben genannten Adresse mit dem Betreff „Datenschutzbeauftragter" entgegen und leitet sie unverändert weiter.

Im Fall von Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV hinsichtlich der Verarbeitung personenbezogener Daten vor.

---

2. Begriffsbestimmungen

Die in diesem AVV verwendeten Begriffe entsprechen den Definitionen der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, „DSGVO“). Ergänzend gilt:

- **Datenschutzrecht** bezeichnet die DSGVO, das Bundesdatenschutzgesetz (BDSG), das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) sowie alle sonstigen auf die Verarbeitung anwendbaren Datenschutzvorschriften in ihrer jeweils geltenden Fassung.
- **Standardvertragsklauseln** bezeichnet die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß dem Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission.
- **Drittland** bezeichnet ein Land außerhalb des Europäischen Wirtschaftsraums (EWR), für das kein Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO vorliegt.
- **Kundendaten** bezeichnet die personenbezogenen Daten, die Diktiro im Auftrag des Verantwortlichen im Rahmen der Erbringung der Dienste verarbeitet.

---

3. Rollen der Parteien

Der Verantwortliche ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die Kundendaten. Diktiro ist Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO.

Der Verantwortliche bleibt im Verhältnis zu den betroffenen Personen und gegenüber den Aufsichtsbehörden allein dafür verantwortlich, die Rechtmäßigkeit der Verarbeitung sowie die Wahrung der Rechte betroffener Personen sicherzustellen.

Soweit Diktiro personenbezogene Daten zu eigenen Zwecken verarbeitet – etwa zur Vertragsabwicklung, zur Abrechnung, zur Erfüllung eigener gesetzlicher Pflichten, zur Sicherheit der eigenen Systeme oder, nur mit ausdrücklicher Einwilligung des einzelnen Nutzers, zur Messung der eigenen Werbung – handelt Diktiro insoweit als eigener Verantwortlicher. Diese Verarbeitungen sind nicht Gegenstand dieses AVV, sondern der Datenschutzhinweise zur Diktiro-Anwendung.

---

4. Gegenstand, Art und Zweck der Verarbeitung

Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen sowie die Dauer der Verarbeitung ergeben sich abschließend aus Anlage 1.

Die Verarbeitung findet ausschließlich in Deutschland statt, soweit in Ziffer 15 und Anlage 2 nichts Abweichendes geregelt ist.

Die Dienste werden in den folgenden Betriebsarten bereitgestellt. Welche Daten in welcher Betriebsart wohin gelangen und wie lange sie gespeichert werden, ist in Anlage 1 im Einzelnen beschrieben.

1. **Cloud-Betrieb** (Standard): Das Audio wird an Diktiro übertragen und auf Servern von Diktiro in Text umgewandelt; der Text wird anschließend dort nachbearbeitet. Die Sprach- und KI-Modelle betreibt Diktiro selbst auf diesen Servern, ein externer Anbieter von Sprach- oder KI-Modellen ist nicht beteiligt. Die Verarbeitung erfolgt ausschließlich in Rechenzentren der Hetzner Online GmbH in Deutschland, siehe Anlage 2. Das Audio wird standardmäßig nicht gespeichert; aktiviert der Verantwortliche oder ein von ihm berechtigter Nutzer die Speicherung des Audios in den Einstellungen, wird es 30 Tage gespeichert und danach gelöscht.
2. **Lokaler Betrieb:** Spracherkennung und Anwendung des Wörterbuchs erfolgen auf dem Endgerät des Nutzers; die dafür nötigen Modelle werden mit der Anwendung installiert. Das Audio verlässt das Endgerät nicht. Zur KI-Nachbearbeitung wird ausschließlich der erkannte Text an die Server von Diktiro in Deutschland übertragen, dort nur für die Dauer der Anfrage im Arbeitsspeicher verarbeitet, an den Nutzer zurückgegeben und nicht gespeichert. Darüber hinaus übermittelt werden die Konto- und Lizenzdaten, Wortzahlen ohne Inhalte, das Wörterbuch des Nutzers zur Synchronisierung, die persönlichen Einstellungen sowie der Verlauf der Diktate, sofern er im Konto gespeichert wird (Voreinstellung).

---

5. Pflichten des Verantwortlichen

Der Verantwortliche ist für die Zulässigkeit der Verarbeitung der Kundendaten sowie für die Wahrung der Rechte betroffener Personen verantwortlich. Er sichert insbesondere zu, dass

1. er über eine tragfähige Rechtsgrundlage für die Erhebung und Übermittlung der Kundendaten an Diktiro verfügt,
2. die Kundendaten im Einklang mit dem Datenschutzrecht erhoben und verarbeitet wurden, und
3. keine gesetzlichen Vorschriften der Erbringung der Dienste durch Diktiro entgegenstehen.

