

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

zwischen

dem Verantwortlichen (in den AGB als „Kunde“ bezeichnet)

– nachfolgend „Verantwortlicher“ –

und

blinkpilot UG (haftungsbeschränkt)

Hahnstr. 70, 60528 Frankfurt am Main

Handelsregister: HRB 142016, Amtsgericht Frankfurt am Main

Vertreten durch: Stefan Dold, Geschäftsführer

E-Mail: datenschutz@blinkpilot.com

(in den AGB als „Anbieter“ bezeichnet)

– nachfolgend „Auftragsverarbeiter“ –

Der Verantwortliche und der Auftragsverarbeiter werden nachfolgend gemeinsam als „Parteien“ und jeweils einzeln als „Partei“ bezeichnet.

Stand: 29.06.2026 **Version:** 1.0

Hinweis zur Lesbarkeit: Aus Gründen der besseren Lesbarkeit wird in diesem Vertrag auf eine geschlechtsspezifische Differenzierung verzichtet. Sämtliche Personenbezeichnungen gelten im Sinne der Gleichbehandlung gleichermaßen für alle Geschlechter. Die verkürzte Sprachform hat ausschließlich redaktionelle Gründe und ist wertungsfrei.

Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV“) konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit der Bereitstellung und Nutzung der SaaS-Anwendung „blinkpilot“ auf Grundlage des zwischen den Parteien geschlossenen Hauptvertrages (Allgemeine Geschäftsbedingungen der blinkpilot UG (haftungsbeschränkt) in der jeweils gültigen Fassung, nachfolgend „AGB“, nebst etwaiger zwischen den Parteien individuell vereinbarter ergänzender oder abweichender Regelungen).

Im Rahmen der Erbringung der vertragsgegenständlichen Leistungen verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen im Sinne des Art. 4 Nr. 8, Art. 28 DSGVO. Dieser AVV regelt die Rechte und Pflichten der Parteien hinsichtlich dieser Auftragsverarbeitung.

Die Parteien schließen diesen AVV in Erfüllung der Anforderungen des Art. 28 Abs. 3 DSGVO sowie der ergänzenden Vorschriften des Bundesdatenschutzgesetzes (BDSG).

Verhältnis zu anderen Vereinbarungen: Dieser AVV ist Bestandteil des Hauptvertrages. Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag in datenschutzrechtlichen Angelegenheiten gehen die Regelungen dieses AVV vor. Bei Widersprüchen zwischen diesem AVV und den EU-Standardvertragsklauseln nach Beschluss 2021/914/EU (soweit anwendbar über Subunternehmer) gehen letztere vor.

Im Übrigen bleiben die Regelungen des Hauptvertrages unberührt.

§ 1 Begriffsbestimmungen

(1) Soweit in diesem AVV Begriffe der Datenschutz-Grundverordnung (DSGVO) verwendet werden, gelten die dort in Art. 4 DSGVO niedergelegten Begriffsbestimmungen.

(2) Ergänzend gelten für diesen AVV folgende Begriffe:

a) **„Verantwortlicher“** bezeichnet den Kunden im Sinne der AGB. Der Verantwortliche ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die im Rahmen der Nutzung der App durch ihn veranlassten Verarbeitungen.

b) **„Auftragsverarbeiter“** bezeichnet die blinkpilot UG (haftungsbeschränkt), Hahnstr. 70, 60528 Frankfurt am Main, eingetragen im Handelsregister des Amtsgerichts Frankfurt am Main unter HRB 142016 (in den AGB als „Anbieter“ bezeichnet). Der Auftragsverarbeiter ist Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO.

c) **„App“** bezeichnet die SaaS-Anwendung „blinkpilot“ einschließlich aller darüber bereitgestellten Funktionen und Schnittstellen, wie im Hauptvertrag näher beschrieben.

d) **„Kundendaten“** bezeichnet alle personenbezogenen Daten, die der Auftragsverarbeiter im Rahmen der Erbringung der vertragsgegenständlichen Leistungen im Auftrag des Verantwortlichen verarbeitet, insbesondere die in Anlage 1 beschriebenen Datenarten.

e) **„Nutzer“** bezeichnet die natürlichen Personen, die im Auftrag und unter der Verantwortung des Verantwortlichen die App verwenden (insbesondere Inhaber, Geschäftsführung, Beschäftigte sowie sonstige berechnigte Personen des Verantwortlichen).

f) **„Endkunden des Verantwortlichen“** bezeichnet die natürlichen oder juristischen Personen, mit denen der Verantwortliche in Geschäftsbeziehung steht und deren personenbezogene Daten der Verantwortliche in der App verarbeitet.

g) **„Subunternehmer“** bezeichnet weitere Auftragsverarbeiter im Sinne des Art. 28 Abs. 2 und 4 DSGVO, derer sich der Auftragsverarbeiter zur Erbringung der vertragsgegenständlichen Leistungen bedient.

h) **„Datenschutzverletzung“** bezeichnet eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO.

i) **„Hauptvertrag“** bezeichnet die zwischen den Parteien geschlossenen Allgemeinen Geschäftsbedingungen der blinkpilot UG (haftungsbeschränkt) in der jeweils gültigen Fassung sowie etwaige zwischen den Parteien individuell vereinbarte ergänzende oder abweichende Regelungen, soweit solche geschlossen wurden.

j) **„Beschäftigte“** bezeichnet Beschäftigte im Sinne des § 26 Abs. 8 BDSG, insbesondere Arbeitnehmer, Auszubildende, Leiharbeiter sowie Bewerber des Verantwortlichen.

(3) Soweit dieser AVV auf die DSGVO Bezug nimmt, gilt diese in der zum Zeitpunkt der jeweiligen Verarbeitung gültigen Fassung. Entsprechendes gilt für das BDSG sowie sonstige anwendbare datenschutzrechtliche Vorschriften.

§ 2 Gegenstand, Art, Dauer und Zweck der Verarbeitung

(1) **Gegenstand der Auftragsverarbeitung** Gegenstand der Auftragsverarbeitung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung und des Betriebs der App im Auftrag des Verantwortlichen. Die App unterstützt den Verantwortlichen bei der Abwicklung seiner betrieblichen Geschäftsprozesse, insbesondere im Bereich der Verwaltung von Endkunden- und Auftragsdaten sowie der Termin- und Einsatzplanung.

(2) **Art der Verarbeitung** Die Verarbeitung umfasst sämtliche Verarbeitungsvorgänge im Sinne des Art. 4 Nr. 2 DSGVO, die zur Erbringung der vertragsgegenständlichen Leistungen erforderlich sind, insbesondere:

- a) das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden und Verknüpfen personenbezogener Daten,
- b) das Übermitteln durch Bereitstellung in der App sowie das Versenden im Auftrag des Verantwortlichen an dessen Endkunden (insbesondere per E-Mail),
- c) die automatisierte Verarbeitung durch Funktionen der App, einschließlich KI-gestützter Funktionen nach Maßgabe von § 7,
- d) die Berechnung geografischer Koordinaten aus Adressdaten sowie die Berechnung von Fahrtrouten und Reisezeiten für Zwecke der Einsatzplanung,
- e) das Einschränken, Löschen und Vernichten der Daten gemäß § 16 dieses AVV sowie das Bereitstellen zur Ausübung von Betroffenenrechten gemäß § 11 dieses AVV,
- f) Verarbeitungen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit (insbesondere Protokollierung, Datensicherung, Fehlermonitoring) gemäß der in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen.

(3) **Zweck der Verarbeitung** Die Verarbeitung dient ausschließlich der Erbringung der vertragsgegenständlichen Leistungen gemäß dem Hauptvertrag sowie der Erfüllung gesetzlicher Verpflichtungen des Auftragsverarbeiters. Eine Verarbeitung der Kundendaten zu eigenen Zwecken des Auftragsverarbeiters – insbesondere zur Erstellung personenbezogener Profile, zu Werbezwecken oder zum Training eigener oder fremder Modelle künstlicher Intelligenz – findet nicht statt; abweichende Regelungen für die zweckgebundene Nutzung anonymisierter Daten zur Produktverbesserung bleiben § 7 vorbehalten.

(4) **Dauer der Verarbeitung** Die Auftragsverarbeitung beginnt mit Wirksamwerden dieses AVV und endet mit Beendigung des Hauptvertrages, soweit nicht aufgrund gesetzlicher Aufbewahrungspflichten oder zur Erfüllung nachvertraglicher Pflichten (insbesondere gemäß § 16 dieses AVV) eine längere Speicherung erforderlich ist.

(5) **Art und Kategorien betroffener Personen sowie Datenkategorien** Die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen ergeben sich aus Anlage 1.

(6) **Ort der Verarbeitung** Die Verarbeitung der Kundendaten findet grundsätzlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums statt. Soweit Subunternehmer eingesetzt werden, deren Sitz außerhalb des EWR liegt oder die ihrerseits Subunternehmer in Drittländern einsetzen, gilt § 15 dieses AVV.

§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) **Datenkategorien** Im Rahmen der Auftragsverarbeitung werden personenbezogene Daten der in Anlage 1 näher bezeichneten Art verarbeitet. Anlage 1 enthält insbesondere Angaben zu:

- a) Stamm- und Kontaktdaten, b) Auftrags-, Termin- und Einsatzdaten, c) Kommunikationsdaten, d) technischen und Nutzungsmetadaten sowie e) besonderen Kategorien personenbezogener Daten gemäß Absatz (3).

(2) **Kategorien betroffener Personen** Von der Auftragsverarbeitung sind die in Anlage 1 näher bezeichneten Kategorien betroffener Personen erfasst, insbesondere:

a) Nutzer des Verantwortlichen, b) Beschäftigte des Verantwortlichen, c) Endkunden des Verantwortlichen (soweit natürliche Personen oder deren Ansprechpartner) sowie d) Ansprechpartner bei Lieferanten und sonstigen Geschäftspartnern des Verantwortlichen.

(3) **Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)** Im Rahmen der Beschäftigten-Abwesenheitsverwaltung kann der Verantwortliche Daten erfassen, die besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO unterfallen können, insbesondere:

a) Abwesenheitsstatus mit der Kennzeichnung „krank“ oder einer gleichbedeutenden Statuskennzeichnung, b) Zeitraum der Abwesenheit, c) freiwillige Angaben des Verantwortlichen oder seiner Nutzer in einem hierfür vorgesehenen Notizfeld, deren Einordnung sich nach dem jeweils eingegebenen Inhalt richtet.

Darüber hinaus kann der Verantwortliche in den über die App bereitgestellten Freitext-, Notiz- und Kommentarfeldern sowie über die Upload-/Anhangfunktionen (insbesondere Bilddateien/Fotos) nach eigenem Ermessen Angaben erfassen bzw. Inhalte hochladen, die im Einzelfall besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO enthalten können. Der Auftragsverarbeiter fordert die Erfassung besonderer Kategorien personenbezogener Daten nicht und richtet die genannten Felder und Funktionen nicht gezielt auf deren Erfassung aus. Der Verantwortliche stellt sicher, dass er besondere Kategorien personenbezogener Daten nicht in Freitextfelder oder Upload-/Anhangfunktionen einbringt, soweit er hierfür nicht über eine eigenständige Rechtsgrundlage verfügt; dies gilt insbesondere, soweit Eingaben oder hochgeladene Inhalte automatisiert mittels KI-Modellen verarbeitet werden (§ 7 AVV). Soweit der Verantwortliche solche Daten dennoch erfasst, erfolgt deren Verarbeitung durch den Auftragsverarbeiter ausschließlich auf Weisung und im Rahmen der eigenständigen Rechtsgrundlage des Verantwortlichen.

