Vertrag zur Auftragsverarbeitung

Anlage zu den Allgemeinen Geschäftsbedingungen für die Plattform Zentrana

Stand **03.11.2026** Auftragsverarbeiter **Tom Gewiese**

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen dem Kunden als Verantwortlichem und Tom Gewiese, Obernaglbach 2, 94259 Kirchberg im Wald, Deutschland, als Auftragsverarbeiter. Die Begriffe Anbieter, Kunde, Nutzer, Vertragsverwalter, Plattform, Bestellung, Angebot, Leistungsbeschreibung, Preisliste, Vertrag, Vertragsschluss, Kundendaten und Kennzahlen haben die Bedeutung aus den Allgemeinen Geschäftsbedingungen; „dieser Vertrag“ ist dieser Vertrag zur Auftragsverarbeitung.

§ 1 Gegenstand und Geltung

(1) Der Anbieter erbringt für den Kunden die Leistungen aus dem Vertrag, auch Zusatzleistungen nach Bestellung oder Angebot. Dabei verarbeitet er im Auftrag des Kunden personenbezogene Daten, die zu den Kundendaten gehören, bei der Nutzung der Plattform durch den Kunden und seine Nutzer entstehen oder die der Anbieter auf Veranlassung des Kunden selbst in die Plattform überträgt (im Folgenden „Auftragsdaten“). Dieser Vertrag regelt die Rechte und Pflichten von Kunde und Anbieter bei dieser Verarbeitung nach Art. 28 DSGVO. Keine Auftragsdaten sind die Daten des Kunden und seiner Ansprechpartner, die der Anbieter als Verantwortlicher verarbeitet, um den Vertrag anzubahnen, durchzuführen und abzurechnen, etwa Bestell-, Rechnungs- und Zahlungsdaten, Annahmen der Rechtstexte und Supportanfragen mit dem Schriftverkehr dazu, sowie die Zugänge der Vertragsverwalter und der Nutzer, die für den Kunden Zugänge und Rechte verwalten dürfen, mit Name, E-Mail Adresse, Rollen, Status und dem Zeitpunkt der letzten Anmeldung; für diese Daten gilt die Datenschutzerklärung. Den Zeitpunkt der letzten Anmeldung dieser Zugänge nutzt der Anbieter nur für den Support, und zwar um bei Anmeldeproblemen zu helfen, nicht mehr genutzte Zugänge zu erkennen und den Zugang für die Supportansicht nach Anlage 1 zu wählen; darüber hinaus fließt er nur wie die Anmeldungen aller Nutzer in Kennzahlen nach § 3 Abs. 4 ein und in keine andere Bewertung des Kunden. Was diese Nutzer in der Plattform verarbeiten, bleibt Auftragsdaten.

(2) Dieser Vertrag ist ein eigener Vertrag und zugleich Anlage der Allgemeinen Geschäftsbedingungen. Der Kunde stimmt ihm mit der Bestellung oder der Annahme eines Angebots zu; er gilt ab der ersten Verarbeitung von Auftragsdaten, auch vor dem Vertragsschluss, und für alle Leistungen aus dem Vertrag, auch für später hinzugebuchte. Regeln dieser Vertrag und die übrigen Teile des Vertrags die Pflichten bei der Verarbeitung von Auftragsdaten unterschiedlich, geht dieser Vertrag vor; Abreden, die Kunde und Anbieter nur für ihren Vertrag oder nur für diesen Vertrag getroffen haben, auch in einem Angebot, gehen ihm für ihren Gegenstand vor. Für Vergütung, Laufzeit, Kündigung und Haftung gelten die Allgemeinen Geschäftsbedingungen, soweit dieser Vertrag nicht ausdrücklich etwas anderes bestimmt. Innerhalb dieses Vertrags gehen die Paragraphen den Anlagen vor; Paragraphen ohne Zusatz sind solche dieses Vertrags.

(3) Dieser Vertrag wird in einem elektronischen Format geschlossen (Art. 28 Abs. 9 DSGVO); der Anbieter speichert die Annahme mit Fassung und Zeitpunkt. Er kann jederzeit unter https://zentrana.de/dpa abgerufen und als PDF gespeichert werden.

(4) Fragen zum Datenschutz richtet der Kunde an info@zentrana.de. Mitteilungen nach diesem Vertrag richtet der Anbieter in Textform an die Vertragsverwalter und an eine weitere E-Mail Adresse, die der Kunde ihm dafür in Textform genannt hat, etwa die seines Datenschutzbeauftragten; im Übrigen gilt § 14 der Allgemeinen Geschäftsbedingungen. Der Kunde hält diese Angaben aktuell und leitet Mitteilungen bei Bedarf an seinen Datenschutzbeauftragten weiter.

(5) Darf der Kunde die Plattform nach § 5 der Allgemeinen Geschäftsbedingungen für Dritte nutzen und verarbeitet er dabei Auftragsdaten im Auftrag eines anderen Verantwortlichen, ist er insoweit Auftragsverarbeiter und der Anbieter weiterer Auftragsverarbeiter (Art. 28 Abs. 4 DSGVO). Der Kunde sichert zu, dass der andere Verantwortliche den Einsatz des Anbieters genehmigt hat und dass die Pflichten aus diesem Vertrag denen genügen, die der Kunde ihm gegenüber übernommen hat; weitergehende Pflichten übernimmt der Anbieter nur durch gesonderte Vereinbarung. Weisungen des anderen Verantwortlichen erteilt allein der Kunde, und Rechte aus diesem Vertrag stehen nur dem Kunden zu. Fällt der Kunde rechtlich oder tatsächlich weg, kann abweichend von Satz 3 der andere Verantwortliche vom Anbieter verlangen, die ihn betreffenden Auftragsdaten nach § 14 herauszugeben oder zu löschen.

§ 2 Dauer

(1) Dieser Vertrag gilt für jede Verarbeitung von Auftragsdaten, auch für eine Verarbeitung vor dem Vertragsschluss, etwa nach dem Absenden der Bestellung, bei einer Freischaltung vor der Annahme eines Angebots oder in einem Testzugang. Er läuft so lange wie der Vertrag und gilt darüber hinaus fort, bis der Anbieter die Auftragsdaten nach § 14 zurückgegeben und gelöscht hat; kommt kein Vertrag zustande, gilt § 14 Abs. 2 bis 5 entsprechend.

(2) Dieser Vertrag kann nicht für sich allein gekündigt werden; seine Dauer richtet sich nach Abs. 1. Verstößt der Anbieter schwerwiegend gegen diesen Vertrag oder bei der Verarbeitung der Auftragsdaten gegen Datenschutzvorschriften, kann der Kunde den Vertrag ganz oder für die betroffenen Leistungen außerordentlich kündigen, wenn der Anbieter den Verstoß nach einer Aufforderung in Textform nicht in angemessener Frist abstellt oder die Aufforderung nach § 314 Abs. 2 BGB entbehrlich ist. Das Recht beider Seiten zur außerordentlichen Kündigung aus anderem wichtigem Grund bleibt unberührt.

§ 3 Art und Zweck der Verarbeitung

(1) Der Anbieter verarbeitet die Auftragsdaten mit den Vorgängen, die die Leistungen aus dem Vertrag und die Einstellungen des Kunden vorsehen, insbesondere durch Erheben, Speichern, Ordnen, Anzeigen, Auswerten, Übermitteln, Exportieren, Pseudonymisieren, Anonymisieren und Löschen (Art. 4 Nr. 2 DSGVO). Dazu gehören Benachrichtigungen an Nutzer, Dokumente und Exporte auf Anforderung, Übermittlungen an Empfänger, die der Kunde in der Plattform festlegt, und der lesende Zugriff im Support nach Anlage 1. Setzt eine gebuchte Funktion Verfahren der künstlichen Intelligenz ein, gehört auch diese Verarbeitung dazu.

(2) Zweck der Verarbeitung ist die Erbringung der Leistungen aus dem Vertrag, insbesondere die Bereitstellung und der Betrieb der Plattform, ihre Wartung und Sicherheit, die Analyse und Behebung von Fehlern, die Wiederherstellung nach Störungen, der Support, vereinbarte Zusatzleistungen wie Einrichtung und Datenübernahme sowie die Prüfung gemeldeter Inhalte und Maßnahmen nach § 7 der Allgemeinen Geschäftsbedingungen.

