AUFTRAGSBEARBEITUNGSVERTRAG (AVV)

Bearbeitung von Personendaten

Dieser Vertrag regelt die Bearbeitung von Personendaten durch die iConference AG im Auftrag des Kunden beim Betrieb des Sovereign Cockpit, gemäss dem revidierten Schweizer Datenschutzgesetz (revDSG) und, soweit anwendbar, Art. 28 DSGVO.

Vorlage — rechtliche Prüfung erforderlich. Dies ist eine Arbeitsvorlage, die die technischen Gegebenheiten des Sovereign Cockpit abbildet. Vor der Unterzeichnung ist sie durch qualifizierte Rechtsberatung zu prüfen und mit den kundenspezifischen Angaben zu ergänzen, die *kursiv* markiert sind.

1. Parteien

VERANTWORTLICHER

Kunde

Firmenname
Adresse
Vertreten durch

AUFTRAGSBEARBEITER

iConference AG

Grafenaustrasse 15
6300 Zug · Schweiz
info@iconference.ch

2. Gegenstand und Dauer

Der Auftragsbearbeiter bearbeitet Personendaten ausschliesslich zur Erbringung des Sovereign Cockpit: Anonymisierung / Pseudonymisierung der vom Kunden hochgeladenen Dokumente, sichere Speicherung des Re-Identifikations-Mappings und Re-Identifikation auf Weisung des Kunden. Die Bearbeitung dauert für die Laufzeit des zugrunde liegenden Dienstleistungsvertrags und endet mit dessen Beendigung.

3. Art, Zweck und Kategorien

Art und Zweck der Bearbeitung sind das Erkennen und Maskieren von Personendaten in den Dokumenten des Kunden, sodass nur eine bereinigte Fassung den Einflussbereich des Kunden verlässt. Die **Kategorien der betroffenen Personen und der Personendaten** werden durch die vom Kunden hochgeladenen Dokumente bestimmt und in Anhang 1 festgehalten.

4. Weisungen

Der Auftragsbearbeiter bearbeitet Personendaten nur auf dokumentierte Weisung des Kunden, einschliesslich des Betriebs des Dienstes in der konfigurierten Form. Er informiert den Kunden, wenn eine Weisung nach seiner Auffassung gegen anwendbares Datenschutzrecht verstösst. Freigabe durch den Menschen: Daten verlassen das System nur durch eine ausdrückliche, im Audit-Protokoll erfasste Freigabe.

5. Vertraulichkeit

Der Auftragsbearbeiter stellt sicher, dass die zur Bearbeitung befugten Personen zur Vertraulichkeit verpflichtet und entsprechend geschult sind. Der Zugang zu einer Kunden-Instanz ist auf benannte, authentifizierte Benutzerkonten beschränkt.

Innerhalb des Teams des Kunden ist ein Vorgang nur für die Person zugänglich, die ihn angelegt hat, sowie für Administratoren, sodass der Kunde den Zugriff unter seinen eigenen Nutzern selbst steuert.

6. Sicherheit der Bearbeitung (technische & organisatorische Massnahmen)

Der Auftragsbearbeiter setzt angemessene technische und organisatorische Massnahmen um. Die für das Sovereign Cockpit geltenden Massnahmen sind in Anhang 2 aufgeführt. Sie umfassen insbesondere: Single-Tenant-Isolation (ein Container pro Kunde), At-rest-Verschlüsselung aller Vorgangs-Artefakte (AES-256-GCM; Master-Schlüssel getrennt vom Daten-Volume), auditierbare Löschung ganzer Vorgänge durch den Kunden, ein manipulationssicheres, HMAC-verkettetes Audit-Protokoll, eine erzwungene Egress-Prüfung vor jeder Freigabe, Transportverschlüsselung, authentifizierten Zugriff mit vorgangsbezogener Zuständigkeit und Härtung gegen Denial-of-Service.

7. Unterauftragsbearbeiter

Der Kunde genehmigt den Einsatz des in Anhang 3 aufgeführten Unterauftragsbearbeiters. Der Auftragsbearbeiter erlegt jedem Unterauftragsbearbeiter dieselben Datenschutzpflichten auf und informiert den Kunden über jede beabsichtigte Änderung, sodass dieser Einspruch erheben kann. Beim On-Premise-Betrieb gibt es keinen Unterauftragsbearbeiter; die Namenserkennung läuft dann lokal.

UNTERAUFTRAGSBEARBEITER	ZWECK	STANDORT
Infomaniak Network SA	KI-API zur Namens-/Entitätenerkennung (Freitext-NER) — nur beim gehosteten Betrieb	Schweiz

8. Datenstandort und Bekanntgabe ins Ausland

Die gesamte Bearbeitung erfolgt **in der Schweiz** — entweder beim Kunden vor Ort oder auf einer in der Schweiz gehosteten Single-Tenant-Instanz, die vom Auftragsbearbeiter betrieben wird. Im ausgelieferten Dienst erfolgt **keine Bekanntgabe von Personendaten ins Ausland** und keine Einbindung von Anbietern ausserhalb der Schweiz.

9. Unterstützung des Verantwortlichen

Der Auftragsbearbeiter unterstützt den Kunden unter Berücksichtigung der Art der Bearbeitung bei der Beantwortung von Anfragen betroffener Personen sowie bei der Erfüllung der Pflichten des Kunden hinsichtlich Sicherheit, Meldung von Verletzungen und, soweit anwendbar, Datenschutz-Folgenabschätzungen.