Der Auftragsverarbeiter erhebt selbst keine medizinischen Diagnosen, ärztlichen Bescheinigungen oder vergleichbaren Gesundheitsdaten und bietet keine Funktion zum Upload solcher Dokumente an. Die Verarbeitung der vorgenannten Daten erfolgt durch den Auftragsverarbeiter ausschließlich auf Weisung und im Rahmen der eigenständigen Rechtsgrundlage des Verantwortlichen (insbesondere für Gesundheitsdaten im Beschäftigungskontext Art. 9 Abs. 2 lit. b DSGVO i.V.m. § 26 Abs. 3 BDSG).

Die ergänzenden Pflichten des Verantwortlichen im Zusammenhang mit der Verarbeitung besonderer Kategorien personenbezogener Daten regelt § 6 dieses AVV.

(4) **Aktualisierung der Anlage 1** Wesentliche Änderungen der Art der verarbeiteten Daten oder der Kategorien betroffener Personen werden vom Auftragsverarbeiter durch Aktualisierung der Anlage 1 dokumentiert. Der Auftragsverarbeiter informiert den Verantwortlichen über wesentliche Änderungen mit angemessenem Vorlauf, mindestens jedoch 30 Tage vor Inkrafttreten, durch Mitteilung in Textform. Geringfügige redaktionelle Anpassungen (insbesondere zur Klarstellung) bleiben hiervon unberührt.

§ 4 Weisungsrecht und Weisungsdokumentation

(1) **Verarbeitung nur auf dokumentierte Weisung** Der Auftragsverarbeiter verarbeitet die Kundendaten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dies gilt auch für die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) **Standardweisungen aus dem Vertrag** Die zur Erbringung der vertragsgegenständlichen Leistungen erforderlichen Verarbeitungen gelten als durch den Hauptvertrag, diesen AVV nebst Anlagen sowie durch

die Nutzung der App durch den Verantwortlichen und seine Nutzer dokumentiert weisungsmäßig veranlasst. Hierzu zählen insbesondere Verarbeitungen im Rahmen der in § 2 Abs. 2 dieses AVV beschriebenen Verarbeitungsarten sowie der in Anlage 1 beschriebenen Verarbeitungstätigkeiten.

(3) **Form von Einzelweisungen** Weisungen, die über die Standardweisungen nach Absatz 2 hinausgehen, erteilt der Verantwortliche in Textform (§ 126b BGB). Die Textform ist insbesondere durch E-Mail an datenschutz@blinkpilot.com oder durch eine etwaige vom Auftragsverarbeiter im Kundenaccount bereitgestellte Weisungsfunktion gewahrt. Der Auftragsverarbeiter setzt nur Weisungen um, die in Textform erteilt wurden.

(4) **Weisungsberechtigte Personen** Weisungsberechtigt auf Seiten des Verantwortlichen sind die im Account des Verantwortlichen mit der Rolle „Administrator“ oder „Inhaber“ geführten Nutzer. Die Benennung weiterer weisungsberechtigter Personen kann ausschließlich durch den primären Accountinhaber oder einen Nutzer mit der Rolle „Inhaber“ erfolgen; sie erfolgt durch Mitteilung an datenschutz@blinkpilot.com unter Angabe von Name, Funktion und E-Mail-Adresse der zu benennenden Person und wird mit Bestätigung durch den Auftragsverarbeiter wirksam. Der Auftragsverarbeiter kann zur Bestätigung eine schriftliche Vollmacht des primären Accountinhabers verlangen. Der Auftragsverarbeiter dokumentiert die benannten weisungsberechtigten Personen in geeigneter Weise; soweit hierfür eine Funktion im Kundenaccount bereitgestellt wird, werden die Personen dort geführt. Weisungsempfänger auf Seiten des Auftragsverarbeiters ist die unter datenschutz@blinkpilot.com erreichbare Stelle. Der Auftragsverarbeiter darf auf die im Account des Verantwortlichen hinterlegten Rollenzuweisungen sowie auf die ihm nach diesem Absatz benannten weisungsberechtigten Personen vertrauen. Weisungen, die von einer im Account mit der Rolle „Administrator“ oder „Inhaber“ geführten Person oder von einer benannten weisungsberechtigten Person erteilt werden, gelten als wirksam vom Verantwortlichen veranlasst. Der Verantwortliche ist für die ordnungsgemäße und aktuelle Pflege der Rollen- und Berechtigungszuweisungen in seinem Account verantwortlich; eine fehlerhafte, unterlassene oder nicht rechtzeitig aktualisierte Vergabe oder Entziehung von Berechtigungen muss er sich zurechnen lassen. Eine darüber hinausgehende Prüfung der Vertretungsmacht weisender Personen schuldet der Auftragsverarbeiter nicht.

(5) **Hinweispflicht bei unzulässigen Weisungen** Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Vorschriften verstößt, teilt er dies dem Verantwortlichen unverzüglich mit. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung durch den Verantwortlichen auszusetzen. Die Pflicht zur Mitteilung gilt auch dann, wenn der Auftragsverarbeiter offenkundige Verstöße gegen diesen AVV feststellt.

(6) **Dokumentation** Der Auftragsverarbeiter dokumentiert die Weisungen des Verantwortlichen und ihre Umsetzung in geeigneter Weise und stellt diese Dokumentation dem Verantwortlichen auf begründete Anfrage zur Verfügung. Standardweisungen nach Absatz 2 sind durch den Hauptvertrag, diesen AVV und die in der App protokollierten Nutzeraktivitäten dokumentiert; einer gesonderten Dokumentation bedarf es insoweit nicht.

§ 5 Pflichten des Auftragsverarbeiters

(1) **Verarbeitung nach Weisung** Der Auftragsverarbeiter verarbeitet die Kundendaten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Maßgabe der dokumentierten Weisungen des Verantwortlichen (§ 4). Eine Verarbeitung der Kundendaten zu eigenen Zwecken des Auftragsverarbeiters – mit Ausnahme der in § 2 Abs. 3 dieses AVV vorbehaltenen Verarbeitungen – findet nicht statt. Wird der

Auftragsverarbeiter durch das Recht der Union oder eines Mitgliedstaats, dem er unterliegt, zu einer abweichenden Verarbeitung verpflichtet, gilt § 4 Abs. 1 Satz 2 entsprechend.

(2) **Vertraulichkeit der zur Verarbeitung befugten Personen** Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Kundendaten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeitsverpflichtung wirkt auch nach Beendigung des jeweiligen Beschäftigungs- oder Dienstverhältnisses fort. Weitere Einzelheiten regelt § 9 dieses AVV.

(3) **Technische und organisatorische Maßnahmen** Der Auftragsverarbeiter trifft alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung. Die zum Zeitpunkt des Abschlusses dieses AVV getroffenen Maßnahmen sind in Anlage 2 beschrieben. § 10 dieses AVV regelt das Verfahren zur Anpassung der Maßnahmen.

(4) **Inanspruchnahme von Subunternehmern** Der Auftragsverarbeiter nimmt Subunternehmer nur nach Maßgabe von § 8 dieses AVV in Anspruch.

(5) **Unterstützung des Verantwortlichen bei Betroffenenrechten** Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seinen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Personen nachzukommen, soweit dies möglich ist. § 11 dieses AVV regelt die Einzelheiten.

(6) **Unterstützung des Verantwortlichen bei Sicherheit, Meldepflichten und Datenschutz-Folgenabschätzung** Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten, insbesondere

a) bei der Sicherstellung des Sicherheitsniveaus der Verarbeitung (Art. 32 DSGVO), b) bei der Meldung von Datenschutzverletzungen an die Aufsichtsbehörde sowie der Benachrichtigung betroffener Personen (Art. 33, 34 DSGVO; § 12 dieses AVV), c) bei der Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO; § 13 dieses AVV) sowie d) bei der vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DSGVO; § 13 dieses AVV).

Für Umfang, Reaktionsfristen und Vergütung der Unterstützungsleistungen nach diesem Absatz gelten § 11 Abs. 6, § 12 sowie § 13 dieses AVV. Die Reaktionsfristen des § 11 Abs. 5 finden auf die Unterstützung nach lit. c und lit. d keine Anwendung; maßgeblich sind insoweit die jeweiligen gesetzlichen Fristen, innerhalb derer der Verantwortliche seinen eigenen Pflichten nach Art. 35, 36 DSGVO nachzukommen hat.

(7) **Löschung oder Rückgabe nach Beendigung** Nach Beendigung der vertragsgegenständlichen Leistungen löscht oder gibt der Auftragsverarbeiter die Kundendaten nach Wahl des Verantwortlichen zurück, soweit nicht eine gesetzliche Verpflichtung zur weiteren Speicherung besteht. § 16 dieses AVV regelt die Einzelheiten.

(8) **Nachweis- und Informationspflichten** Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO und in diesem AVV niedergelegten Pflichten zur Verfügung. Insbesondere ermöglicht er Überprüfungen – einschließlich Inspektionen – durch den Verantwortlichen oder einen von diesem beauftragten Prüfer nach Maßgabe von § 14 dieses AVV und trägt zu diesen Überprüfungen bei.

(9) **Verzeichnis der Verarbeitungstätigkeiten** Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO. Er stellt dieses Verzeichnis auf Anfrage der zuständigen Aufsichtsbehörde sowie auf

begründete Anfrage des Verantwortlichen – jeweils bezogen auf die diesen betreffenden Verarbeitungen – zur Verfügung.

(10) **Datenschutzbeauftragter** Der Auftragsverarbeiter ist gegenwärtig nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet (§ 38 Abs. 1 BDSG). Die zentrale Ansprechstelle für datenschutzrechtliche Angelegenheiten ist unter datenschutz@blinkpilot.com erreichbar. Im Falle einer gesetzlichen Bestellungspflicht oder einer freiwilligen Bestellung informiert der Auftragsverarbeiter den Verantwortlichen über die Kontaktdaten des Datenschutzbeauftragten.

(11) **Hinweispflicht bei Datenschutzverletzungen** Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Datenschutzverletzungen, die Kundendaten betreffen. § 12 dieses AVV regelt die Einzelheiten.

§ 6 Pflichten des Verantwortlichen

(1) **Datenschutzrechtliche Verantwortlichkeit** Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung der Kundendaten sowie für die Wahrung der Rechte der betroffenen Personen allein verantwortlich (Art. 5 Abs. 2, Art. 24 DSGVO). Dies umfasst insbesondere

a) das Vorliegen einer Rechtsgrundlage für die durch ihn veranlassten Verarbeitungen (Art. 6, ggf. Art. 9 DSGVO), b) die Wahrung der Grundsätze des Art. 5 DSGVO (Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit), c) die Erfüllung der Informationspflichten nach Art. 13, 14 DSGVO gegenüber den betroffenen Personen sowie d) die Erfüllung etwaiger Pflichten zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und zur vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DSGVO).