(3) Der Anbieter verarbeitet Auftragsdaten nicht zu eigenen Zwecken, insbesondere nicht für Werbung, zur Bildung von Profilen oder zum Training von Modellen der künstlichen Intelligenz; Abs. 4 und 5 bleiben unberührt. Bestimmt er unter Verstoß gegen die DSGVO selbst die Zwecke und Mittel einer Verarbeitung, gilt er insoweit als Verantwortlicher (Art. 28 Abs. 10 DSGVO).

(4) Aus Auftragsdaten bildet der Anbieter Kennzahlen über Umfang und Art der Nutzung nach § 5 der Allgemeinen Geschäftsbedingungen, indem er je Kunde und Leistung Personen mit Zugang, Anmeldungen, Vorgänge und Zeitpunkte der Nutzung zählt und zusammenfasst. Inhalte wertet er dafür nicht aus, insbesondere nicht die Art einer Abwesenheit oder andere Daten besonderer Kategorien. Für die Zählung und die Kennzahlen ist der Anbieter selbst Verantwortlicher; Zweck und Rechtsgrundlage nennt die Datenschutzerklärung. Kennzahlen je Kunde bildet er nur für Kunden mit mindestens fünf Personen mit Zugang, gezählt als Bestand zum Zeitpunkt der Zählung nach denselben Regeln wie für die Abrechnung und nicht nach der Nutzung, und nur so, dass sie weder einen Nutzer noch eine andere betroffene Person erkennen lassen, auch nicht zusammen mit anderen Daten des Anbieters; was er daraus ableitet, etwa dass ein Kunde die Plattform lange nicht genutzt hat, bezieht er nur auf den Kunden. Für Kunden unter dieser Schwelle bildet er keine Kennzahlen je Kunde und leitet aus ihren Anmelde- und Nutzungsdaten nichts ab; in Summen über alle Kunden gehen von ihnen nur die Zahl der Personen mit Zugang und Angaben zum Vertrag ein. Er nutzt die Kennzahlen nur zu den Zwecken nach § 5 der Allgemeinen Geschäftsbedingungen und verwendet die gezählten Daten für keinen anderen Zweck; Abs. 5 und § 1 Abs. 1 Satz 4 bis 6 bleiben unberührt.

(5) Daten über Zugänge, Anmeldungen und Sitzungen der Nutzer verarbeitet der Anbieter außerdem als Verantwortlicher, soweit er sie für die Sicherheit der Plattform, die Abwehr von Missbrauch und die Abrechnung nach der Zahl der Personen mit Zugang braucht. Ebenso verarbeitet er als Verantwortlicher Meldungen von E-Mail Diensten, dass eine Empfängeradresse von E-Mails der Plattform dauerhaft nicht zustellbar ist oder dass sich ihr Inhaber über eine solche E-Mail beschwert hat; diese Adressen führt er in einer Sperrliste, die beim Versand für alle Kunden und beim eigenen Versand des Anbieters gilt, auch an Kontakte seines Vertriebs, allein um die Zustellbarkeit seiner E-Mails und der E-Mails der Plattform zu schützen und Beschwerden zu beachten. Meldungen zu E-Mails, die die Plattform im Auftrag des Kunden versendet, vermerkt er nicht an bestehenden Kontakten seines Vertriebs; legt er aus einer Anfrage einen neuen Kontakt mit einer gesperrten Adresse an, zeigt dieser nur die Sperre nach Satz 2 mit ihrem Grund. Für andere Zwecke, insbesondere um Werbung zu senden oder Kontakte für den Vertrieb zu gewinnen, verwendet er die Daten nach Satz 1 und 2 nicht; Zweck, Rechtsgrundlage und Fristen nennt die Datenschutzerklärung. Abs. 4, § 1 Abs. 1 Satz 4 bis 6 und die Verarbeitung dieser Daten im Auftrag des Kunden nach Abs. 1 und 2, etwa im Support, bleiben unberührt.

§ 4 Art der Daten

(1) Verarbeitet werden die Auftragsdaten, die der Kunde und seine Nutzer in die Plattform eingeben, über Schnittstellen oder Importe einspielen oder bei der Nutzung erzeugen, sowie Auftragsdaten, die der Anbieter für den Kunden übernimmt, je nach den Leistungen aus dem Vertrag insbesondere:

1. Stammdaten: Name, Kontaktdaten wie E-Mail Adresse und Mobilnummer, Personalnummern auch für die Lohnabrechnung, Art der Vergütung, Ein- und Austrittsdatum, Firma bei externen Personen, Zuordnung zu Organisationseinheiten und Standorten, Rollen und Rechte.

2. Zugangs- und Sicherheitsdaten: Kennwörter als Hashwert, Daten des zweiten Anmeldefaktors, vertrauenswürdige Geräte, Sitzungen mit Netzadresse und Browserkennung sowie Zugangsschlüssel für Schnittstellen.

3. Protokolldaten: Änderungen mit Zeitpunkt, handelnder Person, vorherigem und neuem Stand, Grund, Netzadresse und Browserkennung.

4. Arbeitszeit- und Abrechnungsdaten: Kommen, Gehen und Pausen, Korrekturen mit Begründung, Arbeitszeitmodelle, Salden, Abschlüsse, Projektzeiten und ihre Bestätigung sowie Angaben zur Vorbereitung der Lohnabrechnung, etwa Lohnarten, Stunden und Tage je Lohnart, Zuschläge, Auszahlungen, Abgeltungen und Exporte an die Lohnbuchhaltung.

5. Abwesenheitsdaten: Art, Zeitraum, Begründung, Antrag und Entscheidung, Urlaubsansprüche sowie der Stand von Nachweisen, etwa zu einer Arbeitsunfähigkeit.

6. Standortbezogene Daten der Zeiterfassung, nur wenn der Kunde die Standortprüfung einschaltet: das Ergebnis der Prüfung, gerundete Werte zu Entfernung und Genauigkeit, Begründungen und Prüfvermerke sowie die Information und Einwilligung der Beschäftigten.

7. Unterschriften als Bild, etwa bei Kontrollen, Unterweisungen, Prüfungen, Übergaben und Quittungen.

8. Fahrzeug-, Fahrt- und Fahrerdaten: Buchungen, Zuordnungen und Übergaben, Fahrtenbuch mit Art der Fahrt, Orten, Zweck und Kilometerständen, Ladevorgänge, Schäden mit Fotos und Angaben zum Verschulden, Kosten einschließlich Bußgeldern, Führerscheinklassen, Gültigkeit, Kontrollen und Unterweisungen.

9. Schlüssel- und Zutrittsdaten: Ausgaben, Rückgaben, Quittungen, Schließberechtigungen, Verluste und Inventuren.

10. Inhalte der Zusammenarbeit, der Projekte und des Kalenders: Karten, Kommentare, Dateien, Termine, Aufgaben, Fristen und Projektzuordnungen.

11. Finanz- und Kostendaten: Stammdaten von Rechnungsempfängern und ihren Ansprechpartnern, Angebote, Rechnungen und andere Belege, Zahlungen, offene Posten und Mahnungen, Versand- und Exportdaten sowie Kosten- und Verrechnungssätze, die einer Person zugeordnet sind.

12. Sonstige Inhalte: Daten jeder Art, die Nutzer in Freitextfelder, Kommentare oder Dateien eingeben; welche das sind, bestimmt allein der Kunde.

(2) Zu den Auftragsdaten können Daten besonderer Kategorien nach Art. 9 Abs. 1 DSGVO gehören, insbesondere Gesundheitsdaten der Beschäftigten und ihrer Angehörigen in Abwesenheiten wegen Krankheit oder der Erkrankung eines Kindes, im Stand von Nachweisen dazu, in Lohnarten für Krankheit und in Nachweisen zu Führerscheinkontrollen. Für Abwesenheitsarten der Kategorie „Krank“ gelten zusätzlich die Maßnahmen, die Anlage 1 unter „Datensparsamkeit und besondere Kategorien“ beschreibt. Legt der Kunde Abwesenheitsarten mit Gesundheitsbezug in einer anderen Kategorie an, etwa für die Erkrankung eines Kindes, schützt er sie über die Rechte seiner Nutzer. Die Plattform sieht kein Feld für Diagnosen vor; der Kunde sorgt dafür, dass Nutzer Daten besonderer Kategorien in Freitext und Dateien nur erfassen, soweit er sie benötigt.

(3) Ordnet der Kunde Bußgelder oder andere Angaben zu Verkehrsverstößen einer Person zu, können das Daten über Straftaten nach Art. 10 DSGVO sein. Ihre Verarbeitung ist nur zulässig, soweit eine Rechtsgrundlage sie erlaubt; das prüft und verantwortet der Kunde.

