Auftragsbearbeitungsvertrag

Zum Vertrag über die Nutzung von CrewDeck, gemäss Art. 9 des Bundesgesetzes über den Datenschutz (DSG) und Art. 28 der Verordnung (EU) 2016/679 (DSGVO)

Digital Airways GmbH · Mailand-Strasse 32 · CH-4053 Basel

Fassung 10-2026 · Stand 20. Oktober 2026

1. Allgemeine Regelungen

1.1 Einleitung, Geltungsbereich, Begriffe

1.1.1 Dieser Vertrag regelt die Rechte und Pflichten des Kunden («Verantwortlicher») und der Digital Airways GmbH, Mailand-Strasse 32, CH-4053 Basel («Auftragsbearbeiterin») bei der Bearbeitung von Personendaten im Auftrag des Verantwortlichen im Zusammenhang mit der Software CrewDeck und den damit verbundenen Leistungen. Er ist darauf ausgelegt, die Anforderungen von Art. 9 DSG und von Art. 28 DSGVO zu erfüllen.

1.1.2 Dieser Vertrag ist integraler Bestandteil des Vertrags über die Nutzung von CrewDeck (Allgemeine Geschäftsbedingungen und Bestellung, zusammen «Hauptvertrag») und konkretisiert Abschnitt 7 der Allgemeinen Geschäftsbedingungen (AGB). Er kommt mit dem Abschluss des Hauptvertrags zustande und bedarf keiner gesonderten Unterzeichnung. Verantwortlicher ist die Vertragspartei der Auftragsbearbeiterin im Hauptvertrag.

1.1.3 Bei Widersprüchen zwischen diesem Vertrag und den AGB geht dieser Vertrag in Fragen des Datenschutzes vor.

1.1.4 Soweit in diesem Vertrag nicht anders definiert, haben die Begriffe die Bedeutung, die ihnen der Hauptvertrag, das DSG oder die DSGVO geben.

1.1.5 Der Verantwortliche stimmt diesem Vertrag für sich und für alle verbundenen Unternehmen zu, deren Personendaten er in CrewDeck bearbeiten lässt. Er stellt sicher, dass er dazu berechtigt ist.

1.2 Umfang der Bearbeitung, Datenkategorien, betroffene Personen

1.2.1 Der Umfang der Bearbeitung liegt im Ermessen des Verantwortlichen und hängt davon ab, wie er CrewDeck nutzt (gebuchtes Paket, aktivierte Module). Die möglichen Datenkategorien und betroffenen Personen sind in den Ziffern 1.2.2 und 1.2.3 aufgeführt.

1.2.2 Datenkategorien können sein:

- Stammdaten der Mitarbeitenden, zum Beispiel Name, Adresse, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Nationalität, Zivilstand und Bankverbindung
- Vertrags- und Dossierdaten, zum Beispiel Arbeitsverträge, Zeugnisse und weitere Dokumente
- Zeit- und Abwesenheitsdaten, zum Beispiel Arbeitszeiten, Ferien und Absenzen, auch wegen Krankheit oder Unfall (besonders schützenswerte Personendaten)
- Lohn- und Spesendaten, zum Beispiel Löhne, Vergütungen, Spesen und Belege
- Leistungs- und Entwicklungsdaten, zum Beispiel Beurteilungen, Kompetenzen und Schulungen
- Bewerbungsdaten, zum Beispiel Lebensläufe, Unterlagen und Nachrichten an Bewerbende
- Konto- und Nutzungsdaten, zum Beispiel Anmeldedaten und Änderungsprotokolle

1.2.3 Kategorien betroffener Personen können sein: Mitarbeitende, ehemalige Mitarbeitende, Bewerbende sowie die von Mitarbeitenden angegebenen Notfallkontakte.

1.2.4 Die Bearbeitung findet in der Schweiz statt (Azure Switzerland North). Eine Bearbeitung ausserhalb der Schweiz erfolgt ausschliesslich durch die KI-Funktionen in der EU-Datenzone von Microsoft, und nur, wenn eine Person des Verantwortlichen eine solche Funktion auslöst. Vor der Übermittlung werden Lebensläufe um Name, Adresse, Geburtsdatum, Telefonnummer, E-Mail-Adresse und weitere direkte Merkmale bereinigt. Nach den Bedingungen von Microsoft werden die übermittelten Inhalte nicht zum Training von Modellen verwendet.