(2) **Information eingeladener Nutzer** Der Verantwortliche stellt sicher, dass von ihm eingeladene Nutzer (insbesondere Beschäftigte) vor erstmaliger Nutzung der App über die Verarbeitung ihrer personenbezogenen Daten gemäß Art. 13 DSGVO informiert werden. Hierzu zählen insbesondere Angaben zum Verantwortlichen, zu den Zwecken und Rechtsgrundlagen, zur Dauer der Speicherung sowie zu den Betroffenenrechten. Die Erfüllung der Informationspflichten nach Art. 13 DSGVO gegenüber den eingeladenen Nutzern obliegt allein dem Verantwortlichen.

(3) **Beschäftigtendatenschutz** Soweit der Verantwortliche die App zur Verarbeitung personenbezogener Daten seiner Beschäftigten nutzt, beachtet er die Anforderungen des § 26 BDSG sowie etwaige weitere arbeitsrechtliche Vorgaben (insbesondere Mitbestimmungsrechte des Betriebsrats nach §§ 87 Abs. 1 Nr. 6, 80 Abs. 2 BetrVG, soweit ein Betriebsrat besteht). Die Verantwortung für etwaige Beteiligungsverfahren und für die Information der Beschäftigten liegt beim Verantwortlichen.

(4) **Besondere Kategorien personenbezogener Daten** Der Verantwortliche stellt sicher, dass er für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO – insbesondere der in § 3 Abs. 3 dieses AVV genannten Gesundheitsdaten – über eine eigenständige Rechtsgrundlage verfügt. Der Verantwortliche stellt durch geeignete organisatorische Maßnahmen sicher, dass die über die App bereitgestellten Freitext-, Notiz- und Kommentarfelder sowie die Upload-/Anhangfunktionen (insbesondere für Bilddateien/Fotos) – einschließlich des in § 3 Abs. 3 lit. c dieses AVV genannten Notizfeldes – nicht für die Erfassung besonderer Kategorien personenbezogener Daten genutzt werden, für die der Verantwortliche nicht über eine eigenständige Rechtsgrundlage verfügt. Hierzu zählen insbesondere Hinweise an die Nutzer im Rahmen der internen Schulung sowie die Beobachtung der tatsächlichen Nutzung dieser Felder.

(5) **Rechtmäßigkeit der eingegebenen Daten** Der Verantwortliche gewährleistet, dass er zur Eingabe und Verarbeitung der von ihm in die App eingestellten Daten berechtigt ist und insbesondere keine Rechte Dritter verletzt. Sofern der Verantwortliche personenbezogene Daten Dritter (insbesondere von

Endkunden und Lieferanten) in die App einstellt, versichert er, dass er hierzu nach den anwendbaren datenschutzrechtlichen Vorschriften berechtigt ist und – soweit erforderlich – die betroffenen Personen über die Verarbeitung informiert hat.

(6) **Pflichten bei der Nutzung KI-gestützter Funktionen** Soweit der Verantwortliche KI-gestützte Funktionen der App nutzt, beachtet er die in § 7 dieses AVV geregelten zusätzlichen Pflichten.

(7) **Mitwirkungspflichten** Der Verantwortliche stellt dem Auftragsverarbeiter die für die ordnungsgemäße Erbringung der Auftragsverarbeitung erforderlichen Informationen und Mitwirkungsleistungen rechtzeitig zur Verfügung. Dies umfasst insbesondere

a) die Benennung weisungsberechtigter Personen (§ 4 Abs. 4), b) die unverzügliche Mitteilung erkennbarer Fehler oder Auffälligkeiten in der Verarbeitung, c) die Information des Auftragsverarbeiters über für die Auftragsverarbeitung wesentliche Änderungen auf Seiten des Verantwortlichen (insbesondere Übergänge der Verantwortlichkeit, gesellschaftsrechtliche Änderungen mit Auswirkungen auf die Datenverarbeitung).

(8) **Aufsichtsbehördliche Anfragen und Anfragen betroffener Personen** Wendet sich eine Aufsichtsbehörde oder eine betroffene Person unmittelbar an den Auftragsverarbeiter in Bezug auf Verarbeitungen, für die der Verantwortliche datenschutzrechtlich verantwortlich ist, leitet der Auftragsverarbeiter die Anfrage unverzüglich an den Verantwortlichen weiter und unterstützt diesen bei der Beantwortung nach Maßgabe von § 11 dieses AVV. Der Verantwortliche ist verpflichtet, derartige weitergeleitete Anfragen ordnungsgemäß und fristgerecht zu beantworten.

§ 7 Besondere Bestimmungen für KI-gestützte Verarbeitung

(1) **Gegenstand** Die App stellt KI-gestützte Funktionen bereit. Zur Bereitstellung dieser Funktionen übermittelt der Auftragsverarbeiter Kundendaten an einen externen KI-Anbieter, der als Subunternehmer im Sinne des Art. 28 Abs. 2, 4 DSGVO tätig wird. Die konkreten KI-Funktionen ergeben sich aus dem Hauptvertrag und der jeweils aktuellen Leistungsbeschreibung in der App. Der eingesetzte KI-Anbieter sowie der Verarbeitungsort ergeben sich aus Anlage 3.

(2) **Datenminimierung** Der Auftragsverarbeiter übermittelt an den KI-Anbieter ausschließlich diejenigen Kundendaten, die für die Ausführung der jeweils ausgelösten KI-Funktion erforderlich sind. Der Auftragsverarbeiter trifft geeignete Maßnahmen, um die an den KI-Anbieter übermittelten Kundendaten und die den KI-Funktionen zur Verfügung stehenden Datenzugriffe auf den jeweiligen Funktionszweck zu beschränken. Eine über den jeweiligen Funktionszweck hinausgehende, anlasslose oder vorsorgliche Übermittlung von Kundendaten an den KI-Anbieter findet nicht statt.

(3) **Ausschluss der Nutzung zu Trainingszwecken** Der Auftragsverarbeiter stellt vertraglich sicher, dass der eingesetzte KI-Anbieter die im Rahmen der KI-Funktionen übermittelten Kundendaten weder zum Training noch zur Weiterentwicklung eigener oder fremder Modelle künstlicher Intelligenz nutzt. Dies gilt auch für eine etwaige Anonymisierung der Kundendaten zu Trainingszwecken.

(4) **Speicherdauer beim KI-Anbieter** Der Auftragsverarbeiter setzt KI-Anbieter ein, die die übermittelten Kundendaten nicht zum Training von Modellen künstlicher Intelligenz nutzen (Absatz 3) und die übermittelten Daten nach Abschluss der jeweiligen Verarbeitung löschen, soweit nicht eine kurzfristige Speicherung zur Sicherheits- und Missbrauchskontrolle erforderlich ist. Diese Speicherung zur Missbrauchskontrolle beträgt bei den eingesetzten KI-Anbietern in der Regel bis zu 30 Tage. Eine darüber hinausgehende Speicherung einzelner Eingaben und Ausgaben kann ausnahmsweise erfolgen, soweit der KI-Anbieter hierzu gesetzlich verpflichtet ist oder dies zur Verfolgung von Verstößen gegen seine Nutzungsbedingungen erforderlich ist; in diesen Fällen kann die Speicherdauer länger sein. Die konkrete Ausgestaltung ergibt sich aus den mit den jeweiligen KI-Anbietern geschlossenen

Auftragsverarbeitungsverträgen, die auf Anfrage in der jeweils aktuellen öffentlichen Fassung bereitgestellt werden.

(5) **Verantwortung für den Output** Die durch KI-Funktionen erzeugten Inhalte sind als Vorschläge zu verstehen und ersetzen keine fachliche Prüfung durch den Verantwortlichen. Die Prüfung und Freigabe KI-generierter Inhalte vor deren Verwendung gegenüber Dritten obliegt dem Verantwortlichen. Der Auftragsverarbeiter übernimmt keine Verantwortung für die inhaltliche Korrektheit, Vollständigkeit oder Eignung KI-generierter Ausgaben.

(6) **Transparenzpflichten gegenüber Betroffenen** Soweit der Verantwortliche KI-generierte Ausgaben gegenüber betroffenen Personen verwendet, beachtet er etwaige Transparenzpflichten nach Art. 50 der Verordnung (EU) 2024/1689 (KI-Verordnung). Der Auftragsverarbeiter weist im Rahmen der App auf das Vorliegen KI-generierter Inhalte hin, soweit dies technisch sinnvoll und für den Verantwortlichen erkennbar ist. Eine darüber hinausgehende Kennzeichnung gegenüber Dritten und betroffenen Personen sowie die Erfüllung der Transparenzpflichten nach Art. 50 der Verordnung (EU) 2024/1689 obliegen dem Verantwortlichen.

(7) **Keine automatisierte Entscheidungsfindung mit Rechtswirkung** Die KI-Funktionen der App treffen keine automatisierten Entscheidungen, die gegenüber betroffenen Personen rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (Art. 22 DSGVO). Sofern der Verantwortliche Ausgaben der KI-Funktionen als Grundlage für derartige Entscheidungen verwenden möchte, liegt die diesbezügliche Verantwortung – einschließlich der Erfüllung der Voraussetzungen des Art. 22 Abs. 2 bis 4 DSGVO – beim Verantwortlichen.

(8) **Risikoeinstufung nach der KI-Verordnung** Die in der App bereitgestellten KI-Funktionen stellen nach derzeitiger Einschätzung des Auftragsverarbeiters KI-Systeme mit minimalem Risiko im Sinne der Verordnung (EU) 2024/1689 dar. Eine Einordnung als Hochrisiko-KI-System gemäß Art. 6 i.V.m. Anhang III der KI-Verordnung erfolgt nicht. Sollte sich diese Einschätzung aufgrund von Funktionserweiterungen oder geänderter Rechtslage ändern, wird der Auftragsverarbeiter den Verantwortlichen unterrichten und die erforderlichen Anpassungen vornehmen.

(9) **Wechsel des KI-Anbieters** Der Wechsel des in Anlage 3 benannten KI-Anbieters richtet sich nach den Regelungen für Subunternehmerwechsel gemäß § 8 dieses AVV.

§ 8 Subunternehmer

(1) **Inanspruchnahme von Subunternehmern** Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter (Subunternehmer) zur Erbringung der vertragsgegenständlichen Leistungen einzusetzen, soweit dies nach Maßgabe dieses Paragraphen geschieht.

(2) **Allgemeine Vorabgenehmigung** Der Verantwortliche erteilt dem Auftragsverarbeiter hiermit die allgemeine schriftliche Genehmigung im Sinne des Art. 28 Abs. 2 Satz 1 DSGVO zur Inanspruchnahme der in Anlage 3 zum Zeitpunkt des Abschlusses dieses AVV aufgeführten Subunternehmer.

(3) **Pflichten bei der Auswahl und Einbindung** Der Auftragsverarbeiter wählt Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen aus. Er stellt sicher, dass dem Subunternehmer im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten Datenschutzpflichten auferlegt werden, die den in diesem AVV festgelegten Pflichten im Schutzniveau entsprechen, insbesondere die Anforderungen des Art. 28 Abs. 4 DSGVO erfüllen. Dieser Anforderung wird insbesondere genügt, wenn der Subunternehmer einen den Vorgaben des Art. 28 DSGVO entsprechenden Auftragsverarbeitungsvertrag oder eine vergleichbare Datenschutzvereinbarung (insbesondere auf Grundlage der Standardvertragsklauseln) abschließt. Insbesondere stellt der

Auftragsverarbeiter sicher, dass hinreichende Garantien dafür geboten werden, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt.