Der Verantwortliche informiert Diktiro unverzüglich, wenn er bei der Prüfung der Ergebnisse der Verarbeitung Fehler oder Unregelmäßigkeiten feststellt oder wenn die Verarbeitung nicht mehr

im Einklang mit dem Datenschutzrecht steht.

Diktiro ist darauf eingerichtet, dass Diktate und Meeting-Notizen Gesundheitsdaten und andere besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO sowie Daten im Sinne des Art. 10 DSGVO enthalten. Diktiro verarbeitet solche Daten unter den Maßnahmen nach Anlage 3; einer gesonderten Mitteilung oder Vereinbarung bedarf es dafür nicht. Die Zulässigkeit der Verarbeitung nach Art. 9 Abs. 2 und Art. 10 DSGVO prüft der Verantwortliche.

Hinweis für Berufsgeheimnisträger: Die Verpflichtung von Diktiro zur Verschwiegenheit nach § 203 StGB ist nicht Bestandteil dieses AVV. Sie wird zusätzlich in einer gesonderten Vereinbarung geschlossen, die Kunden in den Tarifen Secure und Enterprise unter diktiro.ai/berufsgeheimnistraeger anfordern können.

---

6. Weisungsgebundene Verarbeitung

Diktiro verarbeitet die Kundendaten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Als Weisung gelten der Hauptvertrag einschließlich dieses AVV sowie die Nutzung der Dienste durch den Verantwortlichen im Rahmen der von Diktiro bereitgestellten Funktionen.

Weisungen des Verantwortlichen, die über den Hauptvertrag hinausgehen, bedürfen der Textform. Mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen. Ein durch Sonderweisungen entstehender Mehraufwand kann Diktiro gesondert vergütet werden.

Diktiro informiert den Verantwortlichen unverzüglich, wenn eine Weisung nach Auffassung von Diktiro gegen Datenschutzrecht verstößt. Diktiro ist berechtigt, die Ausführung einer solchen Weisung bis zu ihrer Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.

Ist Diktiro nach dem Recht der Union oder eines Mitgliedstaates zu einer Verarbeitung verpflichtet, die über die Weisungen hinausgeht, teilt Diktiro dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

7. Zweckbindung und Verbote

Diktiro ist es untersagt,

1. Kundendaten zu verkaufen oder zu vermieten,
2. Kundendaten für Zwecke der Werbung, der Marktforschung oder des interessenbezogenen Marketings zu verwenden; ausgenommen ist die Messung der eigenen Werbung mit E-Mail-Adresse und Kontokennung eines Nutzers, der selbst ausdrücklich eingewilligt hat (Datenschutzhinweise zur Anwendung, Ziffer 8), niemals jedoch mit Inhalten,
3. Kundendaten mit personenbezogenen Daten aus anderen Quellen oder aus der Geschäftsbeziehung mit anderen Kunden zusammenzuführen, sofern dies nicht zur Erbringung der Dienste erforderlich ist oder es sich um die Werbemessung nach Nr. 2 handelt, und
4. Kundendaten außerhalb der unmittelbaren Geschäftsbeziehung mit dem Verantwortlichen zu verwenden, aufzubewahren oder offenzulegen, ausgenommen die Werbemessung nach Nr. 2.

Keine Nutzung zum Training von KI-Modellen: Diktiro verwendet Kundendaten - insbesondere Audioaufnahmen und daraus erzeugte Transkripte - nicht zum Training, zur Weiterentwicklung oder zur Verbesserung eigener oder fremder Modelle künstlicher Intelligenz. Eine Weitergabe der Kundendaten an Anbieter von Sprach- oder Sprachverarbeitungsmodellen zu deren eigenen Trainingszwecken findet nicht statt.

Diktiro darf aggregierte, anonymisierte Nutzungsstatistiken, die keinen Personenbezug mehr aufweisen und auch nicht wiederherstellbar sind, zur Verbesserung und Absicherung der Dienste verwenden.

8. Vertraulichkeit

Diktiro verpflichtet alle zur Verarbeitung der Kundendaten befugten Personen in Textform zur Vertraulichkeit, sofern diese nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung der Tätigkeit oder des Beschäftigungsverhältnisses fort.

Diktiro stellt sicher, dass die zur Verarbeitung befugten Personen in den datenschutzrechtlich relevanten Anforderungen unterwiesen und regelmäßig geschult werden.

Diktiro nimmt von Kundendaten nur Kenntnis, soweit dies zur Erbringung der Dienste erforderlich ist.

Von den Unterauftragsverarbeitern nach Anlage 2 hat nur die Hetzner Online GmbH Zugang zu Inhalten, als Betreiberin der Rechenzentren und Server, auf denen Diktiro die Dienste betreibt. Verarbeitung und Speicherung der Inhalte erfolgen ausschließlich in Rechenzentren in Deutschland. Die übrigen Unterauftragsverarbeiter erhalten keine Inhalte.