§ 5 Kategorien betroffener Personen

1. Beschäftigte des Kunden und Personen in vergleichbarer Stellung, etwa Auszubildende, Praktikanten, Aushilfen, Leiharbeitnehmer und Organmitglieder, auch nach ihrem Ausscheiden.

2. Nutzer, auch solche, deren Zugang der Anbieter auf Veranlassung des Kunden einrichtet.

3. Personen, denen der Kunde Fahrzeuge, Schlüssel oder andere Betriebsmittel überlässt, ohne dass sie bei ihm beschäftigt sind.

4. Abnehmer, Lieferanten, Werkstätten und andere Geschäftspartner des Kunden sowie deren Ansprechpartner.

5. Angehörige von Beschäftigten, soweit Abwesenheiten oder andere Einträge sie betreffen, etwa bei der Erkrankung eines Kindes.

6. Weitere Personen, deren Daten der Kunde oder seine Nutzer in die Plattform eingeben.

§ 6 Verantwortung des Kunden

(1) Der Kunde ist für die Auftragsdaten Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, soweit nicht § 3 Abs. 4 und 5 den Anbieter als Verantwortlichen bestimmen; verarbeitet der Kunde sie im Auftrag eines anderen Verantwortlichen, gilt § 1 Abs. 5. Er entscheidet, welche Daten er in der Plattform verarbeitet, und ist dafür verantwortlich, dass diese Verarbeitung zulässig ist, insbesondere dass für Daten seiner Beschäftigten und für Daten besonderer Kategorien eine Rechtsgrundlage besteht und die Verarbeitung erforderlich ist. Die eigenen Pflichten des Anbieters aus der DSGVO und aus diesem Vertrag bleiben unberührt. Erklärungen des Kunden in der Plattform, etwa die Wahl einer Rechtsgrundlage, die Freigabe einer Funktion oder die Information und Einwilligung von Beschäftigten, prüft der Anbieter nicht; er darf sich auf sie verlassen. § 7 Abs. 5 bleibt unberührt.

(2) Besteht beim Kunden eine Arbeitnehmervertretung, etwa ein Betriebsrat, ein Personalrat oder eine Mitarbeitervertretung, wahrt er in eigener Verantwortung deren Beteiligungsrechte, bevor er Funktionen einführt oder anwendet, die objektiv geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen. Verlangt die Plattform für eine solche Funktion eine Freigabe, bestätigt der Kunde mit ihr, dass er diese Rechte gewahrt hat.

(3) Ob vor dem Einsatz einer Funktion eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO nötig ist, prüft der Kunde, insbesondere bei Funktionen mit Daten besonderer Kategorien oder mit Standortbezug. Dabei prüft er auch, ob die Maßnahmen nach Anlage 1 für das Risiko seiner Verarbeitung ausreichen; der Anbieter unterstützt ihn nach § 12.

(4) Der Kunde informiert die betroffenen Personen nach Art. 13 und 14 DSGVO.

(5) Der Kunde vergibt die Zugänge, Rollen und Rechte seiner Nutzer selbst und hält sie aktuell. Er trägt Austritte spätestens zum Austrittstag ein, sperrt nicht mehr benötigte Zugänge unverzüglich und sorgt dafür, dass Nutzer ihre Zugangsdaten geheim halten. Nutzer, die Daten besonderer Kategorien sehen dürfen, hält er an, den zweiten Anmeldefaktor der Plattform einzurichten. Für die Sicherheit der Endgeräte und Netze, mit denen seine Nutzer auf die Plattform zugreifen, und für Daten, die der Kunde oder seine Nutzer aus der Plattform exportieren, herunterladen oder ausdrucken, ist der Kunde verantwortlich.

(6) Stellt der Kunde Fehler oder Unregelmäßigkeiten bei der Verarbeitung fest oder vermutet er eine Verletzung des Schutzes von Auftragsdaten, teilt er das dem Anbieter unverzüglich in Textform an info@zentrana.de mit.

(7) Verletzt der Kunde seine Pflichten nach diesem Paragraphen schuldhaft, bleiben die Ansprüche des Anbieters nach den Allgemeinen Geschäftsbedingungen, insbesondere auf Freistellung von Ansprüchen Dritter, unberührt.

§ 7 Weisungen

(1) Der Anbieter und die ihm unterstellten Personen verarbeiten die Auftragsdaten nur auf dokumentierte Weisung des Kunden, auch bei einer Übermittlung an ein Drittland oder eine internationale Organisation (Art. 28 Abs. 3 Buchst. a und Art. 29 DSGVO). Das gilt nicht, soweit das Recht der Union oder eines Mitgliedstaats, dem der Anbieter unterliegt, ihn zur Verarbeitung verpflichtet. Dann teilt er dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Kunden ergeben sich aus der Leistungsbeschreibung und den übrigen Teilen des Vertrags, aus diesem Vertrag mit seinen Anlagen und aus den Einstellungen und Funktionen der Plattform, etwa zu Rechten, Empfängern sowie Aufbewahrungs- und Löschfristen. Was Nutzer in der Plattform im Rahmen der Rechte tun, die der Kunde ihnen eingeräumt hat, gilt als Weisung des Kunden; dasselbe gilt für Voreinstellungen, solange der Kunde sie nicht ändert. Ohne Einzelweisung greift der Anbieter auf Auftragsdaten nur zu den Zwecken nach § 3 Abs. 2 zu; die Supportanfrage eines Nutzers ist die Weisung, die Auftragsdaten zu verarbeiten, die ihre Bearbeitung erfordert.

(3) Einzelne Weisungen erteilen die Vertragsverwalter und Personen, die einer von ihnen dafür in Textform benennt, in Textform an info@zentrana.de oder über die Supportanfrage der Plattform. Mündliche Weisungen bestätigt der Kunde unverzüglich in Textform; bis dahin und solange die Befugnis der anweisenden Person nicht feststeht, darf der Anbieter die Ausführung zurückstellen, es sei denn, ein Aufschub gefährdet die Auftragsdaten. Der Anbieter dokumentiert jede Einzelweisung und bewahrt sie als eigene Unterlage nach § 14 Abs. 4 auf; Änderungen der Einstellungen hält das Änderungsprotokoll nach Anlage 1 fest.

(4) Weisungen, mit denen der Kunde eine Verarbeitung einschränkt oder beendet oder die Löschung von Auftragsdaten verlangt, befolgt der Anbieter stets; lässt sich eine solche Weisung nur umsetzen, wenn eine Leistung insoweit entfällt, erbringt er diese Leistung insoweit nicht mehr. Andere Weisungen zum Umgang mit Auftragsdaten im Rahmen der vereinbarten Leistungen, etwa sie zu berichtigen oder an den Kunden herauszugeben, führt der Anbieter ebenfalls aus. Außer in den Fällen des Satzes 1 muss der Anbieter eine Weisung nicht ausführen, die verlangt, die Leistungen oder die Plattform zu ändern oder zu erweitern, etwa um eine neue Funktion oder um eine Ausnahme von einer Schutzvorkehrung nach Anlage 1; er kann ihre Umsetzung gegen gesonderte Vergütung anbieten oder sie ablehnen. Lehnt er eine Weisung ab, die der Kunde zur Erfüllung seiner Pflichten aus der DSGVO benötigt, kann der Kunde den Vertrag für die betroffenen Leistungen zu einem Tag, den er bestimmt, außerordentlich kündigen; § 11 Abs. 5 Satz 2 gilt entsprechend.

(5) Ist der Anbieter der Auffassung, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt, weist er den Kunden unverzüglich in Textform darauf hin. Er darf die Ausführung aussetzen, bis der Kunde die Weisung ändert oder ihre Rechtmäßigkeit nachvollziehbar darlegt. Eine Weisung, die offensichtlich gegen Datenschutzvorschriften verstößt oder deren Ausführung den Anbieter gegen eigene Pflichten aus der DSGVO verstoßen ließe, darf er ablehnen. Besteht der Kunde nach dem Hinweis auf der Weisung, kann er den Vertrag für die betroffenen Leistungen außerordentlich kündigen, der Anbieter nur in den Fällen des Satzes 3.

§ 8 Ort der Verarbeitung und Drittländer

(1) Der Anbieter speichert die Auftragsdaten in der Europäischen Union oder im Europäischen Wirtschaftsraum, seine Unterauftragsverarbeiter an den Orten, die Anlage 2 für sie nennt; was die Allgemeinen Geschäftsbedingungen zum Standort des Rechenzentrums zusagen, bleibt unberührt. Übermittlungen in Drittländer, auch durch Zugriffe aus der Ferne, richten sich nach Abs. 2. Will der Anbieter die Speicherung an einen anderen Ort verlegen, gelten § 11 Abs. 3 bis 5 entsprechend.