(4) **Wechsel und Hinzuziehung weiterer Subunternehmer** Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder den Wechsel von Subunternehmern grundsätzlich mit einem Vorlauf von mindestens 30 Tagen vor Inkrafttreten der Änderung. Die Information erfolgt in Textform an die im Account des Verantwortlichen hinterlegte E-Mail-Adresse des primären Accountinhabers.

Bei sicherheitsbedingt erforderlichen Sofortmaßnahmen (insbesondere zur Abwehr akuter Sicherheitsrisiken, zur Behebung eines Ausfalls eines bisherigen Subunternehmers oder zur Erfüllung behördlicher Anordnungen) kann die Information auch unverzüglich nach Inkrafttreten der Änderung erfolgen. Der Auftragsverarbeiter dokumentiert in diesem Fall die Gründe für die Sofortmaßnahme. Das Widerspruchsrecht nach Absatz 5 bleibt unberührt; die Widerspruchsfrist beträgt in diesen Fällen 14 Tage ab Zugang der Information. Bis zum Ablauf der Widerspruchsfrist sowie im Falle eines fristgerechten Widerspruchs bis zur Klärung nach Absatz 6 ist der Auftragsverarbeiter berechtigt, den im Wege der Sofortmaßnahme hinzugezogenen oder gewechselten Subunternehmer einzusetzen, soweit dies zur Aufrechterhaltung der Sicherheit und Verfügbarkeit der App erforderlich ist. Die Anforderungen an das Schutzniveau (Absatz 3) sowie an geeignete Garantien bei Drittlandbezug (§ 15 dieses AVV) bleiben hiervon unberührt. Im Falle eines fristgerechten Widerspruchs gilt das Verfahren nach Absatz 6 entsprechend.

(5) **Widerspruchsrecht** Der Verantwortliche kann der Hinzuziehung oder dem Wechsel eines Subunternehmers aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen nach Zugang der Information widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn der neue Subunternehmer offensichtlich nicht in der Lage ist, ein dem bisherigen Subunternehmer vergleichbares Schutzniveau zu gewährleisten, oder wenn der Wechsel zu einer wesentlichen Verschlechterung der datenschutzrechtlichen Situation des Verantwortlichen führen würde.

(6) **Folgen eines Widerspruchs** Im Falle eines fristgerechten Widerspruchs erörtern die Parteien den Widerspruchgrund. Der Auftragsverarbeiter prüft, ob dem Widerspruchgrund durch verhältnismäßige Maßnahmen Rechnung getragen werden kann; er ist hierzu jedoch nicht verpflichtet, soweit dies mit einem standardisierten Betrieb der App nicht vereinbar ist. Hält der Auftragsverarbeiter an der Hinzuziehung oder dem Wechsel des Subunternehmers fest, teilt er dem Verantwortlichen die Gründe in Textform mit. Der Verantwortliche ist in diesem Fall berechtigt, den Hauptvertrag mit einer Frist von 30 Tagen außerordentlich zu kündigen. § 16 dieses AVV gilt entsprechend.

(7) **Haftung für Subunternehmer** Soweit ein Subunternehmer seinen Datenschutzpflichten nicht nachkommt, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmers (Art. 28 Abs. 4 Satz 2 DSGVO). § 17 dieses AVV bleibt im Übrigen unberührt.

(8) **Konzerninterne Subunternehmer** Konzerninterne Subunternehmer (insbesondere verbundene Unternehmen im Sinne der §§ 15 ff. AktG des Auftragsverarbeiters oder eines bestehenden Subunternehmers) gelten für Zwecke dieses AVV als Subunternehmer im Sinne der vorstehenden Absätze und sind in Anlage 3 entsprechend zu kennzeichnen, sofern sie Kundendaten verarbeiten.

(9) **Begriffliche Abgrenzung** Nicht als Subunternehmer im Sinne dieses Paragraphen gelten Dienstleister, die im Rahmen ihrer Tätigkeit gegenüber dem Auftragsverarbeiter selbst Verantwortliche sind (insbesondere Zahlungsdienstleister im Rahmen der Vertragsabwicklung zwischen Auftragsverarbeiter und Verantwortlichem). Die diesbezüglichen Verarbeitungen sind nicht Gegenstand dieses AVV.

§ 9 Vertraulichkeit

(1) **Verpflichtung der zur Verarbeitung befugten Personen** Der Auftragsverarbeiter verpflichtet alle Personen, die im Auftrag des Verantwortlichen Kundendaten verarbeiten, vor Aufnahme der Tätigkeit zur Vertraulichkeit. Die Verpflichtung erfolgt schriftlich oder in einer geeigneten elektronischen Form mit Unterzeichnungsnachweis. Soweit die betreffenden Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, kann auf eine gesonderte Verpflichtung verzichtet werden.

(2) **Inhalt der Verpflichtung** Die Verpflichtung umfasst insbesondere

a) die Pflicht zur vertraulichen Behandlung der Kundendaten und sonstiger im Rahmen der Tätigkeit zur Kenntnis gelangter Informationen, b) die Pflicht, Kundendaten ausschließlich im Rahmen der zugewiesenen Aufgaben und nach Weisung des Auftragsverarbeiters zu verarbeiten, c) das Verbot, Kundendaten zu eigenen Zwecken oder zugunsten Dritter zu nutzen, d) die Pflicht zur Beachtung der datenschutzrechtlichen Vorgaben, insbesondere des Datengeheimnisses gemäß § 53 BDSG.

(3) **Fortwirkung** Die Vertraulichkeitsverpflichtung wirkt auch nach Beendigung des jeweiligen Beschäftigungs-, Dienst- oder Auftragsverhältnisses fort.

(4) **Schulung und Sensibilisierung** Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung befugten Personen über die einschlägigen datenschutzrechtlichen Vorgaben sowie über die für ihren Tätigkeitsbereich relevanten technischen und organisatorischen Maßnahmen angemessen geschult und regelmäßig sensibilisiert werden. Inhalte und Häufigkeit der Schulungen werden vom Auftragsverarbeiter unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung festgelegt.

(5) **Verpflichtung weiterer Personen** Soweit der Auftragsverarbeiter zur Erbringung der vertragsgegenständlichen Leistungen freie Beschäftigte, externe Dienstleister oder sonstige Auftragnehmer einsetzt, die nicht Subunternehmer im Sinne des § 8 dieses AVV sind und Zugang zu Kundendaten erhalten, gelten die Absätze (1) bis (4) entsprechend.

(6) **Nachweis** Der Auftragsverarbeiter dokumentiert die Vertraulichkeitsverpflichtungen und die durchgeführten Schulungen in geeigneter Weise. Auf begründete Anfrage des Verantwortlichen legt er geeignete Nachweise vor; ein Recht auf Einsicht in einzelne Verpflichtungserklärungen oder Personalakten besteht nicht.

§ 10 Technische und organisatorische Maßnahmen

(1) **Verpflichtung zur Umsetzung** Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (nachfolgend „TOM“), um ein dem Risiko angemessenes Schutzniveau für die Kundendaten zu gewährleisten. Bei der Festlegung der Maßnahmen berücksichtigt der Auftragsverarbeiter den Stand der Technik, die Implementierungskosten sowie die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ebenso wie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

(2) **Beschreibung der TOM** Die zum Zeitpunkt des Abschlusses dieses AVV getroffenen Maßnahmen sind in Anlage 2 beschrieben. Die in Anlage 2 enthaltene Beschreibung erfasst insbesondere Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen.

(3) **Anpassung der TOM** Der Auftragsverarbeiter ist berechtigt und – soweit erforderlich – verpflichtet, die TOM während der Laufzeit dieses AVV anzupassen und fortzuentwickeln, um ein dem jeweiligen

Stand der Technik und der Risikolage entsprechendes Schutzniveau aufrechtzuerhalten. Eine Anpassung der TOM darf nicht zu einer wesentlichen Unterschreitung des in Anlage 2 beschriebenen Schutzniveaus führen.

(4) **Information bei wesentlichen Änderungen** Der Auftragsverarbeiter informiert den Verantwortlichen über wesentliche Änderungen der TOM in Textform oder durch Bereitstellung einer aktualisierten Fassung der Anlage 2 in einem für den Verantwortlichen zugänglichen Bereich. Eine Information vor Inkrafttreten erfolgt, soweit dies möglich und angemessen ist; bei sicherheitsbedingten Sofortmaßnahmen kann die Information auch unverzüglich nach Inkrafttreten erfolgen.

(5) **Bewertung durch den Verantwortlichen** Der Verantwortliche hat die in Anlage 2 beschriebenen TOM zur Kenntnis genommen und bestätigt, dass sie unter Berücksichtigung der Art der von ihm in die App eingestellten Daten ein angemessenes Schutzniveau im Sinne des Art. 32 DSGVO gewährleisten. Der Verantwortliche entscheidet eigenverantwortlich, ob die in Anlage 2 beschriebenen Maßnahmen für die von ihm beabsichtigten Verarbeitungen ausreichen. Hält der Verantwortliche aufgrund der besonderen Sensibilität der von ihm verarbeiteten Daten ein höheres als das in Anlage 2 beschriebene Schutzniveau für erforderlich, obliegt es ihm, von der Eingabe solcher Daten in die App abzusehen. Die App wird als standardisierte Mehrmandantenlösung bereitgestellt; ein Anspruch des Verantwortlichen auf individuelle Anpassung der technischen und organisatorischen Maßnahmen besteht nicht.

(6) **Mitwirkung an Sicherheitsbewertungen** Auf begründete Anfrage des Verantwortlichen stellt der Auftragsverarbeiter die zum Nachweis der Einhaltung seiner Pflichten erforderlichen Informationen zu den getroffenen TOM nach Maßgabe von § 14 Abs. 2 dieses AVV zur Verfügung, soweit dies zur Erfüllung der datenschutzrechtlichen Pflichten des Verantwortlichen erforderlich ist. Die Einzelheiten der Auskunfts- und Auditrechte, einschließlich der Häufigkeit und der Vergütung, regelt § 14 dieses AVV.

§ 11 Unterstützung bei Betroffenenrechten

(1) **Unterstützungspflicht** Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seinen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Art. 12 bis 22 DSGVO niedergelegten Rechte betroffener Personen nachzukommen, soweit dies möglich ist (Art. 28 Abs. 3 lit. e DSGVO).

(2) **Direkte Anfragen betroffener Personen** Wendet sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte nach Art. 15 bis 22 DSGVO unmittelbar an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter, sofern die Anfrage erkennbar Kundendaten betrifft, für die der Verantwortliche datenschutzrechtlich verantwortlich ist. Der Auftragsverarbeiter erteilt in diesen Fällen keine eigene inhaltliche Auskunft, kann jedoch die betroffene Person an den Verantwortlichen verweisen und diesen unverzüglich entsprechend benachrichtigen.

(3) **Bereitgestellte Funktionalitäten** Zur Erleichterung der Wahrnehmung der Betroffenenrechte stellt der Auftragsverarbeiter dem Verantwortlichen über die App geeignete Funktionalitäten zur Verfügung, insbesondere

a) Funktionen zur Einsicht, Berichtigung und Löschung einzelner Datensätze im Rahmen der jeweiligen App-Module, b) eine Datenexportfunktion in strukturierten, gängigen und maschinenlesbaren Formaten (insbesondere CSV und PDF) zur Unterstützung des Rechts auf Datenübertragbarkeit (Art. 20 DSGVO).

