Auftragsbearbeitungsvertrag (AVV)

Integraler Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) der Citrus AG – zwischen der Citrus AG, Technoparkstrasse 1, 8005 Zürich, Schweiz («Auftragsbearbeiterin» bzw. «Citrus AG»), und dem Kunden («Verantwortlicher» bzw. «Kunde»).
Stand: November 2026

1. Gegenstand, Anwendungsbereich und Rollen

1.1 Anwendungsbereich. Dieser Auftragsbearbeitungsvertrag («AVV») regelt die Bearbeitung von Personendaten durch die Citrus AG im Auftrag des Kunden im Rahmen der Erbringung von IT- und Cloud-Dienstleistungen (z. B. Beratung, Implementierung, Migration, Administration, Integrationen, Erweiterungen, Automatisierungen und Support; «Dienstleistungen») gemäss dem jeweiligen Vertrag. Die Pflichten der Citrus AG aus diesem AVV beziehen sich ausschliesslich auf deren eigene Zugriffe und Bearbeitungen von Personendaten im Rahmen der Dienstleistungen.

1.2 Begriffe. Die in diesem AVV verwendeten datenschutzrechtlichen Begriffe richten sich nach dem Schweizer Bundesgesetz über den Datenschutz (DSG) sowie – soweit die Bearbeitung des Kunden im Einzelfall dieser untersteht – der EU-Datenschutz-Grundverordnung (DSGVO).

2. Angaben zur Datenbearbeitung

Gegenstand, Dauer, Art und Zweck der Bearbeitung sowie die Kategorien von Personendaten und betroffenen Personen sind in **Anhang 1** festgelegt.

3. Weisungen und Verantwortung des Kunden

3.1 Weisungsgebundenheit. Die Citrus AG bearbeitet Personendaten ausschliesslich nach dokumentierten Weisungen des Kunden – wozu der Vertrag, dieses AVV, Support-Tickets sowie vom Kunden in Auftrag gegebene Konfigurationen gehören –, sofern die Citrus AG nicht durch anwendbares Recht zu einer Bearbeitung verpflichtet ist. In einem solchen Fall informiert die Citrus AG den Kunden vor der Bearbeitung, sofern das Gesetz eine solche Mitteilung nicht verbietet.

3.2 Hinweispflicht. Die Citrus AG informiert den Kunden unverzüglich, falls sie der Auffassung ist, dass eine Weisung gegen anwendbares Datenschutzrecht verstösst.

3.3 Verantwortung des Kunden. Der Kunde ist allein verantwortlich für die Rechtmässigkeit der Datenbearbeitung, die Information der betroffenen Personen sowie dafür, dass keine gesetzlichen oder vertraglichen Geheimhaltungspflichten dem Beizug der Citrus AG entgegenstehen.

4. Vertraulichkeit

Die Citrus AG stellt sicher, dass alle zur Bearbeitung von Personendaten befugten Mitarbeitenden und Hilfspersonen einer angemessenen gesetzlichen oder vertraglichen Vertraulichkeitspflicht unterstehen.

5. Datensicherheit (TOMs)

Die Citrus AG trifft angemessene technische und organisatorische Massnahmen (TOMs) gemäss Art. 8 DSG und – soweit anwendbar – Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die grundlegenden TOMs sind in **Anhang 1** beschrieben; die Citrus AG darf diese laufend anpassen, solange das allgemeine Sicherheitsniveau nicht wesentlich herabgesetzt wird.

6. Unterauftragsbearbeiter

6.1 Allgemeine Genehmigung. Der Kunde erteilt der Citrus AG eine allgemeine vorgängige Genehmigung zum Beizug von Unterauftragsbearbeitern für Teile der Dienstleistungen, insbesondere in den Kategorien Cloud-Infrastruktur, E-Mail und Kollaboration, Datensicherung (Backup), Projekt- und Ticketverwaltung, Fernwartung, Passwortverwaltung, interne Anwendungs-Infrastruktur, kommerzielle KI-Unterstützung sowie projektbezogene externe Fachkräfte und Subunternehmer, mit Bearbeitungsorten in der Schweiz, der EU/dem EWR, den USA sowie weltweit (gemäss Ziff. 7). Die jeweils aktuelle namentliche Liste der regulär eingesetzten Unterauftragsbearbeiter (einschliesslich deren Bearbeitungsorten) wird dem Kunden jederzeit auf Anfrage per E-Mail an privacy@citrus.ch zur Verfügung gestellt. Kommen darüber hinaus projektbezogen externe Fachkräfte oder Subunternehmer im Rahmen eines Kundenmandats als Unterauftragsbearbeiter mit Kunden-Personendaten in Berührung, legt die Citrus AG diese dem betroffenen Kunden direkt im Projektkontext unter Angabe des Bearbeitungsortes offen.