1.2.5 Die Europäische Union steht auf der Liste des Bundesrats der Staaten mit angemessenem Datenschutz (Anhang 1 der Datenschutzverordnung). Eine Bekanntgabe in ein anderes Land ohne angemessenen Datenschutz erfolgt nur mit den nach dem DSG erforderlichen Garantien und nach vorgängiger Information des Verantwortlichen.

1.2.6 Die Auftragsbearbeiterin bearbeitet die Personendaten für die Dauer des Hauptvertrags und, soweit Ziffer 10 es vorsieht, danach bis zur Rückgabe und Löschung.

1.3 Verwiesene Dokumente

1.3.1 Dieser Vertrag verweist auf die folgenden Dokumente der Auftragsbearbeiterin. Sie sind unter den genannten Adressen abrufbar:

- Allgemeine Geschäftsbedingungen (AGB): https://crewdeck.ch/agb
- Datenschutzerklärung: https://crewdeck.ch/datenschutz

2. Vertraulichkeit

2.1 Die Auftragsbearbeiterin verpflichtet alle Personen, die Zugang zu den Personendaten haben, vertraglich oder gesetzlich zur Vertraulichkeit. Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.

2.2 Beide Parteien behandeln Geschäftsgeheimnisse und Informationen über Datensicherheitsmassnahmen der anderen Partei, die sie im Rahmen dieses Vertrags erfahren, vertraulich.

3. Pflichten des Verantwortlichen

3.1 Der Verantwortliche ist für die Einhaltung des DSG und der DSGVO bei der Nutzung von CrewDeck selbst verantwortlich, insbesondere für die Rechtmässigkeit der Bearbeitung und für die Information der betroffenen Personen.

3.2 Der Verantwortliche informiert die Auftragsbearbeiterin unverzüglich und vollständig, wenn er Fehler oder Unregelmässigkeiten bei der Bearbeitung im Hinblick auf den Datenschutz feststellt.

3.3 Der Verantwortliche nennt der Auftragsbearbeiterin auf Verlangen eine Ansprechperson für Datenschutzfragen.

4. Weisungen

4.1 Die Auftragsbearbeiterin bearbeitet Personendaten nur auf dokumentierte Weisung des Verantwortlichen, soweit diese im Leistungsumfang von CrewDeck liegt, oder soweit das Gesetz sie dazu verpflichtet.

4.2 Weisungsberechtigt sind die Personen, die der Verantwortliche in CrewDeck mit Administratorrechten ausgestattet hat, sowie die vertretungsberechtigten Personen des Verantwortlichen. Weisungen erfolgen über die Anwendung oder in Schriftform, E-Mail genügt.

4.3 Hält die Auftragsbearbeiterin eine Weisung für rechtswidrig, informiert sie den Verantwortlichen unverzüglich. Sie darf die Ausführung bis zur Klärung aussetzen.

5. Pflichten der Auftragsbearbeiterin

5.1 Allgemeine Pflichten

5.1.1 Ansprechstelle der Auftragsbearbeiterin für Datenschutzfragen ist info@digital-airways.ch.

5.1.2 Die Auftragsbearbeiterin unterstützt den Verantwortlichen bei Datenschutz-Folgenabschätzungen und bei der Konsultation des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), soweit ihre Bearbeitung betroffen ist.

5.1.3 Die Auftragsbearbeiterin informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Massnahmen einer Aufsichtsbehörde, soweit sie diesen Vertrag betreffen, es sei denn, das Gesetz oder die Behörde untersagt die Information.

5.1.4 Die Auftragsbearbeiterin gibt Behörden Personendaten nur heraus, wenn sie rechtlich dazu verpflichtet ist. Sie informiert den Verantwortlichen darüber, soweit ihr das erlaubt ist.

5.2 Kontrolle

5.2.1 Die Auftragsbearbeiterin erteilt dem Verantwortlichen auf schriftliche Anfrage die Auskünfte und Nachweise, die zur Überprüfung der Einhaltung dieses Vertrags erforderlich sind.