Soweit die zur Beantwortung eines Antrags erforderlichen Informationen über die App-Funktionen abgerufen oder bereitgestellt werden können, gilt die Unterstützungspflicht durch die Bereitstellung der App-Funktionalität als erfüllt.

(4) **Ergänzende Unterstützung** Soweit die App-Funktionen für die Beantwortung eines konkreten Antrags nicht ausreichen, leistet der Auftragsverarbeiter dem Verantwortlichen auf begründete Anfrage in Textform ergänzende Unterstützung. Diese umfasst insbesondere

a) die Bereitstellung erforderlicher Informationen aus den Systemen des Auftragsverarbeiters, b) die Mitwirkung bei der Identifikation betroffener Datensätze, c) die Durchführung einer Datenlöschung in aktiven Systemen, in denen der Verantwortliche selbst keine direkte Löschmöglichkeit hat. Eine gezielte Einzellöschung aus Backup-Systemen erfolgt nicht; insoweit gilt die Rotations- und Trennungslogik nach § 16 Abs. 4 dieses AVV entsprechend.

(5) **Reaktionsfristen** Der Auftragsverarbeiter bearbeitet Anfragen nach den Absätzen (2) und (4) ohne unangemessene Verzögerung, in der Regel innerhalb von 15 Werktagen nach Zugang der Anfrage. Diese Frist trägt der Tatsache Rechnung, dass die gesetzliche Antwortfrist des Verantwortlichen gegenüber der betroffenen Person nach Art. 12 Abs. 3 DSGVO einen Monat, in komplexen Fällen bis zu drei Monate beträgt.

Die Frist verlängert sich angemessen bei Vorliegen objektiver Hinderungsgründe auf Seiten des Auftragsverarbeiters, insbesondere bei Krankheit, Urlaub, Betriebsferien, technischen Störungen oder vergleichbaren Umständen. Zeichnet sich ab, dass ein Hinderungsgrund die Einhaltung der Frist nach Satz 1 verhindert, teilt der Auftragsverarbeiter dies dem Verantwortlichen unverzüglich mit, sobald ihm dies möglich und zumutbar ist, damit der Verantwortliche die ihm gegenüber der betroffenen Person zur Verfügung stehenden Möglichkeiten (insbesondere die Fristverlängerung nach Art. 12 Abs. 3 DSGVO) wahrnehmen kann. Bei unvorhergesehenen Hinderungsgründen, die eine rechtzeitige Mitteilung nicht zulassen (insbesondere Krankheit), erfolgt die Mitteilung unverzüglich nach Wegfall des Hinderungsgrundes.

In dringenden Fällen, insbesondere wenn dem Verantwortlichen die Einhaltung seiner eigenen Frist gegenüber der betroffenen Person ohne beschleunigte Bearbeitung nicht möglich wäre, bemüht sich der Auftragsverarbeiter um eine vorrangige Bearbeitung. Der Verantwortliche hat in diesem Fall den Grund der Dringlichkeit darzulegen.

(6) **Vergütung** Die Bearbeitung von Anfragen nach diesem Paragraphen erfolgt im Rahmen einer üblichen Mitwirkungsleistung ohne gesonderte Vergütung. Als übliche Mitwirkungsleistung gilt ein Bearbeitungsaufwand des Auftragsverarbeiters von bis zu 60 Minuten je Kalenderhalbjahr und Verantwortlichem.

Darüber hinausgehender Aufwand sowie Anfragen, die einen erheblichen Aufwand erfordern (insbesondere wiederholte Anfragen innerhalb kurzer Zeit, Anfragen zur Wiederherstellung aus Backups, zur Aufbereitung von Daten in nicht standardmäßigen Formaten oder zur Erstellung individueller Auswertungen), werden nach der zum Zeitpunkt der Anfrage gültigen Preisliste des Auftragsverarbeiters vergütet. Es gilt eine Mindestabrechnungseinheit von 30 Minuten je angefangener Bearbeitung.

Bei offensichtlich unbegründeten oder exzessiven Anfragen im Sinne des Art. 12 Abs. 5 DSGVO kann der Auftragsverarbeiter die Bearbeitung darüber hinaus verweigern.

Der Auftragsverarbeiter kündigt die Erhebung einer Vergütung vor Aufnahme der vergütungspflichtigen Bearbeitung in Textform an und weist auf die voraussichtliche Höhe hin. Setzt der Verantwortliche die Anfrage nach dieser Ankündigung nicht binnen fünf Werktagen in Textform aus, gilt die Vergütung als akzeptiert. Die fünftägige Aussetzungsmöglichkeit nach den vorstehenden Sätzen betrifft ausschließlich die vergütungspflichtige Bearbeitung. Die Bearbeitung im Rahmen der üblichen Mitwirkungsleistung (bis zu 60 Minuten je Kalenderhalbjahr) nimmt der Auftragsverarbeiter hiervon unabhängig und ohne Abwarten dieser Frist auf. Mit der vergütungspflichtigen Bearbeitung beginnt der Auftragsverarbeiter erst nach Ablauf der Frist oder nach vorheriger ausdrücklicher Zustimmung des Verantwortlichen; insoweit verlängern sich die Bearbeitungsfristen nach Absatz 5 hinsichtlich des vergütungspflichtigen Teils

entsprechend. Ist eine beschleunigte Bearbeitung im Sinne des Absatzes 5 erforderlich, stimmen sich die Parteien unverzüglich über die Vergütung ab; in diesem Fall kann der Auftragsverarbeiter auch die vergütungspflichtige Bearbeitung vor Ablauf der Frist aufnehmen.

(7) **Begrenzung der Pflicht** Die Unterstützungspflicht besteht nur im Rahmen der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen (Art. 28 Abs. 3 lit. e DSGVO). Eine rechtliche Bewertung der Berechtigung des Antrags oder eine inhaltliche Beratung des Verantwortlichen ist nicht geschuldet.

§ 12 Meldung von Datenschutzverletzungen

(1) **Meldepflicht** Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich nach Bekanntwerden über jede Datenschutzverletzung im Sinne des Art. 4 Nr. 12 DSGVO, die Kundendaten betrifft (Art. 33 Abs. 2 DSGVO).

(2) **Meldefrist** Die Unterrichtung erfolgt ohne unangemessene Verzögerung, in jedem Fall jedoch so rechtzeitig, dass der Verantwortliche seine eigene Meldepflicht nach Art. 33 Abs. 1 DSGVO gegenüber der zuständigen Aufsichtsbehörde einhalten kann. In der Regel erfolgt die Unterrichtung innerhalb von 72 Stunden nach Bekanntwerden der Datenschutzverletzung beim Auftragsverarbeiter.

Eine Datenschutzverletzung gilt als bekannt geworden, sobald der Auftragsverarbeiter aufgrund eigener Feststellungen oder Mitteilungen Dritter (insbesondere Subunternehmer, Sicherheitsforscher, betroffene Personen) hinreichende Gewissheit darüber hat, dass ein Sicherheitsvorfall stattgefunden hat, der zu einer Datenschutzverletzung im Sinne des Art. 4 Nr. 12 DSGVO geführt hat. Die Phase der ersten technischen Aufklärung eines unklaren Sicherheitsvorfalls zählt nicht zur Frist nach Satz 1, sofern sie angemessen ist und unverzüglich durchgeführt wird.

(3) **Inhalt der Meldung** Die Meldung enthält, soweit dies dem Auftragsverarbeiter zum Zeitpunkt der Meldung möglich ist, mindestens

a) eine Beschreibung der Art der Datenschutzverletzung, soweit möglich unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze, b) den Namen und die Kontaktdaten einer für Rückfragen zuständigen Stelle, c) eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung, d) eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Soweit einzelne Angaben zum Zeitpunkt der Erstmeldung noch nicht vorliegen, weist der Auftragsverarbeiter hierauf hin und liefert die Informationen unverzüglich nach Verfügbarkeit nach.

(4) **Form der Meldung** Die Meldung erfolgt in Textform an die im Account des Verantwortlichen hinterlegte E-Mail-Adresse des primären Accountinhabers sowie, soweit benannt, an die in § 4 Abs. 4 dieses AVV benannten weisungsberechtigten Personen.

(5) **Unterstützung bei Pflichten des Verantwortlichen** Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der diesen treffenden Pflichten nach Art. 33 und Art. 34 DSGVO. Die Unterstützung umfasst insbesondere

a) die Bereitstellung der für die Meldung an die zuständige Aufsichtsbehörde erforderlichen Informationen aus dem Verantwortungsbereich des Auftragsverarbeiters, b) die Mitwirkung an der Bewertung des Risikos für die Rechte und Freiheiten betroffener Personen, c) die Mitwirkung bei der Vorbereitung etwaiger Benachrichtigungen betroffener Personen nach Art. 34 DSGVO.

Eine eigenständige Bewertung der Meldepflicht des Verantwortlichen oder die eigenständige Vornahme von Meldungen an Aufsichtsbehörden oder betroffene Personen erfolgt durch den Auftragsverarbeiter nicht.

(6) **Dokumentation** Der Auftragsverarbeiter dokumentiert sämtliche Datenschutzverletzungen einschließlich der diesbezüglichen Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen (Art. 33 Abs. 5 DSGVO analog). Auf begründete Anfrage stellt er dem Verantwortlichen die für dessen eigene Rechenschaftspflicht erforderlichen Auszüge aus dieser Dokumentation zur Verfügung.

(7) **Vertraulichkeit der Meldung** Die Meldung sowie sämtliche im Zusammenhang mit der Datenschutzverletzung ausgetauschten Informationen unterliegen der Vertraulichkeitspflicht beider Parteien, soweit dem nicht gesetzliche Mitteilungspflichten entgegenstehen oder die Information für die Wahrnehmung von Betroffenenrechten oder die Meldung an Aufsichtsbehörden erforderlich ist.

(8) **Sicherheitsvorfälle ohne Datenschutzbezug** Sicherheitsvorfälle, die keine Datenschutzverletzung im Sinne des Art. 4 Nr. 12 DSGVO darstellen (insbesondere abgewehrte Angriffsversuche ohne Erfolg, Auffälligkeiten ohne Datenbezug), sind nicht nach diesem Paragraphen meldepflichtig. Der Auftragsverarbeiter kann den Verantwortlichen über solche Vorfälle nach eigenem Ermessen informieren.

(9) **Vergütung** Die Erfüllung der eigenen Melde- und Unterstützungspflichten des Auftragsverarbeiters nach diesem Paragraphen, insbesondere die Unterrichtung nach Absatz 1 sowie die Bereitstellung der in Absatz 3 und Absatz 5 genannten Informationen aus seinem Verantwortungsbereich, erfolgt ohne gesonderte Vergütung. Eine darüber hinausgehende Unterstützung des Verantwortlichen, die einen erheblichen, nicht in der Sphäre des Auftragsverarbeiters begründeten Aufwand erfordert, kann nach Maßgabe von § 11 Abs. 6 dieses AVV vergütet werden. Beruht die Datenschutzverletzung auf einer Pflichtverletzung des Auftragsverarbeiters, erfolgt die Unterstützung unentgeltlich.