6.2 Information und Widerspruch. Kunden, die vorab über Änderungen bei den Unterauftragsbearbeitern informiert werden möchten, können sich per E-Mail an privacy@citrus.ch für Änderungsmitteilungen registrieren. Die Citrus AG informiert registrierte Kunden mindestens **14 Tage** im Voraus per E-Mail über die Beiziehung neuer oder den Ersatz bestehender, für den Kunden eingesetzter Unterauftragsbearbeiter. Der Kunde kann innert dieser 14 Tage ausschliesslich aus wichtigen, dokumentierten datenschutzrechtlichen Gründen schriftlich Widerspruch erheben. Lässt sich der Widerspruch nicht einvernehmlich lösen, kann jede Partei die betroffenen Dienstleistungen mit angemessener Frist kündigen (vorbehältlich Ziff. 9 der AGB und ohne Auswirkungen auf Verträge mit fester Laufzeit, insbesondere über Drittprodukte).

6.3 Überbindung. Die Citrus AG überbindet ihren Unterauftragsbearbeitern datenschutzrechtliche Pflichten, die diesem AVV materiell gleichwertig sind, und haftet für deren Einhaltung im Rahmen dieses AVV (insbesondere Ziff. 12.1).

6.4 Abgrenzung zu Drittanbietern. Soweit der Kunde im Zusammenhang mit den Dienstleistungen Cloud-Plattformen, Software oder Dienste von Drittanbietern nutzt (z. B. Google Workspace, Google Cloud, Backup- oder Sicherheitslösungen), für welche direkte Vertragsbedingungen zwischen dem Kunden und dem jeweiligen Anbieter gelten, handelt dieser Anbieter gegenüber dem Kunden direkt (als eigener Auftragsbearbeiter oder Verantwortlicher) und nicht als Unterauftragsbearbeiter der Citrus AG.

7. Internationale Datenübermittlungen

7.1 Genehmigung von Auslandsübermittlungen. Der Kunde nimmt zur Kenntnis und genehmigt, dass

die Citrus AG und ihre genehmigten Unterauftragsbearbeiter Personendaten auch ausserhalb der Schweiz und des EU-/EWR-Raums – insbesondere in den **Vereinigten Staaten von Amerika** sowie in weiteren Drittstaaten – bearbeiten und dorthin übermitteln dürfen, wie in der jeweils aktuellen Liste der Unterauftragsbearbeiter (Ziff. 6.1) aufgeführt.

7.2 Datenschutzgarantien. Jede Übermittlung von Personendaten in einen Staat ohne angemessenes Datenschutzniveau gemäss Beschluss des Schweizer Bundesrats (und gegebenenfalls der Europäischen Kommission) erfolgt ausschliesslich unter Anwendung geeigneter Garantien gemäss Art. 16–17 DSG bzw. Kapitel V DSGVO, insbesondere durch:

- die Zertifizierung des Empfängers unter dem **Swiss-US Data Privacy Framework (DPF)** sowie – soweit anwendbar – dem **EU-US DPF**; oder
- die **EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914)** – insbesondere Modul 3 (Auftragsbearbeiter an Auftragsbearbeiter) – ergänzt um den **Schweizer Anhang (EDÖB-Addendum)** sowie allfällige erforderliche ergänzende technische und organisatorische Massnahmen.

7.3 Auffangmechanismus (Fallback). Sollte ein Angemessenheitsrahmen (wie das Swiss-US oder EU-US DPF) wegfallen, ausgesetzt werden oder einen Empfänger nicht abdecken, stützt sich die Citrus AG auf die EU-Standardvertragsklauseln (mit Schweizer EDÖB-Addendum) oder einen anderen gültigen Übermittlungsmechanismus. Soweit erforderlich, ermächtigt der Kunde die Citrus AG, solche Standardvertragsklauseln im Namen oder im Auftrag des Kunden mit Unterauftragsbearbeitern abzuschliessen.

8. Unterstützungspflichten

Unter Berücksichtigung der Art der Bearbeitung unterstützt die Citrus AG den Kunden in angemessenem Umfang bei der Erfüllung seiner gesetzlichen Pflichten betreffend:

- Gesuche betroffener Personen (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerspruch), soweit der Kunde diese nicht selbst erfüllen kann;
- Datensicherheitspflichten, Datenschutz-Folgenabschätzungen (DSFA) sowie vorgängige Konsultationen von Aufsichtsbehörden.

Soweit im jeweiligen Vertrag nichts anderes vereinbart ist, darf die Citrus AG den Aufwand für solche Unterstützungsleistungen zu ihren Standardstundensätzen (Ziff. 4.1 der AGB) verrechnen.