5.2.2 Die Auftragsbearbeiterin ist selbst nicht zertifiziert. Für die Azure-Rechenzentren weist Microsoft eigene Zertifizierungen aus (Microsoft Trust Center). Die Auftragsbearbeiterin stellt die öffentlich verfügbaren Nachweise von Microsoft bereit.

6. Technische und organisatorische Massnahmen

6.1 Die Auftragsbearbeiterin trifft angemessene technische und organisatorische Massnahmen, um die Datensicherheit nach Art. 8 DSG und Art. 32 DSGVO zu gewährleisten. Mindestens gelten die Massnahmen nach Ziffer 6.2.

6.2 Mindeststand der Massnahmen:

Mandantentrennung und Zugriff

- Trennung der Mandanten auf Datenbankebene (PostgreSQL Row-Level-Security), automatisiert getestet.
- Rollen- und Rechtesystem. Lohndaten sind nur für ausdrücklich berechtigte Rollen sichtbar. Mitarbeitende sehen ihre eigenen Daten, Vorgesetzte ihr Team.
- Beschränkung des Zugangs einer Person auf einzelne Gesellschaften des Verantwortlichen (in der Anwendung durchgesetzt).

Authentifizierung

- Passwörter werden nur als Hashwert gespeichert und haben mindestens zwölf Zeichen. Die E-Mail-Adresse wird bestätigt.
- Zwei-Faktor-Anmeldung verfügbar (Authenticator-App mit QR-Code, Backup-Codes).
- Sitzungen laufen nach 30 Minuten Inaktivität ab. Hinweis per E-Mail bei Anmeldung von einem unbekannten Gerät und bei Passwortänderung.

Verschlüsselung

- Übertragung ausschliesslich über HTTPS (HSTS, TLS 1.2 oder höher).

- Datenbank mit einem Schlüssel aus dem Azure Key Vault verschlüsselt, Dateien mit der Standardverschlüsselung von Azure.

Netz und Betrieb

- Datenbank in einem privaten Netz ohne öffentlichen Zugang. Dateispeicher ohne öffentlichen Zugang, Zugriff über kurzlebige, von der Anwendung signierte Anfragen.
- Sicherheitskopfzeilen, darunter HSTS und eine Content-Security-Policy.
- Produktion und Staging sind getrennte Umgebungen. Änderungen durchlaufen automatische Tests und werden zuerst auf Staging geprüft.

Nachvollziehbarkeit

- Revisionssicheres Änderungsprotokoll über alle Änderungen an Personaldaten, fortlaufend verkettet und nächtlich geprüft.
- Betriebsprotokolle werden in Azure geführt (in Produktion 90 Tage).

Verfügbarkeit und Wiederherstellung

- Die Datenbank ist in Produktion bis zu 35 Tage auf einen beliebigen Zeitpunkt wiederherstellbar, die Sicherungen bleiben in der Region. Gelöschte und überschriebene Dateien lassen sich 30 Tage wiederherstellen.

6.3 Die Massnahmen unterliegen dem technischen Fortschritt. Die Auftragsbearbeiterin darf sie weiterentwickeln, das Schutzniveau darf dabei nicht unter den Stand von Ziffer 6.2 sinken.

7. Unterauftragsbearbeiter

7.1 Die Auftragsbearbeiterin setzt die folgenden Unterauftragsbearbeiter ein. Die aktuelle Liste ist zudem in der Datenschutzerklärung der Auftragsbearbeiterin abrufbar (Abschnitt 6):

Unterauftragsbearbeiter	Zweck	Ort der Bearbeitung
Microsoft (Azure)	Betrieb, Datenbank, Dateiablage, Sicherungen	Schweiz (Switzerland North)
Microsoft (Azure Communication Services)	Versand von System-E-Mails	Schweiz
Microsoft (Azure OpenAI)	Ausschliesslich KI-Funktionen, nur auf Veranlassung des Verantwortlichen	EU (Datenzone Europäische Union)

7.2 Der Beizug von Unterauftragsbearbeitern ist nur mit Genehmigung des Verantwortlichen zulässig. Für die in Ziffer 7.1 aufgeführten Unterauftragsbearbeiter erteilt der Verantwortliche die Genehmigung mit diesem Vertrag.