Verlangt eine Behörde oder ein Gericht die Herausgabe von Kundendaten, informiert Diktiro den Verantwortlichen unverzüglich, soweit dies rechtlich zulässig ist, und gibt Kundendaten nur heraus, soweit eine rechtliche Pflicht dazu besteht, und nur im erforderlichen Umfang.

---

9. Unterauftragsverarbeiter

Der Verantwortliche erteilt Diktiro die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 2 abschließend aufgeführt und gelten als genehmigt.

Diktiro informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mindestens **30 Tage** im Voraus per E-Mail an die im Konto hinterlegte Adresse des Verantwortlichen bzw. an die im Hauptvertrag genannte Vertragsadresse; die Aktualisierung dieser Seite allein genügt nicht. Der Verantwortliche kann einer Änderung innerhalb von 14 Tagen ab Zugang der Information aus einem datenschutz- oder berufsrechtlich begründeten Anlass widersprechen.

Widerspricht der Verantwortliche und lässt sich der Einwand nicht innerhalb angemessener Frist ausräumen, ist der Verantwortliche berechtigt, den Hauptvertrag mit Wirkung zum Zeitpunkt der beabsichtigten Änderung außerordentlich zu kündigen. Bereits im Voraus gezahlte Entgelte für nicht in Anspruch genommene Leistungen werden anteilig erstattet.

In dringenden Fällen – insbesondere zur Abwehr einer akuten Sicherheitsgefahr oder zur Aufrechterhaltung des Betriebs bei Ausfall eines bestehenden Unterauftragsverarbeiters – darf Diktiro einen Unterauftragsverarbeiter mit einer verkürzten Frist von 10 Tagen ersetzen. Diktiro informiert den Verantwortlichen in diesem Fall unverzüglich per E-Mail unter Angabe der Gründe; das Widerspruchs- und Kündigungsrecht nach den Absätzen 2 und 3 gilt entsprechend.

Diktiro verpflichtet jeden Unterauftragsverarbeiter vertraglich zu Datenschutzpflichten, die den Pflichten aus diesem AVV mindestens gleichwertig sind, und bleibt gegenüber dem Verantwortlichen für deren Einhaltung verantwortlich.

Nicht als Unterauftragsverarbeitung gelten Nebenleistungen, die Diktiro bei Dritten in Anspruch nimmt und die nicht auf die Verarbeitung von Kundendaten gerichtet sind, etwa Telekommunikationsdienste, Reinigungsdienste oder die Wartung von Endgeräten. Diktiro trifft auch insoweit angemessene Maßnahmen zum Schutz der Kundendaten.

---

10. Unterstützungspflichten

Diktiro unterstützt den Verantwortlichen im Rahmen des Zumutbaren und unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen bei

1. der Erfüllung von Anträgen betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch (Art. 12 bis 23 DSGVO),
2. der Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DSGVO),
3. der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und der Benachrichtigung betroffener Personen (Art. 33 und 34 DSGVO),
4. der Durchführung von Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) und
5. etwaigen vorherigen Konsultationen der Aufsichtsbehörde (Art. 36 DSGVO).

Wendet sich eine betroffene Person unmittelbar an Diktiro, leitet Diktiro das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst, es sei denn, der Verantwortliche hat Diktiro hierzu angewiesen.

Für Unterstützungsleistungen, die über den gesetzlich geschuldeten Umfang hinausgehen oder die auf einem Umstand beruhen, den Diktiro nicht zu vertreten hat, kann Diktiro eine angemessene Vergütung verlangen.

11. Technische und organisatorische Maßnahmen

Diktiro trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen werden dabei berücksichtigt.

Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in Anlage 3 beschrieben. Diktiro darf die Maßnahmen fortentwickeln und anpassen, sofern das vereinbarte Schutzniveau dabei nicht unterschritten wird.

12. Meldung von Datenschutzverletzungen

Diktiro informiert den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von **24 Stunden** nach Bekanntwerden, über jede Verletzung des Schutzes personenbezogener Daten, die die Kundendaten betrifft. Die Meldung geht per E-Mail an die im Konto hinterlegte Adresse des Verantwortlichen bzw. an die im Hauptvertrag genannte Vertragsadresse.

Anlaufstelle bei Diktiro für Datenschutzvorfälle ist info@diktiro.ai mit dem Betreff „Datenschutzvorfall". Unter dieser Adresse kann auch der Verantwortliche einen Verdacht auf eine Verletzung melden.

Die Meldung enthält, soweit verfügbar, mindestens:

1. eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze,
2. den Namen und die Kontaktdaten einer Anlaufstelle für weitere Informationen,
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
4. eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Stehen die Informationen nicht vollständig zur Verfügung, meldet Diktiro zunächst den bekannten Sachverhalt und ergänzt die weiteren Angaben unverzüglich, sobald sie vorliegen. Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen obliegen dem Verantwortlichen; Diktiro unterstützt ihn dabei nach Ziffer 10.