9. Verletzungen der Datensicherheit

Die Citrus AG meldet dem Kunden unverzüglich (so rasch als möglich), nachdem sie Kenntnis von einer Verletzung der Datensicherheit erlangt hat, welche die von der Citrus AG im Auftrag des Kunden bearbeiteten Personendaten betrifft, und stellt die verfügbaren Informationen bereit, die der Kunde zur Erfüllung seiner gesetzlichen Meldepflichten benötigt.

10. Löschung und Rückgabe von Daten

Nach Beendigung des jeweiligen Vertrags bzw. der Geschäftsbeziehung löscht oder retourniert die Citrus AG nach Wahl des Kunden die in dessen Auftrag gespeicherten Personendaten (wie etwa temporäre Migrationsdaten oder Arbeitskopien), sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Wünscht der Kunde eine Rückgabe, hat er dies der Citrus AG innert **30 Tagen** nach Vertragsende schriftlich mitzuteilen; allfälliger Rückgabe- oder Exportaufwand kann gemäss Ziff. 4.1 der AGB verrechnet werden. Erfolgt innert dieser Frist keine Rückmeldung, gilt dies als Weisung zur Löschung im Rahmen der regulären Prozesse der Citrus AG. Eigene Geschäfts-, Vertrags-, Abrechnungs- und Dokumentationsunterlagen der Citrus AG (bei denen sie als Verantwortliche handelt) bleiben hiervon unberührt. Sämtliche Löschpflichten – einschliesslich während der Vertragsdauer (Ziff. 8) – gelten mit der Massgabe, dass Kopien in automatisierten und verschlüsselten Datensicherungen (Backups) der Citrus AG gegen eine aktive Weiterbearbeitung geschützt und im Rahmen der regulären Aufbewahrungs- und Überschreibungszyklen gelöscht werden.

11. Auskunft und Audits

11.1 Nachweise. Auf schriftliche Anfrage stellt die Citrus AG dem Kunden die Informationen zur Verfügung, die vernünftigerweise erforderlich sind, um die Einhaltung dieses AVV nachzuweisen (z. B. Sicherheitsdokumentationen, Richtlinien oder Zertifizierungen Dritter).

11.2 Audits. Reichen die Nachweise gemäss Ziff. 11.1 zur Erfüllung gesetzlicher Prüfpflichten im Einzelfall nicht aus, kann der Kunde höchstens einmal pro Kalenderjahr mit einer schriftlichen Vorankündigung von mindestens **30 Tagen** eine Prüfung durchführen oder durch einen unabhängigen, zur Vertraulichkeit verpflichteten Prüfer (kein Wettbewerber der Citrus AG) durchführen lassen. Umfang, Zeitpunkt und Dauer sind vorgängig abzustimmen; Prüfungen erfolgen vorrangig dokumentenbasiert oder remote, während der üblichen Geschäftszeiten und ohne Beeinträchtigung des Geschäftsbetriebs. Zum Schutz anderer Kunden sowie von Geschäfts- und Sicherheitsgeheimnissen erfolgt die Prüfung ohne direkten Zugriff auf Systeme der Citrus AG (z. B. durch geführte Einsichtnahme oder bereinigte Auszüge). Der Kunde trägt die Kosten der Prüfung einschliesslich des angemessenen Begleitaufwands der Citrus AG (Ziff. 4.1 der AGB), ausser die Prüfung deckt eine wesentliche, von der Citrus AG zu vertretende Verletzung dieses AVV auf.

12. Haftung, Vorrang, Sprache und anwendbares Recht

12.1 Haftung. Die Haftung im Zusammenhang mit diesem AVV richtet sich ausschliesslich nach den Haftungsbeschränkungen in den AGB (insbesondere Ziff. 8 der AGB) bzw. im jeweiligen Vertrag.

12.2 Vorrang. Bei Widersprüchen zwischen diesem AVV und den AGB oder sonstigen Vertragsbestimmungen hinsichtlich der Bearbeitung von Personendaten geht dieses AVV vor (vorbehältlich Ziff. 12.1).

12.3 Massgebende Sprache. Bei Abweichungen zwischen der deutschen und einer fremdsprachigen Fassung ist ausschliesslich die deutsche Fassung massgebend.

12.4 Anwendbares Recht und Gerichtsstand. Dieses AVV untersteht ausschliesslich schweizerischem

materiellem Recht unter Ausschluss der Kollisionsnormen und des UN-Kaufrechts (CISG); ausschliesslicher Gerichtsstand ist **Zürich, Kanton Zürich (Schweiz)**.