7.3 Beabsichtigt die Auftragsbearbeiterin, einen Unterauftragsbearbeiter hinzuzuziehen oder zu ersetzen, informiert sie den Verantwortlichen mindestens 30 Tage im Voraus per E-Mail oder über die Anwendung. Der Verantwortliche kann der Änderung aus wichtigen datenschutzrechtlichen Gründen widersprechen. Im Fall eines Widerspruchs kann er den Hauptvertrag auf den Zeitpunkt des Wechsels kündigen (Sonderkündigungsrecht).

7.4 Die Auftragsbearbeiterin verpflichtet jeden Unterauftragsbearbeiter vertraglich zu mindestens gleichwertigen Datenschutzpflichten, wie sie in diesem Vertrag gelten, und haftet gegenüber dem Verantwortlichen für deren Einhaltung.

8. Rechte der betroffenen Personen

8.1 Wendet sich eine betroffene Person mit einem Begehren nach dem DSG oder dem Kapitel III der DSGVO an die Auftragsbearbeiterin, verweist diese die Person an den Verantwortlichen und leitet das Begehren weiter. Sie entscheidet nicht selbst darüber.

8.2 Mitarbeitende können ihre Daten in CrewDeck selbst als Datei exportieren. Die Auftragsbearbeiterin unterstützt den Verantwortlichen bei der Beantwortung von Begehren auf Auskunft, Berichtigung, Löschung und Herausgabe.

8.3 Die Auftragsbearbeiterin ist nicht verantwortlich, wenn der Verantwortliche ein Begehren einer betroffenen Person nicht, nicht richtig oder nicht rechtzeitig beantwortet.

9. Informations- und Mitteilungspflichten

9.1 Die Auftragsbearbeiterin meldet dem Verantwortlichen eine Verletzung der Datensicherheit, die dessen Personendaten betrifft, unverzüglich, spätestens 24 Stunden nach Kenntnisnahme.

9.2 Die Meldung enthält, soweit bekannt, die Art der Verletzung, die betroffenen Personendaten und Personen, die möglichen Folgen sowie die ergriffenen und vorgesehenen Massnahmen. Fehlende Angaben reicht die Auftragsbearbeiterin nach.

9.3 Die Meldung an den EDÖB und an betroffene Personen obliegt dem Verantwortlichen. Die Auftragsbearbeiterin unterstützt ihn dabei.

9.4 Sind Personendaten des Verantwortlichen durch Beschlagnahme, Insolvenz- oder Vergleichsverfahren oder andere Massnahmen Dritter gefährdet, informiert die Auftragsbearbeiterin den Verantwortlichen unverzüglich.

10. Herausgabe und Löschung von Daten

10.1 Der Verantwortliche kann seine Daten jederzeit selbst exportieren. Nach Vertragsende bleibt der Export während 30 Tagen möglich.

10.2 Nach Ablauf dieser Frist löscht die Auftragsbearbeiterin die Personendaten vollständig, einschliesslich der Sicherungskopien nach deren regulärem Umlauf (AGB, Abschnitt 10).

10.3 Auf schriftliche Weisung des Verantwortlichen löscht die Auftragsbearbeiterin früher, soweit keine gesetzliche Pflicht entgegensteht.

10.4 Gesetzliche Aufbewahrungspflichten bleiben vorbehalten. Die Auftragsbearbeiterin bestätigt die Löschung auf Anfrage schriftlich.

11. Haftung

11.1 Für die Haftung gelten die Bestimmungen der AGB (Abschnitt 9).

11.2 Beschränkungen und Ausschlüsse der Haftung gelten nicht, soweit das Gesetz sie nicht zulässt, insbesondere bei Vorsatz und grober Fahrlässigkeit.

12. Schlussbestimmungen

12.1 Die Auftragsbearbeiterin kann diesen Vertrag nach dem Verfahren von Abschnitt 11 der AGB ändern (Ankündigung mindestens 30 Tage im Voraus). Im Übrigen bedürfen Änderungen und Ergänzungen der Schriftform, E-Mail genügt.

12.2 Es gilt Schweizer Recht. Gerichtsstand ist Basel, wie in den AGB (Abschnitt 12) vereinbart.

12.3 Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleibt der übrige Vertrag gültig. Die unwirksame Bestimmung wird durch eine ersetzt, die dem wirtschaftlichen Zweck am nächsten kommt.