13. Nachweise und Kontrollrechte

Diktiro stellt dem Verantwortlichen auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus diesem AVV erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen.

Der Nachweis kann durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Stellen, durch eine geeignete Zertifizierung oder durch eine Selbstauskunft anhand eines anerkannten Prüfstandards geführt werden. Der Verantwortliche erkennt an, dass ein solcher Nachweis eine Vor-Ort-Prüfung ersetzt, sofern keine konkreten Anhaltspunkte für eine Pflichtverletzung vorliegen.

Vor-Ort-Prüfungen erfolgen nach rechtzeitiger Ankündigung von mindestens 30 Tagen, während der üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs und höchstens einmal je Kalenderjahr. Ein darüber hinausgehendes Prüfungsrecht besteht bei konkretem Anlass, insbesondere nach einer Verletzung des Schutzes personenbezogener Daten.

Beauftragt der Verantwortliche einen Dritten mit der Prüfung, ist dieser zur Verschwiegenheit zu verpflichten. Diktiro kann einem Prüfer widersprechen, der zu Diktiro in einem Wettbewerbsverhältnis steht. Diktiro muss keine Informationen offenlegen, deren Offenlegung gegen Vertraulichkeitspflichten gegenüber anderen Kunden oder gegen gesetzliche Pflichten verstößt.

14. Löschung und Rückgabe

Der Verantwortliche kann seine Daten während der Vertragslaufzeit jederzeit selbst in einem maschinenlesbaren Format (JSON) exportieren sowie einzelne Inhalte - Diktate, Meeting-Notizen - oder das gesamte Konto selbst löschen. Die Löschung eines Kontos erfolgt unmittelbar.

Nach Beendigung des Hauptvertrags bleibt das Konto für 30 Tage im Nur-Lese-Modus zugänglich, damit der Verantwortliche seine Daten exportieren kann. Das gilt auch, wenn der Zugang zuvor wegen Zahlungsverzugs gesperrt wurde.

Nach Beendigung des Hauptvertrags löscht Diktiro sämtliche Kundendaten oder gibt sie nach Wahl des Verantwortlichen zurück, sofern keine gesetzliche Pflicht zur weiteren Speicherung besteht. Der Verantwortliche teilt seine Wahl in Textform mit oder löst Export und Löschung

selbst aus. Ohne eine solche Mitteilung löscht Diktiro die Kundendaten spätestens 90 Tage nach Vertragsende.

Diktiro sichert die Daten regelmäßig und verschlüsselt innerhalb der Rechenzentren in Deutschland. Gelöschte Daten werden mit dem Ablauf der Sicherungszyklen auch aus den Sicherungen entfernt.

Ausgenommen ist das Sicherheitsprotokoll der Anwendung (Audit-Log). Es behält die Art einer Aktion, eine pseudonyme Kennung des Handelnden und den Zeitpunkt, um Änderungen nachvollziehbar zu halten; weitere personenbezogene Angaben werden bei der Löschung daraus entfernt. Die Einträge werden höchstens drei Jahre nach Vertragsende aufbewahrt und danach anonymisiert.

Bestehen gesetzliche Aufbewahrungspflichten, schränkt Diktiro die Verarbeitung der betroffenen Daten ein, statt sie zu löschen. Die Löschung wird auf Anfrage in Textform bestätigt.

---

15. Drittlandübermittlung

Audio-, Transkriptions- und Meetingdaten werden ausschließlich in Rechenzentren in Deutschland verarbeitet (Hetzner Online GmbH). Im lokalen Betrieb nach Ziffer 4 verbleibt das Audio auf dem Endgerät. Auch System-E-Mails werden über einen Anbieter mit Sitz und Verarbeitung in der Europäischen Union versandt (Anlage 2); eine Übermittlung in ein Drittland findet nicht statt.

Eine Übermittlung von Kundendaten in ein Drittland findet nur statt, soweit dies in Anlage 2 ausgewiesen ist oder der Verantwortliche dies angewiesen hat. Davon unberührt bleibt die Werbemessung nach Ziffer 7 Nr. 2, bei der Meta die gehashte E-Mail-Adresse und Kontokennung eines einwilligenden Nutzers in die USA übermitteln kann. Ist eine Übermittlung in ein Drittland erforderlich, stellt Diktiro sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere durch

1. einen Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO,
2. den Abschluss der Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO in Verbindung mit ergänzenden Schutzmaßnahmen und einer dokumentierten Risikoabschätzung der Übermittlung (Transfer Impact Assessment), oder
3. eine andere geeignete Garantie im Sinne des Art. 46 DSGVO.

