Auftragsverarbeitungsvereinbarung

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO — Anlage zu den Allgemeinen Geschäftsbedingungen von Kundoo.

Zwischen dem Kunden von Kundoo — nachfolgend „Verantwortlicher" — und
Karl Emanuel-Mischke, Enderstraße 94, 01277 Dresden — nachfolgend „Auftragsverarbeiter"
wird die folgende Vereinbarung nach Art. 28 DSGVO geschlossen.

Präambel

Zwischen den Parteien besteht ein Vertrag über die Nutzung der Anwendung Kundoo (nachfolgend „Hauptvertrag"). Kundoo unterstützt den Verantwortlichen bei der Verwaltung seiner Geschäftsbeziehungen. Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten, für die der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO allein verantwortlich bleibt.

Eine Übertragung von Aufgaben zur eigenverantwortlichen Erfüllung ist nicht beabsichtigt.

I. Gegenstand und Dauer

1. Gegenstand. Gegenstand des Auftrags ist die Bereitstellung und der Betrieb der Anwendung Kundoo als Software-as-a-Service. Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten ausschließlich weisungsgebunden für den Verantwortlichen. Im Einzelnen umfasst dies:

– die Speicherung und Verwaltung von Kunden- und Kontaktdaten,
– die Verwaltung von Terminen, Wiedervorlagen und Aufgaben,
– die Erfassung von Kundenbesuchen und zugehörigen Notizen,
– die Erfassung und Auswertung von Umsätzen,
– die Speicherung vom Verantwortlichen hochgeladener Dokumente,
– die Darstellung von Kundenadressen auf einer Karte,
– den Export der Daten in gängigen Formaten.

Der Auftragsverarbeiter prüft die Inhalte hochgeladener Dokumente nicht. Die Verantwortung für deren Rechtmäßigkeit trägt allein der Verantwortliche.

2. Dauer. Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Verpflichtungen, die ihrer Natur nach über das Vertragsende hinauswirken — insbesondere Abschnitt X — bleiben davon unberührt.

II. Art und Zweck der Verarbeitung, Datenkategorien, betroffene Personen

1. Zweck. Die Verarbeitung dient ausschließlich der Erbringung der im Hauptvertrag vereinbarten Leistungen. Eine Nutzung der Daten des Verantwortlichen zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt. Insbesondere werden die Daten nicht zu Werbezwecken, nicht zur Profilbildung und nicht zum Training von Modellen künstlicher Intelligenz verwendet.

2. Datenkategorien. Der Verantwortliche kann durch Eingabe, Import oder Upload insbesondere folgende Kategorien personenbezogener Daten verarbeiten:

– Stammdaten: Anrede, akademischer Titel, Vor- und Nachname, Firmenname
– Anschrift: Straße, Postleitzahl, Ort, Bundesland
– Ortsangaben: geografische Koordinaten zur Kartendarstellung
– Kommunikationsdaten: Telefonnummer, Mobilnummer, E-Mail-Adresse, Internetadresse
– Zuordnungen: Kundengruppe, Kundenklasse, Ansprechpartner
– Vorgangsdaten: Termine, Wiedervorlagen, Aufgaben, Besuchsberichte samt Datum, Uhrzeit und Ergebnis
– Freitexte: Notizen zu Kunden, Besuchen, Terminen und Wiedervorlagen
– Geschäftsdaten: Umsätze, Positionen, Artikel, Buchungsdatum
– Dokumente: vom Verantwortlichen hochgeladene Dateien mit Kundenbezug
– Einwilligungen: vom Verantwortlichen dokumentierte Einwilligungen seiner Kunden

Daten besonderer Kategorien nach Art. 9 DSGVO sind nicht Gegenstand des Auftrags. Der Verantwortliche wird solche Daten nicht in die Anwendung einstellen.

3. Nutzerdaten. Für die Nutzer des Verantwortlichen verarbeitet der Auftragsverarbeiter zusätzlich: Name, E-Mail-Adresse, Firmen- und Anschriftsangaben, Branche, Telefonnummer, Anmeldedaten sowie Zeitstempel und gehashte IP-Adresse sicherheitsrelevanter Vorgänge.