10. Verletzung des Datenschutzes

Der Auftragsbearbeiter benachrichtigt den Kunden unverzüglich, nachdem ihm eine Verletzung des Datenschutzes bekannt geworden ist, die die Daten des Kunden betrifft, und stellt die Informationen bereit, die der Kunde zur Erfüllung seiner eigenen Meldepflichten benötigt.

11. Löschung und Rückgabe

Bei Beendigung löscht der Auftragsbearbeiter die Personendaten oder gibt sie nach Wahl des Kunden zurück, sofern keine gesetzliche Aufbewahrungspflicht besteht. Sämtliche Vorgangs-Artefakte sind at-rest verschlüsselt und werden bei Beendigung zusammen mit der übrigen Akte gelöscht.

12. Überprüfungen

Der Auftragsbearbeiter stellt die zum Nachweis der Einhaltung dieses Vertrags erforderlichen Informationen bereit und ermöglicht Überprüfungen einschliesslich Inspektionen durch den Kunden oder einen von ihm beauftragten Prüfer und trägt dazu bei, unter Wahrung angemessener Ankündigung und Vertraulichkeit.

13. Anwendbares Recht und Sprachfassung

Dieser Vertrag untersteht Schweizer Recht. Gerichtsstand ist *Zug, Schweiz*, soweit zwingendes Recht nichts anderes vorsieht.

Diese deutsche Fassung und die englische Fassung sind inhaltsgleich. Im Vertrag ist *eine Sprachfassung als massgeblich* zu bezeichnen.

ANHÄNGE

ANHANG	INHALT
Anhang 1	Kategorien betroffener Personen und Personendaten — vom Kunden pro Vertrag auszufüllen (bestimmt durch die vom Kunden hochgeladenen Dokumente)
Anhang 2	Technische und organisatorische Massnahmen — siehe unten
Anhang 3	Genehmigte Unterauftragsbearbeiter (siehe Ziffer 7)

ANHANG 2

Technische & organisatorische Massnahmen

Die nachstehenden Massnahmen gelten für das Sovereign Cockpit im Auslieferungszustand. Sie setzen die Sicherheitspflichten aus Ziffer 6 um.

BEREICH	MASSNAHME
Datenstandort	Gesamte Bearbeitung in der Schweiz — On-Premise oder auf einer in der Schweiz gehosteten Single-Tenant-Instanz. Keine Bekanntgabe von Personendaten ins Ausland.
Mandantentrennung	Eine isolierte Container-Instanz pro Kunde, mit eigenem Schlüssel und eigenem Audit-Protokoll. Kein geteilter Speicher zwischen Kunden.
Verschlüsselung (ruhend)	Alle Vorgangs-Artefakte (Original, anonymisierte und re-identifizierte Fassung, Quelldatei, Mapping, Metadaten, Benutzerliste, Standardbegriffe) sind mit AES-256-GCM verschlüsselt und verbleiben ausschliesslich in der Kundeninstanz. Der Master-Schlüssel liegt getrennt vom Daten-Volume und den Backups, je Instanz eigen. Das Audit-Protokoll enthält keine Dokument-Inhalte, jedoch Benutzernamen und Vorgangs-Metadaten im Klartext. Vorgänge werden bis zur Löschung durch den Kunden aufbewahrt; die Löschung wird in der Audit-Kette protokolliert. *Master-Schlüssel: hosted führt der Auftragsbearbeiter den Escrow, on-premise der Kunde (Verlust = Totalverlust). Entwurf, Rechtsprüfung offen.*
Verschlüsselung (Transport)	TLS ist für die Weboberfläche und für jeden Aufruf der Schweizer Namenserkennungs-API (gehosteter Betrieb) erzwungen.
Zugriffskontrolle	Benannte, authentifizierte Benutzerkonten (bcrypt-Passwort-Hashing, offline-fähig). Innerhalb des Kunden-Teams ist ein Vorgang nur für dessen Ersteller und für Administratoren zugänglich; Rollen werden bei jeder Anfrage frisch geprüft.
Egress-Kontrolle	Daten verlassen das System nur durch eine ausdrückliche Freigabe des Menschen. Eine fail-closed Egress-Prüfung hält die Freigabe zurück, falls geschützte Werte im Klartext verblieben; eine bewusste Freigabe wird protokolliert.
Nachvollziehbarkeit	Manipulationssicheres, HMAC-verkettetes und PII-freies Audit-Protokoll; Umsortierung, Umschreiben oder eingefügte Einträge werden erkannt.
Web-Härtung	Content-Security-Policy mit Per-Request-Nonce, HSTS, X-Frame-Options DENY, CSRF-Schutz bei allen zustandsändernden Anfragen, Login-Rate-Limiting; öffentliche API-Dokumentation im Produktivbetrieb deaktiviert.
Ressourcenschutz	Speicher- und Nebenläufigkeitsgrenze des Containers; Upload-Grössen- und Dekompressionsgrenzen — eine einzelne Anfrage kann den Host nicht erschöpfen (DoS-Härtung).
Löschung	Bei Beendigung werden Personendaten nach Wahl des Kunden gelöscht oder zurückgegeben. Der Kunde kann Vorgänge jederzeit selbst vollständig löschen; jede Löschung wird in der Audit-Kette protokolliert.

Die Massnahmen bilden den Auslieferungszustand ab und können im Zeitverlauf durch gleichwertige oder stärkere Massnahmen ersetzt werden. Dieser Anhang ist Teil des AVV und ist vor der Verwendung rechtlich zu prüfen.

Kunde (Verantwortlicher)
Name, Datum, Unterschrift

iConference AG (Auftragsbearbeiter)
Name, Datum, Unterschrift