§ 13 Datenschutz-Folgenabschätzung und vorherige Konsultation

(1) **Unterstützung bei der Datenschutz-Folgenabschätzung** Soweit der Verantwortliche im Rahmen seiner Pflichten nach Art. 35 DSGVO zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist und diese Verpflichtung Verarbeitungen betrifft, die im Rahmen dieses AVV durch den Auftragsverarbeiter durchgeführt werden, unterstützt der Auftragsverarbeiter den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

(2) **Umfang der Unterstützung** Die Unterstützung umfasst insbesondere die Bereitstellung der folgenden Informationen, soweit der Auftragsverarbeiter über diese verfügt:

a) eine systematische Beschreibung der durch den Auftragsverarbeiter durchgeführten Verarbeitungsvorgänge sowie der Verarbeitungszwecke (Art. 35 Abs. 7 lit. a DSGVO), b) Informationen zu den eingesetzten Subunternehmern und Drittlandübermittlungen (Anlage 3), c) eine Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (Anlage 2), d) gegebenenfalls vorhandene Zertifizierungen oder Prüfberichte eingesetzter Subunternehmer.

(3) **Unterstützung bei der vorherigen Konsultation** Ist der Verantwortliche aufgrund einer Datenschutz-Folgenabschätzung zur vorherigen Konsultation der zuständigen Aufsichtsbehörde nach Art. 36 DSGVO verpflichtet, unterstützt der Auftragsverarbeiter den Verantwortlichen nach Maßgabe der Absätze (1) und (2) entsprechend. Der Auftragsverarbeiter wirkt zudem an der Beantwortung etwaiger Rückfragen der Aufsichtsbehörde mit, soweit diese seinen Verantwortungsbereich betreffen.

(4) **Begrenzung der Unterstützungspflicht** Die Unterstützungspflicht besteht ausschließlich im Rahmen der in Art. 28 Abs. 3 lit. f DSGVO niedergelegten Anforderungen. Eine rechtliche Bewertung der

Erforderlichkeit oder Durchführung einer Datenschutz-Folgenabschätzung sowie die eigenständige Erstellung einer Datenschutz-Folgenabschätzung für den Verantwortlichen sind nicht geschuldet.

(5) **Reaktionsfristen und Vergütung** Die Unterstützungsleistungen nach diesem Paragraphen erbringt der Auftragsverarbeiter ohne unangemessene Verzögerung. Die Reaktionsfristen des § 11 Abs. 5 finden hierauf keine Anwendung; maßgeblich ist die jeweilige gesetzliche Frist, innerhalb derer der Verantwortliche seinen eigenen Pflichten nach Art. 35, 36 DSGVO nachzukommen hat. Für die Vergütung gilt § 11 Abs. 6 dieses AVV entsprechend. Standardanfragen und die Bereitstellung der in Absatz (2) genannten Informationen erfolgen ohne gesonderte Vergütung.

§ 14 Kontroll- und Auditrechte

(1) **Nachweispflicht** Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO und in diesem AVV niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen nach Maßgabe der nachfolgenden Absätze.

(2) **Erste Stufe – Selbstauskunft und Bescheinigungen** Auf begründete Anfrage des Verantwortlichen stellt der Auftragsverarbeiter folgende Informationen in Textform zur Verfügung:

a) eine aktuelle Fassung dieses AVV nebst Anlagen, b) die zum Zeitpunkt der Anfrage aktuelle Beschreibung der technischen und organisatorischen Maßnahmen (Anlage 2), c) die zum Zeitpunkt der Anfrage aktuelle Subunternehmerliste (Anlage 3), d) eine schriftliche Selbstauskunft zu konkreten datenschutzrechtlichen Fragen des Verantwortlichen, e) soweit vorhanden, Zertifizierungen, Prüfberichte und Auditberichte des Auftragsverarbeiters oder seiner Subunternehmer.

Die Bereitstellung der unter lit. a bis c genannten Dokumente erfolgt ohne gesonderte Vergütung; sie ist auf bis zu zwei Anfragen je Kalenderjahr und Verantwortlichem beschränkt. Für die unter lit. d und e genannten Auskünfte und Berichte gilt § 11 Abs. 6 dieses AVV entsprechend.

(3) **Zweite Stufe – Audit bei konkretem Anlass** Soweit die in Absatz (2) genannten Informationen für den Nachweis der Einhaltung der Pflichten des Auftragsverarbeiters nicht ausreichen und ein konkreter, begründeter Anlass besteht, kann der Verantwortliche eine Überprüfung (Audit) durchführen oder durch einen von ihm beauftragten Prüfer durchführen lassen.

Ein konkreter Anlass liegt insbesondere vor bei

a) berechtigten Anhaltspunkten für eine wesentliche Verletzung dieses AVV durch den Auftragsverarbeiter, b) einer Anordnung der für den Verantwortlichen zuständigen Aufsichtsbehörde, die ein solches Audit verlangt, c) einer wesentlichen Datenschutzverletzung im Sinne des § 12 dieses AVV, die nach Art und Schwere ein Audit gebietet.

(4) **Verfahren des Audits** Für die Durchführung eines Audits gelten folgende Bedingungen:

a) Ankündigung mindestens 60 Tage vor dem geplanten Termin, sofern nicht eine kürzere Frist aufgrund behördlicher Anordnung erforderlich ist, b) Durchführung während üblicher Geschäftszeiten und in einer Weise, die den Geschäftsbetrieb des Auftragsverarbeiters nicht unverhältnismäßig beeinträchtigt, c) maximal ein Audit je Kalenderjahr je Verantwortlichem, sofern nicht eine wesentliche Datenschutzverletzung oder eine behördliche Anordnung weitere Audits erfordert, d) Beschränkung auf die für die Auftragsverarbeitung relevanten Bereiche; keine Einsicht in Daten anderer Auftraggeber, in Geschäftsgeheimnisse oder in Personalakten, e) der Verantwortliche und ein etwaiger Prüfer verpflichten sich vor Durchführung des Audits schriftlich zur Vertraulichkeit hinsichtlich aller im Rahmen des Audits zur Kenntnis gelangten Informationen, f) Audits finden grundsätzlich remote über sichere Video- und Dokumentenfreigabe-Lösungen statt; der Auftragsverarbeiter stellt hierzu die erforderlichen technischen

Verbindungen sowie eine geeignete Dokumentenübergabe sicher. Ein Audit in physischen Geschäftsräumen ist nur möglich, soweit der Auftragsverarbeiter dies im Einzelfall ausdrücklich anbietet; die diesbezügliche Entscheidung liegt im billigen Ermessen des Auftragsverarbeiters und kann insbesondere von der Verfügbarkeit geeigneter Räumlichkeiten und der Schwere des Auditanlasses abhängig gemacht werden. Soweit eine zuständige Aufsichtsbehörde aufgrund konkreter Anordnung ein physisches Vor-Ort-Audit verlangt, wirkt der Auftragsverarbeiter an dessen Durchführung in angemieteten Geschäftsräumen mit; die Mehrkosten trägt der Verantwortliche entsprechend Absatz 6.

(5) **Beauftragte Prüfer** Soweit der Verantwortliche einen Prüfer mit der Durchführung des Audits beauftragt, muss dieser unabhängig und fachlich qualifiziert sein. Der Auftragsverarbeiter kann der Person des Prüfers aus wichtigem Grund widersprechen; ein wichtiger Grund liegt insbesondere vor, wenn der Prüfer ein unmittelbarer Wettbewerber des Auftragsverarbeiters ist oder begründete Zweifel an dessen Unabhängigkeit bestehen.

(6) **Kostentragung** Die Kosten eines Vor-Ort-Audits trägt der Verantwortliche, einschließlich der für die Mitwirkung des Auftragsverarbeiters aufgewendeten Personalkosten nach dessen jeweils gültiger Preisliste. Werden im Rahmen des Audits wesentliche Verstöße des Auftragsverarbeiters gegen diesen AVV festgestellt, trägt dieser die Kosten des Audits sowie die ihm selbst entstandenen Mitwirkungskosten.

(7) **Audits durch Aufsichtsbehörden** Audits und Kontrollen durch zuständige Aufsichtsbehörden bleiben von den vorstehenden Regelungen unberührt. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei behördlichen Audits, soweit dies den Verantwortungsbereich des Auftragsverarbeiters betrifft.

(8) **Subunternehmer-Audits** Soweit ein Audit Subunternehmer des Auftragsverarbeiters betrifft, erfolgt die Auditierung in der Regel durch Vorlage der vom Subunternehmer bereitgestellten Zertifizierungen und Prüfberichte (Absatz 2 lit. e). Soweit dies nicht ausreicht, vermittelt der Auftragsverarbeiter dem Verantwortlichen einen Auskunftsanspruch gegenüber dem Subunternehmer; eine eigene Audit-Berechtigung des Verantwortlichen gegenüber Subunternehmern wird durch diesen AVV nicht begründet.

§ 15 Drittstaatentransfer

(1) **Grundsatz** Die Verarbeitung der Kundendaten erfolgt vorrangig innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums (EWR). Soweit im Rahmen der Erbringung der vertragsgegenständlichen Leistungen personenbezogene Daten in Länder außerhalb des EWR (Drittländer) übermittelt werden oder aus Drittländern auf sie zugegriffen wird, erfolgt dies ausschließlich nach Maßgabe der nachfolgenden Absätze und auf Grundlage geeigneter Garantien gemäß Art. 44 ff. DSGVO. Die im Einzelnen bestehenden Drittlandbezüge ergeben sich aus Anlage 3.

(2) **Übermittlungen durch Subunternehmer** Bei den in Anlage 3 aufgeführten Subunternehmern können Übermittlungen in Drittländer stattfinden, insbesondere durch

a) den Sitz des Subunternehmers in einem Drittland, b) den Einsatz von Subprozessoren des Subunternehmers in einem Drittland oder c) administrative Zugriffe aus einem Drittland.

Die jeweiligen Drittlandbezüge sowie die anwendbaren Übermittlungsgarantien ergeben sich aus Anlage 3.

(3) **Anwendbare Übermittlungsgarantien** Soweit Übermittlungen in Drittländer stattfinden, erfolgen diese auf Grundlage geeigneter Garantien gemäß Art. 44 ff. DSGVO. Als Übermittlungsgarantien kommen insbesondere in Betracht:

a) Angemessenheitsbeschlüsse der Europäischen Kommission gemäß Art. 45 DSGVO, b) Standardvertragsklauseln der Europäischen Kommission gemäß Art. 46 Abs. 2 lit. c DSGVO in der jeweils gültigen Fassung (insbesondere Durchführungsbeschluss (EU) 2021/914), c) Zertifizierungen unter dem EU-US Data Privacy Framework gemäß Art. 45 DSGVO i.V.m. dem Durchführungsbeschluss (EU) 2023/1795, soweit der Subunternehmer dort zertifiziert ist.

(4) **Pflichten des Auftragsverarbeiters bei Drittstaatentransfers** Der Auftragsverarbeiter stellt sicher, dass mit allen Subunternehmern, die Kundendaten in Drittländer übermitteln oder aus Drittländern auf diese zugreifen, ein dem jeweils geltenden Recht entsprechender Übermittlungsmechanismus vereinbart ist. Insbesondere stellt der Auftragsverarbeiter sicher, dass die mit den Subunternehmern abgeschlossenen Verträge die jeweils aktuellen Standardvertragsklauseln enthalten, soweit diese einschlägig sind.