Auf Anfrage stellt Diktiro dem Verantwortlichen die entsprechende Dokumentation zur Verfügung.

---

16. Haftung

Für die Haftung der Parteien gelten die Regelungen des Hauptvertrags, soweit in diesem AVV nichts Abweichendes bestimmt ist. Die Haftung nach Art. 82 DSGVO gegenüber betroffenen Personen bleibt hiervon unberührt.

Haftungsbeschränkungen gelten nicht bei Vorsatz und grober Fahrlässigkeit, bei der Verletzung von Leben, Körper oder Gesundheit, bei arglistigem Verschweigen eines Mangels, bei Übernahme einer Garantie, nach dem Produkthaftungsgesetz sowie in allen Fällen, in denen eine Beschränkung der Haftung gesetzlich unzulässig ist.

Die Parteien stellen einander von Ansprüchen Dritter frei, soweit diese auf einer Verletzung der jeweils eigenen Pflichten aus diesem AVV oder aus dem Datenschutzrecht beruhen. Eine Freistellung von Bußgeldern findet nicht statt. Im Verhältnis zueinander haften die Parteien entsprechend ihrem jeweiligen Anteil an der Verantwortung (Art. 82 Abs. 5 DSGVO). Für die Freistellung und den Innenausgleich gelten die Haftungsbegrenzungen des Hauptvertrags.

---

17. Laufzeit, Änderungen und Schlussbestimmungen

Dieser AVV gilt für die Dauer des Hauptvertrags. Regelungen, die ihrer Natur nach über das Vertragsende hinaus fortgelten sollen - insbesondere zu Vertraulichkeit, Löschung und Haftung - bleiben auch danach wirksam.

Diktiro kann diesen AVV anpassen, soweit dies zur Einhaltung des Datenschutzrechts, aufgrund geänderter Rechtsprechung oder aufgrund von Vorgaben einer Aufsichtsbehörde erforderlich ist. Änderungen werden dem Verantwortlichen mindestens 30 Tage vor Wirksamwerden per E-Mail an die im Konto hinterlegte Adresse bzw. an die im Hauptvertrag genannte Vertragsadresse mitgeteilt; die Aktualisierung dieser Seite allein genügt nicht. Änderungen dürfen die Rechte des Verantwortlichen nicht wesentlich einschränken und seine Pflichten nicht wesentlich erweitern. Der Verantwortliche kann einer Änderung aus einem datenschutz- oder berufsrechtlich begründeten Anlass widersprechen; für Widerspruch und Kündigung gilt Ziffer 9 Absätze 2 und 3 entsprechend.

Geht der Hauptvertrag nach dessen Regelungen im Wege der Vertragsübernahme auf die SF Software Labs GmbH, Weidenweg 29, 75382 Althengstett, über, geht dieser AVV einschließlich seiner Anlagen mit über, ohne dass es einer weiteren Erklärung bedarf. Die SF Software Labs GmbH tritt in alle Rechte und Pflichten aus diesem AVV ein, auch soweit sie vor dem Übergang entstanden sind, und haftet für diese. Diktiro teilt den Übergang unverzüglich in Textform mit und nennt dabei Registergericht und Registernummer. Der Übergang ändert weder den Ort der Verarbeitung noch die Unterauftragsverarbeiter noch die technischen und organisatorischen Maßnahmen. Das Sonderkündigungsrecht des Verantwortlichen nach dem Hauptvertrag bleibt unberührt.

Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame Regelung, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Ausschließlicher Gerichtsstand ist - soweit gesetzlich zulässig - der Sitz von Diktiro.

Anlage 1 – Einzelheiten der Verarbeitung

1. Gegenstand und Art der Verarbeitung

Kern der Verarbeitung ist die Umwandlung gesprochener Sprache in Text sowie dessen KI-gestützte Nachbearbeitung (Formatierung, Korrektur, Strukturierung). Im Einzelnen umfassen die Dienste:

- **Diktieren:** Aufnahme über das Mikrofon, solange der Nutzer die Diktierfunktion auslöst; Umwandlung in Text und Anwendung des Wörterbuchs in der Cloud oder lokal (siehe Ziffer 4); KI-Nachbearbeitung des Textes; Einfügen des Ergebnisses in die aktive Anwendung über die Zwischenablage.
- **Verlauf:** Speicherung des erkannten Textes nach Anwendung des Wörterbuchs, wahlweise im Konto (Voreinstellung), nur auf dem Endgerät oder an beiden Orten. Die KI-nachbearbeitete Fassung wird nicht gespeichert.
- **Notetaker:** Live-Umwandlung von Mikrofon und Systemton des Endgeräts in Text, wahlweise lokal oder in der Cloud (siehe Ziffer 4); das Audio wird nach der Transkription gelöscht, und es tritt kein Bot einem Meeting bei; Trennung nach Sprechern, ohne die Sprecher zu identifizieren; Erstellung einer Zusammenfassung mit Aufgaben und

Entscheidungen; Beantwortung von Fragen des Nutzers zu einer Notiz. Auf Veranlassung des Nutzers kann eine Notiz über einen Link ohne Anmeldung lesbar freigegeben werden. Den Notetaker gibt es in der Desktop-Anwendung und in der iPhone- und iPad-App.