Anhang 1 zum AVV: Angaben zur Bearbeitung und Basis-TOMs

A. Angaben zur Bearbeitung

Element	Spezifikation
Gegenstand und Zweck	Erbringung von IT- und Cloud-Beratung, Workspace- und Cloud-Implementierung, Datenmigration, System-, Benutzer- und Lizenzadministration (inkl. Onboarding/Offboarding und Verzeichnisbereinigung), kundenspezifischen Integrationen, Erweiterungen und Automatisierungen, Geräte-, Netzwerk- und Telefoniekonfiguration, Backup-Einrichtung, Log- und Sicherheitsanalysen, System- und Sicherheitsüberwachung (Monitoring) und technischem Support sowie Entgegennahme von System- und Sicherheitsmeldungen gemäss dem jeweiligen Vertrag.
Dauer	Für die Dauer des jeweiligen Vertrags sowie eine allfällige anschliessende Löschungs- oder Rückgabephase gemäss Ziff. 10.
Art der Bearbeitung	Temporärer Zugriff, Einsichtnahme, Export, Auswertung, Bereinigung, Konfiguration, Migration, Fehler-, Log- und Sicherheitsanalyse, Administration und Support-Bearbeitung in Systemen und Umgebungen des Kunden sowie die Speicherung und Bearbeitung projekt-, verwaltungs- und supportbezogener Kundendaten (einschliesslich temporärer Arbeitskopien, z. B. Benutzerlisten oder Log-Exporte) in internen Verwaltungs-, Automatisierungs- und Hilfsanwendungen der Citrus AG. Die Citrus AG stellt keine eigenen SaaS-Produktionsplattformen für Endkunden bereit.
Kategorien von Personendaten	Kontakt-, Organisations- und Kontodaten (Namen, geschäftliche sowie – z. B. beim Onboarding – private E-Mail-Adressen und Telefonnummern, Funktion, Abteilung, Ein- und Austrittsdaten, Benutzer-IDs, Rollen, Gruppen- und Lizenzzuordnungen, Konto- und Nutzungsstatus), technische Zugriffs-, Geräte- und Verbindungsdaten (insbesondere IP-Adressen, Gerätekennungen, Authentifizierungs-, Sicherheits-, Audit-, System-, Support- und E-Mail-Metadaten/Logs) sowie –

Element	Spezifikation
	akzessorisch im Rahmen von Migrationen, Fehlerbehebungen, Sicherheitsanalysen oder Administrationsaufgaben – sämtliche vom Kunden in seinen Cloud- oder IT-Umgebungen gespeicherten Personendaten.
Kategorien betroffener Personen	Mitarbeitende, Auftragnehmer und Administratoren des Kunden sowie – akzessorisch – Kunden, Lieferanten oder Kommunikationspartner des Kunden.

B. Grundlegende technische und organisatorische Massnahmen (TOMs)

- **Zugriffskontrolle und Nachvollziehbarkeit:** Individuelle Benutzerkonten (keine gemeinsamen Personenkonten) und rollenbasierte Zugriffsrechte nach dem Minimalprinzip (*Least Privilege*); verpflichtende Multi-Faktor-Authentifizierung (MFA) für sämtliche internen Systeme sowie – soweit technisch unterstützt – für Kunden-Adminkonsolen; unverzüglicher Entzug von Zugriffsrechten bei Rollenwechsel oder Austritt; Aktivierung der systemseitigen Audit- und Zugriffsprotokolle in den eingesetzten Cloud- und Backup-Plattformen.
- **Verschlüsselung und Übertragungssicherheit:** Verschlüsselte Datenübertragung (TLS 1.2+), Festplattenverschlüsselung auf Arbeitsgeräten sowie anbieterseitige Verschlüsselung gespeicherter Daten in den eingesetzten Cloud-Diensten; keine unverschlüsselte Ablage von Kundenzugangsdaten (Einsatz eines Enterprise-Passwortmanagers).
- **Physische und Endgerätesicherheit:** Zugangsgeschützte Büroräumlichkeiten (Zutrittskontrolle); angemessene Absicherung der für Kundenzugriffe eingesetzten Arbeitsgeräte (insbesondere Festplattenverschlüsselung, automatische Bildschirmsperre und zeitnahe Sicherheitsupdates).
- **Datentrennung und Datenminimierung:** Organisatorische und logische Trennung kundenbezogener Projekt- und Supportdaten in internen Ablagen und Arbeitskontexten (keine Vermischung von Daten verschiedener Kunden); administrativer Zugriff auf Kundenumgebungen und Kundendaten erfolgt strikt anlassbezogen (*Need-to-know*) für aktive Tickets, Projekte oder Migrationen; temporäre Migrations- und Arbeitskopien werden nach Abschluss zeitnah gelöscht.
- **Vorfalls- und Resilienzmanagement:** Verfahren zur Behandlung von Sicherheitsvorfällen, regelmässige anbieterseitig verschlüsselte Backups der internen Cloud-Umgebung sowie anlassbezogene und angemessene Überprüfung der Sicherheitsmassnahmen.