4. Betroffene Personen.

– Geschäftskunden des Verantwortlichen sowie deren Ansprechpartner
– Lieferanten und sonstige Geschäftspartner des Verantwortlichen, soweit erfasst
– Nutzer, die der Verantwortliche für die Anwendung freischaltet

III. Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Diese sind in Anlage 2 beschrieben.

2. Die Maßnahmen unterliegen dem technischen Fortschritt. Dem Auftragsverarbeiter ist es gestattet, sie durch gleichwertige oder bessere zu ersetzen. Das vereinbarte Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert und dem Verantwortlichen auf Anfrage mitgeteilt.

3. Der Verantwortliche trägt die Verantwortung dafür, zu beurteilen, ob diese Maßnahmen für das Risiko der von ihm eingestellten Daten ein angemessenes Schutzniveau bieten.

IV. Berichtigung, Einschränkung und Löschung

1. Der Auftragsverarbeiter berichtigt, löscht oder schränkt die Verarbeitung der Daten nicht eigenmächtig ein, sondern nur auf dokumentierte Weisung des Verantwortlichen.

2. Der Verantwortliche kann Daten jederzeit selbst berichtigen und löschen. Die Anwendung stellt hierfür Funktionen bereit.

3. Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Ersuchen unverzüglich an den Verantwortlichen weiter und verweist die betroffene Person an diesen, soweit eine Zuordnung möglich ist.

V. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich:

1. Daten ausschließlich im Rahmen des Auftrags und der Weisungen des Verantwortlichen zu verarbeiten, es sei denn, er ist gesetzlich zu einer Verarbeitung verpflichtet. In diesem Fall teilt er dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

2. den Verantwortlichen unverzüglich zu informieren, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Er ist berechtigt, die Ausführung auszusetzen, bis der Verantwortliche die Weisung bestätigt oder ändert.

3. sicherzustellen, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Pflicht besteht nach Beendigung der Tätigkeit fort.

4. die Maßnahmen nach Art. 32 DSGVO umzusetzen und ihre Wirksamkeit regelmäßig zu überprüfen.

5. den Verantwortlichen im Rahmen seiner Möglichkeiten bei der Erfüllung von Anfragen betroffener Personen nach Kapitel III DSGVO zu unterstützen.

6. den Verantwortlichen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO zu unterstützen, insbesondere bei Meldepflichten und Datenschutz-Folgenabschätzungen.

7. dem Verantwortlichen eine Ansprechstelle für Datenschutzfragen zu benennen: support@kundoo.de

8. den Verantwortlichen unverzüglich zu informieren, wenn seine Daten durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder sonstige Maßnahmen Dritter gefährdet werden, und die Beteiligten darauf hinzuweisen, dass die Verfügung über die Daten allein dem Verantwortlichen zusteht.

VI. Unterauftragsverhältnisse

1. Der Verantwortliche erteilt seine allgemeine Genehmigung zur Hinzuziehung der in Anlage 1

aufgeführten weiteren Auftragsverarbeiter.

2. Nebenleistungen, die der Auftragsverarbeiter in Anspruch nimmt — etwa Telekommunikations- oder Wartungsleistungen ohne bestimmungsgemäßen Zugriff auf die Daten — gelten nicht als Unterauftragsverhältnis. Der Auftragsverarbeiter stellt auch hier ein angemessenes Schutzniveau sicher.

3. Beabsichtigt der Auftragsverarbeiter, einen weiteren Auftragsverarbeiter hinzuzuziehen oder zu ersetzen, teilt er dies dem Verantwortlichen mindestens vier Wochen vorher in Textform mit. Der Verantwortliche kann innerhalb von zwei Wochen ab Zugang aus wichtigem datenschutzrechtlichem Grund widersprechen. Widerspricht er nicht, gilt die Änderung als genehmigt.

4. Im Fall eines berechtigten Widerspruchs, für den keine einvernehmliche Lösung gefunden wird, steht beiden Parteien ein Sonderkündigungsrecht des Hauptvertrags zu.