- **iPhone- und iPad-App und Diktiro-Tastatur:** Diktieren in der App und über die Tastatur; die Tastatur nimmt selbst nicht auf, sondern startet das Diktat in der App und fügt den fertigen Text ein. Wahlweise Erkennung mit der Spracherkennung von Apple auf dem Gerät; dann werden nur der erkannte Text und die Wortzahl übertragen. Konnte ein Diktat nicht übertragen werden, bleibt die Aufnahme verschlüsselt auf dem Gerät, bis sie erneut gesendet wird, höchstens 7 Tage.
- **Wörterbuch und Textbausteine:** vom Nutzer oder einem Administrator der Organisation eingetragene Begriffe und Bausteine. Es findet kein automatisches Lernen aus der Nutzung statt.
- **Kalenderanbindung** (optional): lesender Zugriff auf den Kalender des Nutzers, um anstehende Meetings im Notetaker anzuzeigen und kurz vor Beginn daran zu erinnern.
- **Verwaltung von Organisationen:** Einladungen, Beitrittsanfragen von Personen mit einer E-Mail-Adresse der Domain des Verantwortlichen, die ein Administrator bestätigt, Lizenzverwaltung, Team-Einstellungen durch Administratoren sowie - sofern vom Verantwortlichen erteilt - eine eingeschränkte Verwaltungsbefugnis für einen IT-Partner. Weder Administratoren noch Partner erhalten Zugriff auf Diktate, Wörterbücher, Textbausteine oder Meeting-Notizen.

Die Desktop-Anwendung liest auf dem Endgerät den Namen der aktiven Anwendung, um den Schreibstil zuzuordnen; diese Zuordnung erfolgt ausschließlich auf dem Endgerät. Fenstertitel, Adressen von Webseiten, Dokumentnamen, Bildschirminhalte und Text aus anderen Anwendungen werden nicht gelesen. Der Inhalt der Zwischenablage wird vor dem Einfügen kurzzeitig im Arbeitsspeicher gesichert und anschließend wiederhergestellt; er wird weder gespeichert noch übertragen.

2. Zweck der Verarbeitung

Bereitstellung der Diktiro-Dienste gemäß Hauptvertrag.

3. Kategorien betroffener Personen

- Beschäftigte, freie Mitarbeiter und sonstige Nutzer des Verantwortlichen,
- Personen, die in den vom Verantwortlichen diktierten Inhalten genannt werden (etwa Mandanten, Patienten, Kunden, Bewerber, Geschäftspartner),
- Teilnehmer von Meetings, deren Redebeiträge mit dem Notetaker erfasst werden.

4. Kategorien personenbezogener Daten

Kategorie	Beispiele
Stammdaten	Name, E-Mail-Adresse, Profilbild, Telefonnummer (freiwillig)
Vertrags- und Abrechnungsdaten	Tarif, Lizenzen, Zahlungsstatus
Audiodaten	Audio beim Diktieren und im Notetaker
Transkriptionsdaten	Aus den Audiodaten erzeugte Texte
Meetingdaten	Transkript je Redebeitrag mit Sprecherkennzeichnung („Sprecher 1“), Zusammenfassung, Aufgaben, eigene Notizen des Nutzers
Kalenderdaten	Titel, Beginn und Ende, Meeting-Link und Anzahl der Teilnehmer; keine Teilnehmeridentitäten
Inhaltsdaten des Kontos	Wörterbucheinträge, Textbausteine
Einstellungen	Persönliche Einstellungen der Anwendung, im Konto gespeichert und auf allen Geräten des Nutzers wirksam; Team-Einstellungen der Administratoren
Nutzungsdaten	Wortzahlen, Datum der letzten Nutzung, technischer Startbericht ohne Inhalte (App-Version, Plattform, Berechtigungsstatus)
Technische Daten	IP-Adresse und Browserkennung in Sitzungen und Server-Protokollen

Welche Inhalte in Audio-, Transkriptions- und Meetingdaten enthalten sind, bestimmt allein der Verantwortliche durch die Wahl dessen, was diktiert oder mit dem Notetaker erfasst wird. Diktiro hat hierauf keinen Einfluss.