(2) Auftragsdaten übermittelt der Anbieter in ein Drittland oder an eine internationale Organisation nur unter den Voraussetzungen des Kapitels V DSGVO und nur auf Weisung des Kunden; § 7 Abs. 1 Satz 2 bleibt unberührt. Als Weisung gilt auch, dass Anlage 2 eine Übermittlung mit ihrer Grundlage nennt, etwa einen Angemessenheitsbeschluss (Art. 45 DSGVO) oder Standardvertragsklauseln (Art. 46 Abs. 2 Buchst. c DSGVO), auch durch die weiteren Auftragsverarbeiter eines Unterauftragsverarbeiters. Greift ein Unterauftragsverarbeiter oder einer seiner weiteren Auftragsverarbeiter aus einem Drittland auf Auftragsdaten zu, die in der Europäischen Union oder im Europäischen Wirtschaftsraum gespeichert sind, ist das eine Übermittlung im Sinne von Satz 1.

(3) Legt der Kunde in der Plattform selbst Empfänger fest, etwa Adressen für Webhooks, Schnittstellen oder den Versand von Dokumenten per E-Mail, übermittelt der Anbieter die Daten auf Weisung des Kunden an diese Empfänger. Die Empfänger sind keine Unterauftragsverarbeiter des Anbieters; Dienstleister, über die der Anbieter die Übermittlung abwickelt, etwa für den Versand von E-Mails, sind es nach § 11. Ob eine solche Übermittlung zulässig ist, auch nach Kapitel V DSGVO, prüft und verantwortet im Verhältnis zum Anbieter der Kunde; § 7 Abs. 5 bleibt unberührt.

§ 9 Vertraulichkeit und Datenschutzorganisation

(1) Der Anbieter stellt sicher, dass sich alle Personen, die Auftragsdaten verarbeiten dürfen, zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Buchst. b DSGVO). Die Pflicht gilt über das Ende ihrer Tätigkeit und über das Ende dieses Vertrags hinaus.

(2) Personen, die für den Anbieter tätig sind (Mitarbeitende des Anbieters), greifen auf Auftragsdaten nur zu, soweit es für die Einrichtung, den Betrieb und die Sicherheit der Plattform, die Behebung einer Störung, die Bearbeitung einer Anfrage des Kunden oder die Prüfung gemeldeter Inhalte und Maßnahmen nach § 3 Abs. 2 nötig ist. In der Plattform nutzen sie dafür nur die Wege, die Anlage 1 beschreibt. Der Anbieter stellt sicher, dass ihm unterstellte Personen mit Zugang zu Auftragsdaten diese nur auf Weisung des Kunden verarbeiten, es sei denn, das Recht der Union oder eines Mitgliedstaats verpflichtet sie dazu (Art. 29 und Art. 32 Abs. 4 DSGVO).

(3) Der Anbieter führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO. Ist der Anbieter gesetzlich verpflichtet, einen Datenschutzbeauftragten zu benennen, benennt er ihn und teilt dem Kunden dessen Kontaktdaten und jeden Wechsel unverzüglich in Textform mit. Mit der Aufsichtsbehörde arbeitet er auf Anfrage zusammen (Art. 31 DSGVO); für Prüfungen gilt § 15 Abs. 6.

§ 10 Sicherheit der Verarbeitung

(1) Der Anbieter trifft alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 3 Buchst. c DSGVO). Anlage 1 beschreibt die Maßnahmen, die er dafür mindestens trifft. Die Beschreibung legt fest, welche Maßnahmen er mindestens schuldet; eine Garantie im Sinne von § 11 der Allgemeinen Geschäftsbedingungen übernimmt er damit nicht.

(2) Die Maßnahmen gewährleisten ein Schutzniveau, das dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessen ist, insbesondere bei Daten besonderer Kategorien. Dabei berücksichtigt der Anbieter den Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos. Er überprüft, bewertet und evaluiert die Wirksamkeit der Maßnahmen regelmäßig (Art. 32 Abs. 1 Buchst. d DSGVO). Er darf die Maßnahmen weiterentwickeln und durch andere ersetzen, die mindestens denselben Schutz bieten.

(3) Wesentliche Änderungen hält der Anbieter in Anlage 1 fest und teilt sie dem Kunden spätestens mit ihrem Wirksamwerden in Textform auf den Wegen nach § 1 Abs. 4 mit; solange das Schutzniveau nicht sinkt, bedürfen sie keiner Zustimmung des Kunden. Eine Änderung, die das Schutzniveau senkt, wird nur durch Vereinbarung in Textform wirksam.

§ 11 Unterauftragsverarbeiter

(1) Der Kunde erteilt dem Anbieter mit diesem Vertrag die allgemeine schriftliche Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen (Art. 28 Abs. 2 Satz 1 und Abs. 9 DSGVO). Die Unterauftragsverarbeiter in Anlage 2 und die weiteren Auftragsverarbeiter, die dort genannt oder über einen Verweis aufgeführt sind, sind genehmigt. Der Anbieter wählt jeden Unterauftragsverarbeiter danach aus, ob er hinreichende Garantien für geeignete technische und organisatorische Maßnahmen bietet.

(2) Unterauftragsverarbeiter ist, wer im Auftrag des Anbieters Auftragsdaten verarbeitet oder bei seiner Leistung Zugriff auf sie erhalten kann, auch ein externer Dienst, den eine Funktion der Plattform nutzt, etwa für den Versand von E-Mails oder für Verfahren der künstlichen Intelligenz. Keine Unterauftragsverarbeiter sind Dienstleister für Nebenleistungen ohne Zugriff auf Auftragsdaten, etwa für den reinen Transport von Daten über öffentliche Netze oder für den Zahlungsverkehr des Anbieters, und Empfänger nach § 8 Abs. 3; Dienste, die E-Mails mit Auftragsdaten versenden, empfangen oder speichern, sind Unterauftragsverarbeiter.

(3) Der Anbieter informiert den Kunden mindestens sechs Wochen im Voraus in Textform, wenn er einen Unterauftragsverarbeiter hinzuziehen oder ersetzen will oder wenn sich bei einem Unterauftragsverarbeiter der Ort der Verarbeitung oder eine Übermittlung in Drittländer mit ihrer Grundlage ändern soll. Die Information nennt Name, Anschrift und Leistung des Unterauftragsverarbeiters, die betroffenen Daten, den Ort der Verarbeitung und eine Übermittlung in Drittländer mit ihrer Grundlage. Erfordern der Schutz der Auftragsdaten oder die Aufrechterhaltung des Betriebs einen schnelleren Wechsel, etwa weil ein Unterauftragsverarbeiter ausfällt, informiert der Anbieter den Kunden so früh vor dem Wechsel, dass dieser noch vor ihm Einspruch erheben kann.

(4) Der Kunde kann innerhalb von 14 Kalendertagen nach Zugang der Information in Textform Einspruch erheben; ein Wechsel nach Abs. 3 Satz 3 verkürzt diese Frist nicht. Er soll dabei seine Gründe nennen, etwa Zweifel an den Garantien des Unterauftragsverarbeiters oder an der Grundlage einer Übermittlung. Erhebt er keinen Einspruch, gilt die Änderung als genehmigt; auf die Frist, diese Folge und die Rechte nach Abs. 5 weist der Anbieter in der Information hin. Bei einem Einspruch suchen Kunde und Anbieter gemeinsam eine Lösung, etwa eine andere Einstellung oder den Verzicht auf den Einsatz für die Auftragsdaten des Kunden.

(5) Lässt sich ein Einspruch nicht ausräumen, kann der Kunde den Vertrag für die betroffenen Leistungen zu dem Zeitpunkt außerordentlich kündigen, an dem die Änderung wirksam werden soll, bei einem Wechsel nach Abs. 3 Satz 3 auch mit sofortiger Wirkung. Vergütung, die der Kunde für die Zeit nach dem Ende im Voraus gezahlt hat, schreibt der Anbieter gut oder erstattet sie. Kündigt der Kunde nicht, setzt der Anbieter den Unterauftragsverarbeiter für die Auftragsdaten des Kunden nicht oder nicht weiter ein, außer bei einem Wechsel nach Abs. 3 Satz 3; ist ihm das nicht zumutbar, kann er die betroffenen Leistungen nur nach den Allgemeinen Geschäftsbedingungen einstellen oder den Vertrag nur nach ihnen kündigen.