(5) **Bereitstellung der Übermittlungsgarantien** Der Auftragsverarbeiter stellt dem Verantwortlichen auf begründete Anfrage in Textform Auskunft über die mit den Subunternehmern vereinbarten Übermittlungsgarantien zur Verfügung. Soweit die Subunternehmer ihre Übermittlungsgarantien öffentlich zugänglich machen (insbesondere durch Veröffentlichung im Rahmen ihrer Datenverarbeitungsverträge), genügt die Verweisung auf die entsprechenden Veröffentlichungen.

(6) **Transfer Impact Assessment** Der Auftragsverarbeiter berücksichtigt bei der Auswahl von Subunternehmern mit Drittlandbezug die rechtlichen und tatsächlichen Umstände im jeweiligen Drittland im Einklang mit den Anforderungen der DSGVO und der einschlägigen Rechtsprechung (Transfer Impact Assessment). Er kann sich dabei auf die vom jeweiligen Subunternehmer bereitgestellten Transfer-Risiko-Bewertungen und Compliance-Unterlagen stützen. Bei Subunternehmern, die unter einem geltenden Angemessenheitsbeschluss der Europäischen Kommission tätig sind, beschränkt sich die Bewertung auf die Verifikation des aktuellen Status. Die durchgeführten Bewertungen werden dem Verantwortlichen auf begründete Anfrage in zusammengefasster Form zur Verfügung gestellt.

(7) **Information bei wesentlichen Änderungen** Wesentliche Änderungen der Drittlandbezüge oder der anwendbaren Übermittlungsgarantien (insbesondere Wegfall eines Angemessenheitsbeschlusses, Inkrafttreten neuer Standardvertragsklauseln) teilt der Auftragsverarbeiter dem Verantwortlichen nach Maßgabe von § 8 dieses AVV mit.

(8) **Direkter Drittlandtransfer durch den Auftragsverarbeiter** Führt eine Änderung der eingesetzten Dienste oder Subunternehmer zu einer wesentlichen Erweiterung der Drittlandbezüge, gelten die Anforderungen der Absätze (3) bis (6) entsprechend. Eine solche Änderung wird dem Verantwortlichen nach Maßgabe von § 8 dieses AVV mitgeteilt. Das Widerspruchs- und Kündigungsrecht nach § 8 dieses AVV bleibt unberührt; es besteht nur, soweit für die erweiterten Drittlandbezüge keine geeigneten Garantien gemäß Art. 44 ff. DSGVO bestehen.

(9) **Sitz des Verantwortlichen in einem Drittland** Hat der Verantwortliche seinen Sitz oder maßgeblichen Niederlassungsort außerhalb des Europäischen Wirtschaftsraums (Drittland) und besteht für dieses Drittland kein Angemessenheitsbeschluss der Europäischen Kommission, so erfolgt eine Übermittlung von Kundendaten durch den Auftragsverarbeiter an den Verantwortlichen – insbesondere die Bereitstellung und Rückübermittlung im Rahmen der App – auf Grundlage der Standardvertragsklauseln der Europäischen Kommission gemäß Durchführungsbeschluss (EU) 2021/914, Modul 4 (Übermittlung von einem Auftragsverarbeiter an einen Verantwortlichen). Die Standardvertragsklauseln werden in diesem Fall mit Abschluss dieses AVV einbezogen und gehen ihm im Kollisionsfall vor. Die Absätze (3) bis (6) gelten entsprechend. Der Auftragsverarbeiter ist berechtigt, die Bereitstellung der Leistungen auf Verantwortliche mit Sitz im Europäischen Wirtschaftsraum zu beschränken.

§ 16 Löschung und Rückgabe nach Beendigung

(1) **Wahlrecht des Verantwortlichen** Nach Beendigung der vertragsgegenständlichen Leistungen löscht oder gibt der Auftragsverarbeiter sämtliche im Auftrag verarbeiteten Kundendaten nach Wahl des Verantwortlichen zurück (Art. 28 Abs. 3 lit. g DSGVO). Der Verantwortliche teilt seine Wahl spätestens mit Beendigung des Hauptvertrages mit. Trifft der Verantwortliche keine ausdrückliche Wahl, gilt das Verfahren nach Absatz (2) als Standard-Rückgabeweg.

(2) **Datenexport als Standard-Rückgabeweg** Der Auftragsverarbeiter stellt dem Verantwortlichen ab Beendigung der vertragsgegenständlichen Leistungen für einen Zeitraum von 30 Tagen eine Funktion zum vollständigen Export der Kundendaten in strukturierten, gängigen und maschinenlesbaren Formaten (insbesondere CSV) sowie der gespeicherten Dokumente in einem gängigen Format (insbesondere PDF) über die App zur Verfügung. Der Datenexport kann ausschließlich durch Nutzer mit der Rolle „Administrator“ oder „Inhaber“ angestoßen werden. Die Durchführung des Datenexports innerhalb der vorgenannten Frist liegt in der Verantwortung des Verantwortlichen.

(3) **Löschung aus aktiven Systemen** Nach Ablauf der in Absatz (2) genannten 30-Tage-Frist entfernt der Auftragsverarbeiter die Kundendaten aus den aktiven Systemen im Rahmen der regulären Löschroutinen.

(4) **Löschung aus Backup-Systemen** Die vollständige Entfernung der Kundendaten aus Backup-Systemen erfolgt im Rahmen der regulären Backup-Rotation, spätestens jedoch 180 Tage nach Beendigung der vertragsgegenständlichen Leistungen. Während der Backup-Rotationsphase werden die Kundendaten technisch von einer aktiven Nutzung getrennt; ein Zugriff erfolgt ausschließlich

a) im Rahmen einer Wiederherstellung im Notfall (insbesondere bei Datenverlust in den aktiven Systemen vor Ablauf der Frist nach Absatz 3), oder b) soweit gesetzliche Aufbewahrungspflichten nach Absatz 6 dies erfordern.

Bei wesentlichen Änderungen der Backup-Architektur des Auftragsverarbeiters, die eine längere Rotationsphase erforderlich machen, informiert der Auftragsverarbeiter den Verantwortlichen entsprechend § 10 Abs. 4 dieses AVV.

(5) **Rückgabe statt Löschung** Wählt der Verantwortliche die Rückgabe der Kundendaten anstelle der Löschung, gilt der Datenexport nach Absatz (2) als Rückgabeweg. Eine über den Datenexport nach Absatz (2) hinausgehende Rückgabeverpflichtung des Auftragsverarbeiters besteht nicht, soweit nicht gesetzliche Vorgaben etwas anderes erfordern.

(6) **Gesetzliche Aufbewahrungspflichten** Soweit der Auftragsverarbeiter aufgrund gesetzlicher Aufbewahrungspflichten (insbesondere § 257 HGB, § 147 AO) zur weiteren Speicherung verpflichtet ist, bleiben diese Verpflichtungen unberührt. Die betroffenen Daten werden zweckgebunden für die Erfüllung der Aufbewahrungspflicht aufbewahrt und nach Ablauf der jeweiligen gesetzlichen Frist gelöscht. Aufbewahrungspflichten, die ausschließlich den Verantwortlichen treffen, lösen keine eigene Aufbewahrungspflicht des Auftragsverarbeiters aus.

(7) **Nachweis der Löschung** Auf begründete Anfrage des Verantwortlichen bestätigt der Auftragsverarbeiter die erfolgte Löschung in Textform. Die Bestätigung enthält Angaben zum Zeitpunkt und zum Umfang der Löschung sowie zu etwaigen aufgrund gesetzlicher Aufbewahrungspflichten weiter gespeicherten Daten.

(8) **Inaktive Accounts und Testaccounts** Die in den AGB geregelten Löschrufen für inaktive Accounts und Testaccounts bleiben unberührt. Für deren Datenlöschung gelten die vorstehenden Absätze entsprechend.

§ 17 Haftung

(1) **Verweis auf Hauptvertrag** Für die Haftung der Parteien aus oder im Zusammenhang mit diesem AVV gelten die Regelungen des Hauptvertrages, insbesondere § 9 AGB, soweit in den nachfolgenden Absätzen nichts Abweichendes geregelt ist.

(2) **Außenhaftung nach Art. 82 DSGVO** Die Haftung der Parteien gegenüber betroffenen Personen für Schäden, die durch eine Verletzung der DSGVO entstehen (Art. 82 DSGVO), bleibt durch die Regelungen dieses AVV und des Hauptvertrages unberührt. Die Parteien haften gegenüber betroffenen Personen nach Maßgabe von Art. 82 Abs. 1, 2 DSGVO.

(3) **Innenausgleich** Im Innenverhältnis der Parteien gilt für die Verteilung der Haftung aus Art. 82 DSGVO sowie für etwaige Bußgelder nach Art. 83 DSGVO:

a) Jede Partei trägt im Innenverhältnis denjenigen Anteil an der gegenüber betroffenen Personen oder Aufsichtsbehörden geleisteten Zahlung, der ihrem Anteil an der Verantwortung für den entstandenen Schaden bzw. den geahndeten Verstoß entspricht.

b) Hat eine Partei den gesamten Schaden gegenüber der betroffenen Person ersetzt oder ein Bußgeld vollständig getragen, kann sie von der anderen Partei den auf diese entfallenden Anteil gemäß Art. 82 Abs. 5 DSGVO zurückfordern.

c) Die Beweislast für den Anteil der anderen Partei an der Verantwortung trägt die regressierende Partei.

(4) **Haftungsausschluss bei Weisungsverstößen** Hat eine Partei die andere Partei nachweislich auf einen Verstoß gegen datenschutzrechtliche Vorschriften hingewiesen (§ 4 Abs. 5 dieses AVV) und ist die hingewiesene Partei dem Hinweis nicht gefolgt, trägt diese im Innenverhältnis den Schaden in voller Höhe.

(5) **Haftung des Auftragsverarbeiters für vertragswidrige Dateneingaben** Soweit der Verantwortliche entgegen § 6 Abs. 4 und 5 dieses AVV sowie § 3 Abs. 8 AGB Daten in die App eingibt, für deren Verarbeitung er keine Rechtsgrundlage hat oder die nicht den vertraglichen Vorgaben entsprechen, ist eine Haftung des Auftragsverarbeiters für hieraus resultierende Schäden ausgeschlossen. § 3 Abs. 9 AGB gilt entsprechend.

(6) **Freistellung** Werden Ansprüche Dritter (insbesondere betroffener Personen, Aufsichtsbehörden oder anderer Auftragnehmer des Verantwortlichen) gegen den Auftragsverarbeiter geltend gemacht, die auf einer Verletzung der Pflichten des Verantwortlichen nach diesem AVV oder dem Hauptvertrag durch den Verantwortlichen beruhen, stellt der Verantwortliche den Auftragsverarbeiter im Innenverhältnis von diesen Ansprüchen einschließlich erforderlicher Rechtsverteidigungskosten frei, soweit nicht eine eigene Haftung des Auftragsverarbeiters nach Absatz (3) besteht.