5. Besondere Kategorien personenbezogener Daten

Diktiro erhebt keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO gezielt, ist aber darauf eingerichtet, dass Diktate und Meeting-Notizen solche Daten enthalten - etwa Gesundheitsdaten in einer Arztpraxis. Diktiro verarbeitet sie ausschließlich im Rahmen der Erbringung der Dienste und unter den Maßnahmen nach Anlage 3 (siehe Ziffer 5). Die Zulässigkeit einer solchen Verarbeitung und die Erfüllung der Voraussetzungen des Art. 9 Abs. 2 DSGVO prüft der Verantwortliche.

Es werden keine Stimmprofile oder sonstigen biometrischen Merkmale erzeugt oder gespeichert. Die Trennung nach Sprechern im Notetaker gilt nur innerhalb eines einzelnen Meetings und erlaubt keine Wiedererkennung einer Person.

6. Speicherdauer

Daten	Speicherung
Audio (Cloud-Betrieb)	Standardmäßig nur im Arbeitsspeicher für die Dauer der Verarbeitung, keine Speicherung auf Datenträgern. Hat der Verantwortliche die Speicherung des Audios aktiviert: 30 Tage ab der Aufnahme, danach Löschung. Zur Vermeidung doppelter Abrechnung werden eine Prüfsumme und die Dateigröße 8 Tage gespeichert.
Text zur KI-Nachbearbeitung	Nur im Arbeitsspeicher für die Dauer der Anfrage, keine Speicherung; die nachbearbeitete Fassung wird nicht gespeichert
Audio auf dem Endgerät	Verschlüsselt bis zum Abschluss des Diktats; bei gescheitertem oder abgebrochenem Diktat zur Wiederherstellung bis zu 14 Tage
Verlauf der Diktate	Bis zur Löschung durch den Nutzer; bei der Einstellung „nur Gerät“ ausschließlich verschlüsselt auf dem Endgerät
Meeting-Transkripte und Zusammenfassungen	Bis zur Löschung durch den Nutzer
Kalenderdaten	Zwischenspeicher von 5 Minuten; dauerhaft nur die Kalenderverbindung
Sitzungsdaten mit IP-Adresse	7 Tage ab der letzten Nutzung
Protokolle der Anwendungsserver mit IP-Adresse	30 Tage
Übrige Kontodaten	Für die Dauer des Hauptvertrags, Löschung nach Ziffer 14
Datensicherungen	Gelöschte Daten werden mit dem Ablauf der Sicherungszyklen auch aus den Sicherungen entfernt
Sicherheitsprotokoll (Audit-Log)	Höchstens drei Jahre nach Vertragsende, danach anonymisiert

Die Verarbeitung erfolgt fortlaufend für die Dauer des Hauptvertrags sowie für den Zeitraum bis zur Löschung nach Ziffer 14.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Zum Stand 3. November 2026 setzt Diktiro die folgenden Unterauftragsverarbeiter ein. Weitere Unterauftragsverarbeiter werden nicht eingesetzt. Spracherkennung und KI-Nachbearbeitung erfolgen auf Servern, die Diktiro in Rechenzentren der Hetzner Online GmbH in Deutschland betreibt, mit Modellen, die Diktiro selbst betreibt. Anmeldedienste, die der Nutzer selbst wählt (Google, Apple, Microsoft), sind keine Unterauftragsverarbeiter von Diktiro.

Unternehmen	Leistung	Ort der Verarbeitung
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland	Rechenzentren und Server für Anwendung, Datenbank, Zwischenspeicher und Server-Protokolle sowie für Spracherkennung, KI-Nachbearbeitung, Zusammenfassungen im Notetaker, Fragen zu Meeting-Notizen und Suche in Textbausteinen (mit Modellen, die Diktiro selbst betreibt)	Deutschland
Lettermint B.V. Willemsvaart 16 B, 8019 AB Zwolle, Niederlande	Versand von System-E-Mails (Einladungen, Bestätigungen, Zurücksetzen des Passworts); übermittelt werden nur E-Mail-Adresse und Name	Europäische Union
Stripe Payments Europe, Limited The One Building, 1 Grand Canal Street Lower, Dublin 2, Irland	Zahlungsabwicklung	Irland (EU)

Inhalte (Audio und Text zur Verarbeitung sowie der gespeicherte Verlauf, Wörterbuch, Textbausteine und Meeting-Notizen in der Datenbank) liegen ausschließlich auf den Servern von Diktiro bei der Hetzner Online GmbH. Lettermint und Stripe erhalten weder Audio- noch Transkriptionsdaten.

Mit Lettermint besteht ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO; Versand und Speicherung der E-Mail-Daten erfolgen ausschließlich in der Europäischen Union, übermittelt

werden nur E-Mail-Adresse und Name. Mit der Hetzner Online GmbH besteht ebenfalls ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO; Verarbeitung und Speicherung der Inhalte erfolgen ausschließlich in Rechenzentren in Deutschland.