(6) Der Anbieter legt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die dieser Vertrag nach Art. 28 Abs. 3 DSGVO für ihn festlegt, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 Satz 1 DSGVO). Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Anbieter dem Kunden für die Einhaltung dieser Pflichten wie für eigene (Art. 28 Abs. 4 Satz 2 DSGVO); für den Umfang gilt § 16. Auf Verlangen stellt der Anbieter dem Kunden die Datenschutzpflichten eines Unterauftragsverarbeiters aus dessen Vertrag in Textform zur Verfügung, Geschäftsgeheimnisse geschwärzt, und teilt ihm unverzüglich mit, wenn dieser sie bei Auftragsdaten des Kunden nicht erfüllt.

(7) Setzt ein Unterauftragsverarbeiter seinerseits weitere Auftragsverarbeiter ein, gilt Abs. 6 für ihn entsprechend; Anlage 2 nennt diese oder verweist auf seine Liste. Der Anbieter verpflichtet jeden Unterauftragsverarbeiter, ihn über beabsichtigte Änderungen dieser Liste vorab zu informieren, und gibt jede solche Information unverzüglich mit den Angaben nach Abs. 3 Satz 2 an den Kunden weiter, soweit sie ihm vorliegen. Der Kunde kann nach Abs. 4 Einspruch erheben; lässt sich der Einspruch nicht ausräumen, kann er die betroffenen Leistungen zum Wirksamwerden der Änderung außerordentlich kündigen, und Abs. 5 Satz 2 gilt entsprechend.

§ 12 Unterstützung des Kunden und Anfragen Dritter

(1) Der Anbieter unterstützt den Kunden angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu beantworten (Art. 28 Abs. 3 Buchst. e DSGVO). Vorrangig dienen dazu die Funktionen der Plattform, mit denen der Kunde Auftragsdaten je nach Leistung anzeigen, berichtigen, exportieren, löschen oder unkenntlich machen kann. Wendet sich eine betroffene Person mit einem Antrag zu Auftragsdaten an den Anbieter, leitet er ihn unverzüglich an den Kunden weiter, soweit er ihn dem Kunden zuordnen kann, und teilt der Person die Weiterleitung mit; in der Sache antwortet er nur auf Weisung des Kunden.

(2) Der Anbieter unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere nach einer Verletzung, bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 28 Abs. 3 Buchst. f DSGVO). Dafür stellt er vorrangig diesen Vertrag mit seinen Anlagen, die Leistungsbeschreibung und Auskünfte über seine Verarbeitung in Textform bereit. Die Datenschutz-Folgenabschätzung, die Bewertung des Risikos einer Verletzung und die rechtliche Beurteilung bleiben Sache des Kunden.

(3) Verlangt eine Behörde, ein Gericht oder ein anderer Dritter Auftragsdaten vom Anbieter, verweist er die anfragende Stelle, soweit zulässig, an den Kunden und informiert diesen unverzüglich, sofern das Recht der Union oder eines Mitgliedstaats die Information nicht wegen eines wichtigen öffentlichen Interesses verbietet. Herausgeben darf er Auftragsdaten nur auf dokumentierte Weisung des Kunden oder soweit ihn das Recht der Union oder eines Mitgliedstaats, dem er unterliegt, dazu verpflichtet, und nur in dem Umfang, den diese Pflicht verlangt; § 7 Abs. 1 gilt. Ersuchen von Gerichten und Behörden eines Drittlands befolgt er nur, wenn sie auf einer internationalen Übereinkunft nach Art. 48 DSGVO beruhen oder der Kunde die Herausgabe nach § 8 Abs. 2 anweist. Drohen den Auftragsdaten beim Anbieter Pfändung, Beschlagnahme oder Maßnahmen in einem Insolvenzverfahren, informiert er den Kunden unverzüglich und weist die Beteiligten darauf hin, dass die Auftragsdaten dem Kunden zustehen und er sie nur in dessen Auftrag verarbeitet.

(4) Ohne gesondertes Entgelt stellt der Anbieter die Funktionen der Plattform bereit, leitet Anträge nach Abs. 1 weiter, erteilt in Textform Auskünfte über seine Verarbeitung, deren Aufbau er bestimmt, erfüllt seine Pflichten nach § 13 und ermöglicht Exporte nach § 10 der Allgemeinen Geschäftsbedingungen. Weitere Unterstützung, die der Kunde verlangt, etwa Auswertungen oder Aufbereitungen von Auftragsdaten außerhalb der Funktionen, Angaben in seinen Formularen oder Fragebögen, Entwürfe für seine Meldungen und Benachrichtigungen oder die Teilnahme an Terminen, vergütet der Kunde. Das gilt nicht, soweit der Aufwand auf einem Verstoß des Anbieters gegen diesen Vertrag oder gegen Datenschutzvorschriften beruht.

(5) Bevor der Anbieter Unterstützung nach Abs. 4 Satz 2 beginnt, nennt er dem Kunden in Textform den Stundensatz aus Angebot oder Preisliste, sonst einen angemessenen Stundensatz, und den voraussichtlichen Aufwand. Hält der Kunde danach an seinem Verlangen fest, vergütet er den tatsächlichen Aufwand zu diesem Satz. Weist das Gesetz dem Kunden die Kosten einer Mitwirkung nach Abs. 3 zu, etwa § 147 Abs. 6 AO bei einer Außenprüfung, vergütet er den Aufwand des Anbieters zum Stundensatz nach Satz 1.

§ 13 Verletzungen des Schutzes personenbezogener Daten

(1) Der Anbieter meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO), die Auftragsdaten betrifft, auch bei einem Unterauftragsverarbeiter, unverzüglich, nachdem sie ihm bekannt geworden ist (Art. 33 Abs. 2 DSGVO). Er meldet in Textform auf den Wegen nach § 1 Abs. 4, ohne zuvor das Risiko für die betroffenen Personen zu bewerten. Hält der Kunde seine Angaben nach § 1 Abs. 4 nicht aktuell und verzögert sich die Meldung deshalb, hat der Anbieter diese Verzögerung nicht zu vertreten.

(2) Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: die Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, eine Anlaufstelle beim Anbieter, die wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Abmilderung. Soweit bekannt, nennt sie außerdem die betroffenen Kategorien personenbezogener Daten mit der Angabe, ob Daten nach Art. 9 Abs. 1 DSGVO darunter sind, sowie den Zeitpunkt der Verletzung und den Zeitpunkt, zu dem der Anbieter von ihr erfahren hat. Was noch nicht bekannt ist, reicht der Anbieter schrittweise und ohne unangemessene weitere Verzögerung nach.

(3) Der Anbieter ergreift unverzüglich die Maßnahmen, die nötig sind, um die Verletzung einzudämmen und ihre Folgen zu mildern; der Kunde weist ihn hierzu mit diesem Vertrag an. Maßnahmen, die allein die Auftragsdaten des Kunden betreffen, stimmt er mit ihm ab, soweit die Lage es erlaubt; Maßnahmen für die ganze Plattform trifft er nach pflichtgemäßem Ermessen. Er dokumentiert die Verletzung mit ihren Umständen, Folgen und Maßnahmen.

(4) Die Meldung an die Aufsichtsbehörde und die Benachrichtigung betroffener Personen sind Sache des Kunden; der Anbieter unterstützt ihn dabei nach § 12 Abs. 2. Übernimmt der Anbieter auf einen Auftrag des Kunden in Textform im Einzelfall die Meldung in dessen Namen, bleibt der Kunde für sie verantwortlich; die Vergütung richtet sich nach § 12 Abs. 4 und 5.

(5) Gegenüber Aufsichtsbehörden und betroffenen Personen äußert sich der Anbieter zu einer Verletzung von Auftragsdaten nur nach Abstimmung mit dem Kunden. Ausgenommen sind Sicherheitshinweise an Nutzer, die zur Eindämmung nötig sind, etwa die Aufforderung, ein Kennwort zu ändern, Äußerungen, zu denen ihn das Recht der Union oder eines Mitgliedstaats verpflichtet, eigene Meldungen als Verantwortlicher und die Wahrnehmung seiner Rechte, etwa die Verteidigung gegen Ansprüche.

(6) Eine Meldung oder Unterstützung nach diesem Paragraphen ist kein Anerkenntnis einer Pflichtverletzung, eines Verschuldens oder einer Haftung des Anbieters.