(7) **Beschränkung der Innenhaftung** Die Haftungsbeschränkungen des Hauptvertrages, insbesondere die in § 9 Abs. 2 AGB enthaltenen Begrenzungen der Höhe nach (50 % der vom Verantwortlichen im betreffenden Kalenderjahr gezahlten Vergütung als Haftungslimit je Schadensfall), gelten auch im Verhältnis der Parteien zueinander für Ansprüche aus oder im Zusammenhang mit diesem AVV. Die Haftung für Vorsatz und grobe Fahrlässigkeit, für die Verletzung von Leben, Körper und Gesundheit sowie nach den Vorschriften des Produkthaftungsgesetzes bleibt unbeschränkt (§ 9 Abs. 1 AGB).

(8) **Anwendung auf vorvertraglichen und nachvertraglichen Zeitraum** Die Regelungen dieses Paragraphen gelten auch für Schäden, die vor Abschluss dieses AVV im Rahmen vorvertraglicher Maßnahmen sowie nach Beendigung der vertragsgegenständlichen Leistungen im Rahmen der nachvertraglichen Pflichten (insbesondere § 16 dieses AVV) entstehen.

§ 18 Schlussbestimmungen

(1) **Laufzeit** Dieser AVV tritt mit Abschluss des Hauptvertrages in Kraft und läuft für die Dauer des Hauptvertrages. Er endet automatisch mit Beendigung des Hauptvertrages, ohne dass es einer gesonderten Kündigung dieses AVV bedarf. Nachvertragliche Pflichten der Parteien (insbesondere § 16 dieses AVV sowie etwaige Aufbewahrungs- und Vertraulichkeitspflichten) bleiben über die Beendigung hinaus wirksam.

(2) **Außerordentliche Kündigung des AVV** Soweit dieser AVV nicht gemäß Absatz (1) endet, kann er nur aus wichtigem datenschutzrechtlichem Grund außerordentlich gekündigt werden. Insbesondere bei einer wesentlichen Verletzung dieses AVV durch eine Partei, die trotz schriftlicher Aufforderung mit Fristsetzung nicht abgestellt wurde, kann die andere Partei den Hauptvertrag gemäß den dortigen Kündigungsregelungen kündigen. Eine isolierte Kündigung des AVV unter Fortbestand des Hauptvertrages ist nicht zulässig.

(3) **Form des Vertragsschlusses und von Änderungen** Dieser AVV wird in Textform (§ 126b BGB) geschlossen. Die elektronische Bestätigung im Rahmen des Onboardings im Kundenaccount – verbunden mit der Protokollierung gemäß § 5.4 der Datenschutzerklärung des Auftragsverarbeiters (IP-Adresse, Browser-Kennung, Zeitstempel, Dokumentversion) – erfüllt die Textform.

Eine durch den Auftragsverarbeiter rechtsverbindlich unterzeichnete Fassung dieses AVV wird dem Verantwortlichen zum Download bereitgestellt. Eine gegenzeichnende Unterschrift des Verantwortlichen ist für die Wirksamkeit dieses AVV nicht erforderlich, kann aber auf Wunsch des Verantwortlichen nachgereicht werden.

Änderungen und Ergänzungen dieses AVV bedürfen der Textform; dies gilt auch für die Änderung dieser Textformklausel.

(4) **Anpassung dieses AVV** Der Auftragsverarbeiter ist berechtigt, diesen AVV einschließlich seiner Anlagen anzupassen, soweit

- a) dies aufgrund von Änderungen der anwendbaren datenschutzrechtlichen Vorschriften, verbindlicher Vorgaben von Aufsichtsbehörden oder relevanter Rechtsprechung erforderlich oder geboten ist,
- b) dies zur Berücksichtigung technischer, organisatorischer oder funktionaler Weiterentwicklungen der App, einschließlich der Hinzuziehung, des Wechsels oder der Anpassung von Subunternehmern, erforderlich ist,
- c) dies zur Schließung von Regelungslücken, zur Verbesserung der Klarheit, zur Korrektur redaktioneller Fehler oder zur Anpassung an Marktstandards für vergleichbare Auftragsverarbeitungsverträge dient, oder
- d) dies zur Berücksichtigung wesentlicher Änderungen der wirtschaftlichen, organisatorischen oder technischen Rahmenbedingungen des Auftragsverarbeiters erforderlich oder zweckmäßig ist, soweit dadurch das in Anlage 2 beschriebene Schutzniveau für die Kundendaten nicht wesentlich unterschritten wird.

Geringfügige redaktionelle Anpassungen, Aktualisierungen der Anlagen 1 und 2 sowie Anpassungen, die ausschließlich der Klarstellung dienen, werden durch Veröffentlichung der aktualisierten Fassung dieses AVV unter der vom Auftragsverarbeiter hierfür im Internet bereitgestellten Adresse mit einer Vorlaufzeit von 30 Tagen wirksam; einer gesonderten Mitteilung an den Verantwortlichen bedarf es nicht. Anpassungen der Anlage 3 (Subunternehmer) richten sich ausschließlich nach § 8 dieses AVV.

Sonstige Änderungen werden dem Verantwortlichen in Textform an die im Account hinterlegte E-Mail-Adresse mit einer Vorlaufzeit von mindestens 30 Tagen vor Inkrafttreten mitgeteilt. Sie gelten als angenommen, wenn der Verantwortliche der Änderung nicht bis zum Inkrafttreten der Änderung in

Textform widerspricht. Auf diese Frist sowie auf die Folgen eines Schweigens wird in der Mitteilung gesondert hingewiesen. Die fortgesetzte Nutzung der App nach Inkrafttreten der Änderung gilt im Übrigen als Annahme.

Eine außerordentliche Kündigung des Hauptvertrages aufgrund einer Änderung dieses AVV ist nur zulässig, soweit die Änderung zu einer wesentlichen und nicht nur unerheblichen Verschlechterung der datenschutzrechtlichen Position des Verantwortlichen führt. Als wesentliche Verschlechterung gilt ausschließlich:

- i) die wesentliche Reduzierung des in Anlage 2 beschriebenen Schutzniveaus,
- ii) die Aufnahme von Verarbeitungen zu Eigenzwecken des Auftragsverarbeiters, die über die in § 2 Abs. 3 dieses AVV vorgesehenen Verarbeitungen hinausgehen, oder
- iii) die Aufnahme regelmäßiger Drittlandstransfers ohne geeignete Garantien gemäß Art. 44 ff. DSGVO, soweit der Auftragsverarbeiter selbst diese Transfers durchführt.

Nicht als wesentliche Verschlechterung gelten insbesondere: redaktionelle Klarstellungen, Aktualisierungen der Subunternehmerliste, Anpassungen der technischen und organisatorischen Maßnahmen zur Berücksichtigung des Stands der Technik, Anpassungen aufgrund geänderter Rechtslage sowie Anpassungen, die das Schutzniveau erhöhen oder neutral wirken.

(5) **Mitteilungen** Mitteilungen, Erklärungen und Anfragen nach diesem AVV erfolgen

a) an den Auftragsverarbeiter: datenschutz@blinkpilot.com b) an den Verantwortlichen: an die im Account des Verantwortlichen hinterlegte E-Mail-Adresse des primären Accountinhabers sowie, soweit benannt, an die in § 4 Abs. 4 dieses AVV bezeichneten weisungsberechtigten Personen.

Mitteilungen des Auftragsverarbeiters an den Verantwortlichen können zusätzlich über etwaige im Account des Verantwortlichen integrierte Kommunikationsfunktionen (insbesondere In-App-Inbox, Push- oder In-App-Benachrichtigungen) erfolgen, soweit der Auftragsverarbeiter solche Funktionen bereitstellt. Ein Anspruch des Verantwortlichen auf Bereitstellung oder Nutzung solcher Funktionen besteht nicht.

Die Parteien teilen sich Änderungen der Kontaktdaten unverzüglich mit.

(6) **Anwendbares Recht** Auf diesen AVV findet das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG) Anwendung. Zwingende Vorschriften des Unionsrechts, insbesondere der DSGVO, bleiben unberührt.

(7) **Gerichtsstand** Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist Frankfurt am Main, soweit der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder keinen allgemeinen Gerichtsstand in Deutschland hat.

(8) **Kirchliche Auftraggeber** Soweit der Verantwortliche dem Anwendungsbereich des Gesetzes über den Kirchlichen Datenschutz der Katholischen Kirche (KDG) oder des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) unterliegt, finden ergänzend die Vorschriften dieser kirchlichen Datenschutzregelungen Anwendung. In diesem Fall schließen die Parteien auf Anforderung des Verantwortlichen einen gesonderten Auftragsverarbeitungsvertrag, der die spezifischen Anforderungen des einschlägigen kirchlichen Datenschutzrechts berücksichtigt. Bis zum Abschluss eines solchen gesonderten Auftragsverarbeitungsvertrages gelten die Regelungen dieses AVV auch im Verhältnis zu kirchlichen Auftraggebern entsprechend, soweit das einschlägige kirchliche Datenschutzrecht (KDG bzw. DSG-EKD) dem nicht zwingend entgegensteht.

(9) **Vorrang dieses AVV** Im Verhältnis zu den AGB gehen die Regelungen dieses AVV in datenschutzrechtlichen Angelegenheiten vor. Im Übrigen gilt die in der Präambel niedergelegte Konfliktauflösungsregel.

(10) **Salvatorische Klausel** Sollte eine Bestimmung dieses AVV unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt. Die Parteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Bestimmung möglichst nahekommt. Entsprechendes gilt für etwaige Regelungslücken.

(11) **Anlagen** Bestandteil dieses AVV sind die folgenden Anlagen:

- Anlage 1: Verarbeitungstätigkeiten und Datenkategorien
- Anlage 2: Technische und organisatorische Maßnahmen (TOM)
- Anlage 3: Subunternehmer

Die Anlagen werden dem Verantwortlichen vom Auftragsverarbeiter in der jeweils aktuellen Fassung unter der vom Auftragsverarbeiter im Internet veröffentlichten Adresse bereitgestellt.

Soweit dieser AVV oder seine Anlagen auf Abschnitte der Datenschutzerklärung des Auftragsverarbeiters verweisen, dienen diese Verweise allein der näheren Erläuterung. Bei Abweichungen zwischen der Datenschutzerklärung und diesem AVV oder seinen Anlagen gehen dieser AVV und seine Anlagen vor.

– Ende des Vertragstextes; Anlagen 1, 2 und 3 sind in separaten Dokumenten geführt –

Unterzeichnung

Dieser Auftragsverarbeitungsvertrag einschließlich seiner Anlagen 1 bis 3 wird von beiden Parteien rechtsverbindlich geschlossen. Die Anlagen 1 (Verarbeitungstätigkeiten und Datenkategorien), 2 (Technische und organisatorische Maßnahmen) und 3 (Subunternehmer) sind Bestandteil dieses Vertrages.

Der Verantwortliche

(in den AGB als „Kunde“ bezeichnet)

Ort, Datum

Name (in Druckbuchstaben)

Funktion / Vertretungsbefugnis

Unterschrift

Der Auftragsverarbeiter

blinkpilot UG (haftungsbeschränkt)

Frankfurt am Main, 29. Juni 2026

Ort, Datum

Stefan Dold

Name (in Druckbuchstaben)

Geschäftsführer

Funktion / Vertretungsbefugnis



Unterschrift