Anlage 3 – Technische und organisatorische Maßnahmen

Diktiro trifft die folgenden Maßnahmen nach Art. 32 DSGVO. Die Maßnahmen werden regelmäßig überprüft und an den Stand der Technik angepasst.

1. Vertraulichkeit

- **Zutrittskontrolle:** Die Verarbeitung erfolgt in zertifizierten Rechenzentren der Hetzner Online GmbH in Deutschland mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal. Im lokalen Betrieb liegt die Zutrittskontrolle für die Endgeräte beim Verantwortlichen.
- **Zugangskontrolle:** Zugang zu den Verwaltungsoberflächen der Infrastruktur nur für namentlich benannte Personen über persönliche Konten.
- **Zugriffskontrolle:** Jeder Zugriff auf Diktate, das persönliche Wörterbuch und persönliche Textbausteine ist in der Anwendung auf den angemeldeten Nutzer beschränkt. Meeting-Notizen, das Team-Wörterbuch und Team-Textbausteine sind zusätzlich nur für die Nutzer derselben Organisation zugänglich, mit denen sie geteilt werden. Eine Meeting-Notiz kann der Nutzer außerdem über einen Link ohne Anmeldung lesbar freigeben; sie ist dann für jeden lesbar, der den Link kennt. Administratoren von Organisationen, IT-Partner und Mitarbeiter von Diktiro sehen in der Anwendung Nutzungszahlen, aber keine Inhalte. Befugnisse von IT-Partnern werden bei jeder Anfrage neu geprüft.
- **Trennungskontrolle:** Mandantentrennung auf Anwendungsebene; jeder Datensatz ist einem Nutzer und gegebenenfalls einer Organisation zugeordnet. Test- und Produktionsumgebung verwenden getrennte Datenbanken.
- **Verschlüsselung:** Übertragung ausschließlich über TLS, auch zwischen Anwendung, Datenbank und Zwischenspeicher. Verschlüsselung ruhender Daten durch die Plattformanbieter. Auf dem Endgerät werden Anmeldedaten, Verlauf, Notizblock und zwischengespeichertes Audio über den Schlüsselbund des Betriebssystems verschlüsselt.
- **Datenminimierung:** Audio wird auf den Servern standardmäßig nicht gespeichert, sondern nur im Arbeitsspeicher verarbeitet; nur wenn der Verantwortliche die Speicherung aktiviert, wird es 30 Tage gespeichert und danach gelöscht. Server- und App-Protokolle enthalten

keine Diktat- oder Meetinginhalte. Aus Kalendern werden keine Teilnehmeridentitäten gespeichert.

2. Integrität

- **Weitergabekontrolle:** Datenübertragungen erfolgen ausschließlich verschlüsselt. Datenträger werden nicht zum physischen Transport von Kundendaten verwendet.
- **Eingabekontrolle:** Verändernde Vorgänge - etwa Rechteänderungen, Löschungen und administrative Eingriffe - werden in einem Sicherheitsprotokoll festgehalten, das nicht ohne den zugehörigen Vorgang geschrieben werden kann.
- **Anwendungssicherheit:** Automatisierte Prüfung jeder Änderung (Typprüfung, statische Analyse, Tests, Build) vor der Auslieferung.

3. Verfügbarkeit und Belastbarkeit

- **Betrieb:** Die Anwendung läuft auf einer verwalteten Container-Plattform, die ausgefallene Instanzen automatisch neu startet und bei Last skaliert. Stromversorgung, Brandschutz und Klimatisierung werden auf Ebene des Rechenzentrums sichergestellt.
- **Netzwerksicherheit:** Verbindungen zur Anwendung ausschließlich über HTTPS; Begrenzung der Anfragen je Nutzer in der Anwendung.
- **Datensicherung:** Regelmäßige verschlüsselte Datensicherung innerhalb der Rechenzentren in Deutschland. Gelöschte Daten werden mit dem Ablauf der Sicherungszyklen auch aus den Sicherungen entfernt.

4. Verfahren zur regelmäßigen Überprüfung

- **Meldewege:** Sicherheitsvorfälle werden nach Ziffer 12 gemeldet.
- **Auftragskontrolle:** Sorgfältige Auswahl der Unterauftragsverarbeiter, Abschluss von Auftragsverarbeitungsverträgen, regelmäßige Überprüfung der von ihnen vorgelegten Nachweise.
- **Datenschutz durch Technikgestaltung:** Datenminimierung, Prüfung des Datenschutzes bei der Einführung neuer Funktionen.

Fragen zu diesem Vertrag? Eine unterzeichnete Ausfertigung, die Nachweise der Unterauftragsverarbeiter und Auskunft zu einzelnen Maßnahmen stellt Diktiro auf Anfrage an info@diktiro.ai bereit. Diese Fassung: Stand 3. November 2026.