§ 14 Rückgabe und Löschung

(1) Während der Laufzeit kann der Kunde seine Daten jederzeit über die Exportfunktionen der Plattform abrufen.

(2) Nach dem Ende des Vertrags gibt der Anbieter dem Kunden die Auftragsdaten nach dessen Wahl zurück oder löscht sie (Art. 28 Abs. 3 Buchst. g DSGVO). Zur Rückgabe stellt er sie in dem Umfang, für die Frist und in den Formaten nach § 10 der Allgemeinen Geschäftsbedingungen zum Abruf bereit. Danach löscht er die Auftragsdaten unverzüglich einschließlich Protokollen, Dateien und Kopien, auch soweit sie nicht exportiert werden, es sei denn, das Recht der Union oder eines Mitgliedstaats verpflichtet ihn zur Speicherung; dann verarbeitet er sie nur noch zu diesem Zweck. Seine Unterauftragsverarbeiter verpflichtet er, ebenso zu verfahren; auf Anfrage bestätigt er die Löschung in Textform und teilt mit, welche Daten eine Pflicht zur Speicherung betrifft.

(3) Der Kunde kann vor Ablauf der Frist nach Abs. 2 in Textform verlangen, dass der Anbieter die Auftragsdaten unverzüglich löscht; das Verlangen ist eine Einzelweisung nach § 7 Abs. 3.

(4) Aufbewahrungspflichten, die den Kunden selbst treffen, etwa nach Arbeits- oder Steuerrecht, erfüllt der Kunde, indem er seine Daten rechtzeitig exportiert. Eigene Unterlagen des Anbieters über das Vertragsverhältnis, etwa Rechnungen sowie Vertrags-, Support- und Löschnachweise einschließlich dokumentierter Weisungen, bewahrt er nach § 10 der Allgemeinen Geschäftsbedingungen gesperrt auf und verarbeitet sie dabei als Verantwortlicher. Enthalten sie Auftragsdaten, behält er davon nur, was er zur Erfüllung gesetzlicher Aufbewahrungspflichten oder zum Nachweis der Einhaltung dieses Vertrags braucht, verwendet es zu keinem anderen Zweck und löscht es, sobald dieser Zweck entfällt; die Fristen nennt die Datenschutzerklärung. E-Mails, die die Plattform im Auftrag des Kunden versendet, etwa Benachrichtigungen, Erinnerungen, Belege und Quittungen an Nutzer und andere Empfänger, sind keine solchen Unterlagen; sie löscht der Anbieter mit den übrigen Auftragsdaten nach Abs. 2. Nicht im Auftrag des Kunden versendet der Anbieter E-Mails zur Anmeldung, etwa mit einem Link zum Festlegen oder Zurücksetzen eines Kennworts oder zur Bestätigung oder Änderung einer E-Mail Adresse; für sie ist er Verantwortlicher nach § 1 Abs. 1 Satz 4 und § 3 Abs. 5, und ihre Fristen nennt die Datenschutzerklärung.

(5) Soweit Auftragsdaten in Datensicherungen enthalten sind, löscht der Anbieter sie dort nicht einzeln. Sie werden innerhalb von 30 Tagen nach der Löschung der Auftragsdaten überschrieben, auch nach einer Löschung während der Laufzeit, und sind bis dahin gesperrt. Der Anbieter verwendet sie nur, um nach einer Störung den Betrieb oder auf Weisung des Kunden einzelne Daten wiederherzustellen; wird eine Sicherung zurückgespielt, löscht er die zuvor gelöschten Auftragsdaten erneut.

(6) Endet nur eine einzelne Leistung, etwa nach einer Teilkündigung nach § 9 der Allgemeinen Geschäftsbedingungen, § 7 Abs. 4 oder § 11 Abs. 5, speichert der Anbieter die Auftragsdaten dieser Leistung bis zum Ende des Vertrags weiter und schützt sie nach diesem Vertrag. Der Kunde kann sie bis dahin über die Exportfunktionen abrufen oder in Textform verlangen, dass der Anbieter sie vorher löscht; für Kopien in Datensicherungen gilt Abs. 5.

§ 15 Nachweise und Überprüfungen

(1) Der Anbieter stellt dem Kunden alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind (Art. 28 Abs. 3 Buchst. h DSGVO). Dazu gehören dieser Vertrag mit seinen Anlagen und Auskünfte in Textform auf Anfrage. Soweit vorhanden, legt er außerdem Prüfberichte und Zertifikate seiner Unterauftragsverarbeiter sowie Nachweise über genehmigte Verhaltensregeln oder Zertifizierungen nach Art. 40 und 42 DSGVO vor.

(2) Hält der Kunde diese Nachweise nicht für ausreichend oder besteht ein besonderer Anlass, etwa eine Verletzung des Schutzes von Auftragsdaten oder der begründete Verdacht eines Verstoßes gegen diesen Vertrag, ermöglicht der Anbieter Überprüfungen einschließlich Inspektionen durch den Kunden oder einen von ihm beauftragten Prüfer und trägt dazu bei. Der Prüfer muss unabhängig und zur Verschwiegenheit verpflichtet sein und darf nicht im Wettbewerb mit dem Anbieter stehen; unterliegt er keiner gesetzlichen Verschwiegenheitspflicht, verpflichtet er sich vor der Prüfung gegenüber dem Anbieter in Textform. Ohne besonderen Anlass findet eine Inspektion höchstens einmal im Kalenderjahr statt; Inspektionen für einen anderen Verantwortlichen nach § 1 Abs. 5 zählen mit.

(3) Eine Inspektion kündigt der Kunde mindestens 30 Kalendertage vorher in Textform an, bei einem besonderen Anlass mit einer angemessen kürzeren Frist. Sie findet montags bis freitags, außer an gesetzlichen Feiertagen am Sitz des Anbieters, von 8 bis 18 Uhr und ohne vermeidbare Störung des Betriebs statt, vor Ort in den Räumen, in denen der Anbieter Auftragsdaten verarbeitet, oder nach Wahl des Kunden aus der Ferne. Einsicht in Daten anderer Kunden und in Geschäftsgeheimnisse, die für die Prüfung nicht erforderlich sind, muss der Anbieter nicht gewähren; Sicherheitsvorkehrungen legt er so offen, dass ihre Wirksamkeit nicht gefährdet wird. Das Ergebnis teilt der Kunde dem Anbieter in Textform mit.

(4) Für Räume und Systeme eines Unterauftragsverarbeiters legt der Anbieter zunächst dessen Nachweise vor. Hält der Kunde sie nicht für ausreichend, übt der Anbieter auf sein Verlangen die Prüfrechte aus, die er nach § 11 Abs. 6 mit dem Unterauftragsverarbeiter vereinbart hat, oder ermöglicht dem Kunden, sie selbst auszuüben. Das Ergebnis teilt er dem Kunden mit.

(5) Kunde und Prüfer tragen ihre eigenen Kosten. Abweichend von § 12 Abs. 4 Satz 1 vergütet der Kunde dem Anbieter den Aufwand für Inspektionen; § 12 Abs. 5 Satz 1 und 2 gilt entsprechend. Keine Vergütung schuldet er für Inspektionen wegen einer Verletzung des Schutzes von Auftragsdaten im Verantwortungsbereich des Anbieters, auf Verlangen einer Aufsichtsbehörde und wenn die Inspektion einen erheblichen Verstoß des Anbieters gegen diesen Vertrag oder gegen Datenschutzvorschriften ergibt. Verlangt ein Unterauftragsverarbeiter für eine Prüfung nach Abs. 4 ein Entgelt, trägt der Kunde es nur, soweit der Anbieter es ihm vor der Prüfung in Textform genannt hat und ohne Aufschlag weiterreicht; Satz 3 gilt entsprechend.

(6) Die Befugnisse der Aufsichtsbehörden bleiben unberührt. Prüft eine Aufsichtsbehörde den Kunden, unterstützt der Anbieter ihn dabei; § 12 Abs. 4 gilt. Prüft sie den Anbieter zu Auftragsdaten des Kunden, informiert er den Kunden unverzüglich, soweit das zulässig ist.