5. Der Auftragsverarbeiter verpflichtet weitere Auftragsverarbeiter vertraglich auf ein Schutzniveau, das dieser Vereinbarung entspricht.

6. Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet nicht statt. Sollte sie künftig erforderlich werden, erfolgt sie nur unter den Voraussetzungen der Art. 44 ff. DSGVO und nach vorheriger Mitteilung nach Absatz 3.

VII. Kontrollrechte des Verantwortlichen

1. Der Verantwortliche hat das Recht, sich von der Einhaltung dieser Vereinbarung zu überzeugen. Der Nachweis erfolgt vorrangig durch Auskünfte, durch Vorlage der Dokumentation nach Anlage 2 oder durch Testate, Berichte oder Zertifizierungen unabhängiger Stellen.

2. Reichen diese Nachweise im Einzelfall nicht aus, kann der Verantwortliche eine Überprüfung vor Ort verlangen. Diese erfolgt nach Ankündigung mit angemessener Vorlaufzeit, zu üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs. Der Auftragsverarbeiter kann sie von der Unterzeichnung einer Verschwiegenheitserklärung abhängig machen und einem Prüfer widersprechen, der zu ihm im Wettbewerb steht.

3. Der Umfang solcher Überprüfungen ist auf einen Tag je Kalenderjahr begrenzt, soweit kein besonderer Anlass besteht.

4. Für Überprüfungen einer zuständigen Aufsichtsbehörde gilt Absatz 2 entsprechend; eine Verschwiegenheitserklärung ist dabei nicht erforderlich.

VIII. Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten unverzüglich, in der Regel innerhalb von 24 Stunden nach Kenntniserlangung.

2. Die Meldung enthält, soweit verfügbar: die Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl betroffener Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Gegenmaßnahmen.

3. Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen und stimmt sich hierzu mit dem Verantwortlichen ab.

4. Meldungen an die Aufsichtsbehörde und an betroffene Personen obliegen dem Verantwortlichen.

IX. Weisungsbefugnis

1. Die Weisungen ergeben sich zunächst aus dieser Vereinbarung und dem Hauptvertrag. Der Verantwortliche kann sie in Textform ändern, ergänzen oder ersetzen.

2. Mündliche Weisungen bestätigt der Verantwortliche unverzüglich in Textform.

3. Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, gelten als Antrag auf Leistungsänderung. Der Auftragsverarbeiter kann hierfür eine Vergütung verlangen.

X. Löschung und Rückgabe nach Vertragsende

1. Der Verantwortliche kann seine Daten jederzeit über die Exportfunktion der Anwendung in einem

gängigen Format herunterladen.

2. Nach Beendigung des Hauptvertrags werden die Daten für eine Kulanzfrist von 30 Tagen vorgehalten, damit der Verantwortliche den Export nachholen kann. Danach werden sie gelöscht.

3. Der Verantwortliche kann die sofortige Löschung jederzeit verlangen; die Anwendung stellt hierfür eine Funktion bereit.

4. Von der Löschung ausgenommen sind Daten, für die eine gesetzliche Aufbewahrungspflicht besteht, sowie Sicherungskopien, bis diese im regulären Zyklus überschrieben werden. Solche Daten werden in der Verarbeitung eingeschränkt.

5. Ein Löschprotokoll wird auf Anforderung in Textform vorgelegt.

XI. Schlussbestimmungen

1. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen die Regelungen dieser Vereinbarung vor, soweit sie den Datenschutz betreffen.

2. Änderungen bedürfen der Textform. Das gilt auch für den Verzicht auf dieses Formerfordernis.

3. Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

4. Es gilt das Recht der Bundesrepublik Deutschland.

5. Die Haftung richtet sich nach Art. 82 DSGVO und den Regelungen des Hauptvertrags.

Anlage 1 — Weitere Auftragsverarbeiter

Der Verantwortliche genehmigt die Hinzuziehung der folgenden weiteren Auftragsverarbeiter:

– Mittwald CM Service GmbH & Co. KG, Königsberger Straße 4–6, 32339 Espelkamp — Betrieb der Server, der Datenbank und der Dateiablage sowie Versand der Transaktions-E-Mails. Ort der Verarbeitung: Espelkamp, Deutschland.
– KEPTAGO LTD („Geoapify"), N. Nikolaidi & T. Kolokotroni, 8011 Paphos, Zypern — Ortsbestimmung von Anschriften und Ortsangaben. Übermittelt werden ausschließlich Straße, Postleitzahl und Ort — entweder aus einem Kundendatensatz, einmalig je Anschrift, oder aus der Ortsangabe eines Termins, oder als Suchbegriff, den der Verantwortliche zur Umkreissuche eingibt. Ort der Verarbeitung: Europäische Union (Endpunkt api-eu.geoapify.com).