§ 16 Haftung

(1) Für Ansprüche des Kunden gegen den Anbieter auf Schadensersatz oder auf Ersatz vergeblicher Aufwendungen aus diesem Vertrag oder im Zusammenhang mit der Verarbeitung der Auftragsdaten gilt, gleich aus welchem Rechtsgrund, § 11 der Allgemeinen Geschäftsbedingungen. Das gilt auch, soweit der Anbieter nach § 11 Abs. 6 dieses Vertrags für einen Unterauftragsverarbeiter einsteht; er haftet dann in demselben Umfang wie für eigenes Handeln. Diese Ansprüche und Ansprüche aus dem Vertrag unterliegen den Höchstbeträgen nach § 11 der Allgemeinen Geschäftsbedingungen gemeinsam. § 2 der Allgemeinen Geschäftsbedingungen bleibt für einen unentgeltlichen Testzugang unberührt.

(2) Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt. Die Beschränkungen der Haftung und der Verjährung nach § 11 der Allgemeinen Geschäftsbedingungen gelten weder für diese Haftung noch für den Ausgleich zwischen Kunde und Anbieter nach Art. 82 Abs. 5 DSGVO. Ansprüche des Anbieters gegen den Kunden nach den Allgemeinen Geschäftsbedingungen, auch auf Freistellung, bleiben unberührt.

§ 17 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform, soweit sie nicht nach § 13 der Allgemeinen Geschäftsbedingungen wirksam werden; für ihre Mitteilung gilt dann allein § 13 der Allgemeinen Geschäftsbedingungen. Die Anlagen ändert der Anbieter allein nach § 10 Abs. 2 und 3 und nach § 11 dieses Vertrags; einer Annahme durch den Kunden bedarf es dafür nicht, auch wenn der Anbieter die Änderung als neue Fassung dieses Vertrags veröffentlicht. Eine Änderung, die das Schutzniveau der Anlage 1 senkt, wird nur durch Vereinbarung in Textform wirksam.

(2) Eine neue Fassung dieses Vertrags gilt, sobald der Kunde sie annimmt oder sie nach § 13 der Allgemeinen Geschäftsbedingungen oder nach Abs. 1 Satz 2 wirksam wird; sie ersetzt dann für die Zukunft alle früheren Fassungen zwischen Kunde und Anbieter. Geht der Vertrag nach den Allgemeinen Geschäftsbedingungen auf ein anderes Unternehmen über, tritt dieses zugleich in diesen Vertrag ein.

(3) Es gilt das Recht der Bundesrepublik Deutschland; die Vorschriften der DSGVO bleiben unberührt. Der Gerichtsstand richtet sich nach den Allgemeinen Geschäftsbedingungen.

(4) Ist eine Bestimmung dieses Vertrags nicht Vertragsbestandteil geworden oder unwirksam, richtet sich sein Inhalt insoweit nach den gesetzlichen Vorschriften; der übrige Vertrag bleibt wirksam. Fehlt eine Regelung, die Art. 28 Abs. 3 DSGVO verlangt, gilt sie mit dem dort bestimmten Inhalt als vereinbart.

(5) Dieser Vertrag liegt auch in englischer Sprache vor; die englische Fassung dient nur der Information. Maßgeblich ist die deutsche Fassung.

Stand dieser Fassung: 03.11.2026

Vertrag zur Auftragsverarbeitung

Anlage zu den Allgemeinen Geschäftsbedingungen für die Plattform Zentrana

Stand **03.11.2026** Auftragsverarbeiter **Tom Gewiese**

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

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 Buchst. a DSGVO)

T1 Die Plattform wird über verschlüsselte Verbindungen (HTTPS) bereitgestellt; der Browser wird angewiesen, ein Jahr lang nur verschlüsselt zu verbinden (HSTS).

T2 Kennwörter speichert die Plattform nur als Hashwert mit Argon2id; ältere Hashwerte stellt sie bei der nächsten Anmeldung um. Sitzungskennungen, Wiederherstellungscodes und Kennungen vertrauenswürdiger Geräte liegen nur als Hashwert vor; Signaturgeheimnisse für Webhooks speichert sie nicht, sondern leitet sie aus einem Schlüssel außerhalb der Datenbank ab.

T3 Geheimnisse, die die Plattform lesbar benötigt, etwa für den zweiten Anmeldefaktor und für Zugänge zu angebundenen Diensten, speichert sie verschlüsselt (AES-256-GCM); der Schlüssel liegt außerhalb der Datenbank.

T4 Wo die Plattform ein Merkmal nur wiedererkennen muss, speichert sie statt des Werts einen Prüfwert mit geheimem Schlüssel (HMAC), etwa bei Netzadressen in Zählungen und bei Tankkartennummern; Tankkartennummern zeigt sie nur gekürzt an.

T5 Die Personendaten einer ausgeschiedenen Person macht der Anbieter mit einer Funktion der Plattform unkenntlich, sobald die Frist abläuft, die der Kunde in den Einstellungen wählt: zwei bis zehn Jahre ab dem Ende des Jahres, in dem die Person ausgeschieden ist, ohne Wahl drei Jahre. Eine längere Frist, die der Kunde für Schlüssel, Projekte oder Nachweise im Fuhrpark wählt, geht vor. Einträge im Änderungsprotokoll, auch solche mit der Art einer Abwesenheit, bleiben bis zur Löschung nach § 14 erhalten.

Vertraulichkeit: Anmeldung und Sitzungen

T6 Kennwörter müssen 12 bis 128 Zeichen lang sein, eine Ziffer und ein Sonderzeichen enthalten und dürfen nicht auf einer Sperrliste stehen. Einladungen und einmalige Kennwörter verfallen nach 24 Stunden.

T7 Jeder Nutzer kann einen zweiten Anmeldefaktor einrichten, per App (TOTP) oder per Code an seine E-Mail Adresse, der zehn Minuten gilt. Nach fünf falschen Codes bricht die Anmeldung ab. Nach der Anmeldung mit dem E-Mail-Code gilt ein Gerät höchstens 90 Tage als vertrauenswürdig; diese Freigabe lässt sich widerrufen.

T8 Anmeldecookies sind für Skripte nicht lesbar, werden nur über verschlüsselte Verbindungen übertragen und bei Anfragen, die von fremden Seiten ausgehen, nur beim direkten Aufruf einer Seite mitgesendet (SameSite=Lax). Sitzungen enden spätestens 12 Stunden nach der letzten Aktivität, mit „angemeldet bleiben“ spätestens 30 Tage danach. Abmelden beendet die Sitzung auf dem Server; trägt der Kunde einen Austritt ein oder sperrt er ein Konto, endet auch eine laufende Sitzung.

T9 Nach fünf Fehlversuchen je E-Mail Adresse und Netzadresse sperrt die Plattform die Anmeldung zeitweise, mit wachsender Wartezeit bis 15 Minuten, und vermerkt das im Protokoll des Kunden.

T10 Nach dem Austrittsdatum, das der Kunde einträgt, ist mit dem Zugang der Person keine Anmeldung mehr möglich.

T11 Sitzungen der Mitarbeitenden des Anbieters enden nach 60 Minuten ohne Aktivität und spätestens 8 Stunden nach der Anmeldung. Nach zehn Fehlversuchen wird der Zugang gesperrt und lässt sich nur über einen anderen Zugang des Anbieters entsperren; sicherheitsrelevante Einstellungen verlangen eine erneute Anmeldung.

Vertraulichkeit: Berechtigungen, Trennung und Zugriffe des Anbieters

T12 Der Server prüft jede Anfrage gegen Anmeldung, Konto, Kunde und die Rechte der Person für die jeweilige Funktion. Rechte vergibt der Kunde je Modul über Rollen, mit einem Geltungsbereich für die eigene Person, Organisationseinheiten, Standorte oder die ganze Firma. Module, die der Kunde nicht gebucht hat, sind gesperrt.

T13 Die Daten der Kunden sind logisch getrennt: Der Kunde einer Anfrage ergibt sich aus der Anmeldung, nicht aus der Anfrage, und Dateien liegen je Kunde in einem eigenen Ordner. Hochgeladene und erzeugte Dateien liegen außerhalb des öffentlichen Webverzeichnisses; ein direkter Abruf über das Web ist gesperrt.

T14 Lesend greifen Mitarbeitende des Anbieters auf Daten eines Kunden über die Supportansicht zu. Außerhalb von ihr zeigt der Bereich des Anbieters die Nutzerkonten des Kunden mit Name, E-Mail Adresse, Rollen, Status, Stand des Kennworts und der Angabe, ob ein zweiter Anmeldefaktor eingerichtet ist, bei den Zugängen nach § 1 Abs. 1 Satz 4 auch mit der letzten Anmeldung, Empfänger, Zeitpunkt und Zustellstand der E-Mails, die die Plattform im Auftrag des Kunden versendet, ohne Betreff und Inhalt, gesperrte Empfängeradressen nach § 3 Abs. 5 sowie Einträge im Protokoll des Kunden, die auf Vorgänge des Anbieters, des Systems oder von Automationen zurückgehen. Mitarbeitende des Anbieters mit dem Recht dazu können für einen Kunden Zugänge mit Verwaltungsrechten anlegen sowie Zugänge seiner Nutzer sperren, entsperren und löschen, ihr Kennwort zurücksetzen und eine Einladung erneut senden; diese Wege nutzen sie nur zur Einrichtung, auf Weisung nach § 7 Abs. 3 oder, für den eigenen Zugang, auf Anfrage der Person selbst. Legt ein Mitarbeitender des Anbieters einen Zugang an oder sendet er eine Einladung erneut, sendet die Plattform der Person einen Link an ihre E-Mail Adresse, über den sie innerhalb von 24 Stunden ein eigenes Kennwort festlegt; löst er das Zurücksetzen eines Kennworts aus, sendet sie ihr einen Link, der 60 Minuten gilt. Kennwörter der Zugänge des Kunden zeigt die Plattform den Mitarbeitenden des Anbieters nicht an. Jede solche Änderung wird protokolliert. Öffnen kann die Supportansicht nur, wer als Mitarbeitender des Anbieters das Recht dazu hat; sie erlaubt nur Lesen, endet nach 30 Minuten, verlangt Grund un…

T15 Rechte für Mitarbeitende des Anbieters werden über Rollen und einzelne Rechte vergeben. Vergeben darf sie nur, wer selbst Rechte verwalten darf, und nur Rechte, die er selbst besitzt; jede Vergabe und jeder Entzug wird protokolliert.

T16 Den Gesamtexport aller Daten einer Firma kann nur auslösen, wer beim Kunden das Recht dazu hat; der Link zum Herunterladen gilt 15 Minuten.

Integrität

T17 Änderungen werden je Kunde mit Zeitpunkt, handelnder Person, Kennung einer Supportsitzung, vorherigem und neuem Stand, Grund, Netzadresse und Browserkennung protokolliert; Geheimnisse und Kontonummern werden dabei unkenntlich gemacht. Regeln der Datenbank verhindern, dass einzelne Einträge geändert oder gelöscht werden. Das Protokoll wird erst mit der Löschung nach § 14 entfernt.

T18 Schlüsselquittungen und Schlüsselbewegungen, Fahrzeugübergaben, Projektkosten sowie Fassungen und Annahmen der Rechtstexte sind nach dem Abschluss durch Regeln der Datenbank unveränderlich; eine abgeschlossene Führerscheinkontrolle lässt sich in der Plattform nicht mehr ändern, sondern nur durch einen neuen Eintrag berichtigen. Gespeicherte Dateien tragen eine Prüfsumme (SHA-256).

T19 Datenbankzugriffe laufen über vorbereitete Anweisungen, und Ausgaben werden für die Anzeige kodiert. Seiten der Plattform tragen Sicherheitskopfzeilen gegen das Einbetten in fremde Seiten und gegen falsch erkannte Inhaltstypen, Downloads und Dateivorschauen werden mit gesperrten aktiven Inhalten ausgeliefert, und die Verwaltungszugänge des Anbieters schränken zusätzlich ein, welche Inhalte geladen werden (Content Security Policy).

T20 Webhooks sendet die Plattform nur über HTTPS und nicht an private Netzadressen; jede Nachricht ist mit einem Geheimnis signiert (HMAC-SHA256).

Datensparsamkeit und besondere Kategorien

T21 Besondere Kategorien (Art. 9 DSGVO): Die Begründung einer Abwesenheit der Art Krankheit sieht nur die betroffene Person selbst; Genehmigende und Teamansichten sehen sie nicht, der Export der Zeiterfassung enthält sie nicht, und das Änderungsprotokoll speichert sie nicht. Die Art einer Abwesenheit sehen nur Personen mit dem Recht dafür, in Teamansichten und im Protokoll; alle anderen sehen nur „Abwesend“. Nachweise über eine Arbeitsunfähigkeit speichert die Plattform nicht als Datei, sondern nur, ob sie offen, eingereicht oder anerkannt sind. Der Gesamtexport an den Kunden enthält alle diese Angaben. Ein Feld für Diagnosen gibt es nicht.

T22 Ansichten der Projekte, die Auslastung oder Kosten einzelner Personen zeigen, zeigt die Plattform nur verdichtet oder ohne Namen, bis der Kunde bestätigt, dass die Mitbestimmung gewahrt und eine Rechtsgrundlage vorhanden ist; diese Freigabe kann er zurücknehmen und jede dieser Funktionen abschalten. Auswertungen der Arbeitszeit, der Projektzeiten und der Kapazität über Gruppen zeigt die Plattform erst ab einer Mindestgröße von drei Personen, in der Voreinstellung ab fünf.

T23 Die Standortprüfung ist ausgeschaltet, bis der Kunde sie aktiviert, und wirkt für eine Person erst, wenn sie informiert wurde oder eingewilligt hat. Die Position des Geräts dient nur der Prüfung; gespeichert werden das Ergebnis, die auf 50 Meter gerundete Entfernung und die auf 10 Meter gerundete Genauigkeit, keine Koordinaten der Beschäftigten. Die Einträge löscht der Anbieter nach der vom Kunden gewählten Frist von 7 bis 90 Tagen.

T24 Fahrzeuge werden nicht geortet; das Fahrtenbuch erfasst Orte nur als Eingabe. Führerscheindaten und Führerscheinkontrollen sehen nur Personen mit den Rechten dafür.

Verfügbarkeit, Belastbarkeit, Wiederherstellung

T25 Für die Plattform stellt der Hoster nach Anlage 2 Server, Speicher, Stromversorgung, Netzanbindung und den physischen Schutz des Rechenzentrums; seine Nachweise legt der Anbieter nach § 15 Abs. 4 vor.

T26 Fehler der Anwendung erfasst die Plattform und fasst gleiche Fehler zusammen.

Löschung und Verfahren bei Verletzungen

T27 Nach dem Vertragsende überwacht der Anbieter mit der Plattform die Frist für den Abruf und erinnert an sie; danach löscht er die Daten des Kunden mit dem Löschlauf der Plattform, der sie aus den Modulen und Grundfunktionen samt Dateien, Exporten und den Kopien der E-Mails entfernt, die die Plattform im Auftrag des Kunden versendet hat.

T28 Verletzungen des Schutzes personenbezogener Daten erfasst der Anbieter in einem Register mit dem Zeitpunkt der Kenntnis, der Meldefrist, dem Risiko, den Kategorien und der ungefähren Zahl der Betroffenen und Datensätze, den Folgen und den Maßnahmen sowie den betroffenen Kunden mit dem Tag ihrer Benachrichtigung. Die Unterlagen bewahrt er drei Jahre ab dem Abschluss auf.

Verfahren zur regelmäßigen Überprüfung

T29 Automatisierte Prüfstände prüfen Rechte, Sichtbarkeit und Trennung der Kunden; der Anbieter führt sie bei Änderungen an diesen Bereichen aus. Das Protokoll der Zugänge des Anbieters ist als Kette von Prüfwerten versiegelt, deren Prüfung bei einem Bruch Alarm auslöst.

Anlage 2: Unterauftragsverarbeiter

Name	OVH GmbH
Anschrift	Oskar-Jäger-Straße 173/K6, 50825 Köln
Leistung	Hosting: Server, Speicher und Netzanbindung der Plattform
Ort der Verarbeitung	Rechenzentrum in Deutschland
Daten	alle Auftragsdaten, auch Gesundheitsdaten und andere Daten besonderer Kategorien
Übermittlung in Drittländer	Nach der Liste der weiteren Auftragsverarbeiter des Hosters sind Fernzugriffe von Gesellschaften seiner Unternehmensgruppe aus Kanada und dem Vereinigten Königreich möglich. Für das Vereinigte Königreich besteht ein Angemessenheitsbeschluss der Europäischen Kommission, für Kanada einer für Empfänger, die dem kanadischen Bundesgesetz über den Datenschutz in der Privatwirtschaft (PIPEDA) unterliegen.

Die weiteren Auftragsverarbeiter des Hosters (§ 11 Abs. 7) stehen in dessen Liste unter https://contract.eu.ovhapis.com/1.0/pdf/OVH_Sub_processors-de.pdf; Änderungen dieser Liste teilt der Anbieter nach § 11 Abs. 7 mit.