Der erstgenannte weitere Auftragsverarbeiter betreibt ein eigenes Rechenzentrum in Espelkamp und ist nach ISO/IEC 27001 zertifiziert (Zertifizierungsstelle: TÜV Rheinland). Der Nachweis nach Abschnitt VII Absatz 1 erfolgt insoweit über diese Zertifizierung.

Nicht als weiterer Auftragsverarbeiter aufgeführt: Der Zahlungsdienstleister Paddle tritt als „Merchant of Record" gegenüber dem Verantwortlichen eigenständig als Verantwortlicher für Zahlungs- und Rechnungsdaten auf. Er erhält keinen Zugriff auf die vom Verantwortlichen eingestellten Kundendaten.

Anlage 2 — Technische und organisatorische Maßnahmen

Die nachfolgende Darstellung beschreibt die Schutzkategorien nach Art. 32 DSGVO und das erreichte Schutzniveau. Einzelheiten der technischen Umsetzung teilt der Auftragsverarbeiter im Rahmen von Abschnitt VII auf Anfrage mit.

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

Zutrittskontrolle. Der Betrieb erfolgt in einem Rechenzentrum in Deutschland, das nach ISO/IEC 27001 zertifiziert ist. Die physische Sicherung obliegt dem in Anlage 1 genannten Anbieter.

Zugangskontrolle. Der Zugang ist auf berechtigte Personen beschränkt und durch persönliche Zugangsdaten geschützt. Passwörter werden nicht im Klartext gespeichert. Eine Zwei-Faktor-Anmeldung steht zur Verfügung. Automatisierte Anmeldeversuche werden unterbunden. Sitzungen enden nach einer Zeit der Untätigkeit automatisch.

Zugriffskontrolle. Nutzer haben ausschließlich Zugriff auf die Daten des eigenen Kontos. Zugriffsrechte sind auf das für die Aufgabenerfüllung Erforderliche beschränkt.

Trennungskontrolle. Die Daten verschiedener Verantwortlicher sind voneinander getrennt und nur dem jeweils Berechtigten zugänglich.

Verschlüsselung. Die Übertragung erfolgt ausschließlich über TLS. Freitextnotizen zu Kunden, Besuchen, Terminen und Wiedervorlagen werden im Ruhezustand mit AES-256-GCM verschlüsselt gespeichert.

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

Weitergabekontrolle. Eine Weitergabe erfolgt ausschließlich an die in Anlage 1 genannten Stellen und ausschließlich verschlüsselt. Der Browser des Nutzers ruft für die Kartenansicht keine fremden Server auf; das Kartenmaterial bezieht der Auftragsverarbeiter selbst und hält es vor.

Eingabekontrolle. Änderungen an Kundendaten werden protokolliert; erfasst werden handelnde Person, Zeitpunkt und Art der Änderung.

Schutz vor Manipulation. Die Anwendung ist nach dem Stand der Technik gegen die gängigen Angriffsarten auf Web-Anwendungen abgesichert.

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

Der in Anlage 1 genannte Anbieter führt regelmäßige Sicherungen von Datenbank und Dateibestand durch. Der Verantwortliche kann seine Daten jederzeit selbst exportieren und damit eine eigene Sicherung vorhalten.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Änderungen werden vor der Auslieferung geprüft, versioniert ausgeliefert und sind rücknehmbar. Es werden keine Analyse-, Tracking- oder Marketing-Cookies eingesetzt. IP-Adressen werden zu Sicherheitszwecken ausschließlich pseudonymisiert gespeichert.

Stand: 2026-08-31