

TECHNISCH ORGANISATORISCHE MAßNAHMEN (TOM)

zwischen

HealthCare Consulting GmbH

Kolonitzgasse 2A/DG

1030 Wien

Österreich

Firmenbuch: FN 204710w

– nachfolgend „Anbieter“ –

und dem jeweiligen Unternehmenskunden

– nachfolgend „Kunde“ –

gemeinsam die „Parteien“.

1. INFORMATIONSSICHERHEITSORGANISATION

1.1. Der Anbieter unterhält ein der Größe, Art und Risikolage seiner Tätigkeit angemessenes Informationssicherheitsprogramm.

1.2. Dazu gehören insbesondere:

- a) definierte Verantwortlichkeiten für Informationssicherheit;
- b) dokumentierte Sicherheitsrichtlinien;
- c) regelmäßige Überprüfung relevanter Risiken;
- d) Security Incident Management;
- e) Berechtigungsmanagement;
- f) Business-Continuity- und Backup-Prozesse;

g) regelmäßige Schulung relevanter Mitarbeiter.

1.3. Verantwortliche Funktion für Informationssicherheit: Geschäftsführung des Anbieters

2. HOSTING UND INFRASTRUKTUR

2.1. Convilance wird über professionelle Cloud-/Hosting-Infrastruktur bereitgestellt.

a) Cloud-/Hosting-Anbieter: Microsoft Azure

b) Primäre Datenregion: EU / EWR

c) Backup-Region: EU / EWR

2.2. Produktionssysteme werden logisch von Entwicklungs- und Testsystemen getrennt.

2.3. Produktive Kundendaten sollen nicht für Entwicklungs- oder Testzwecke verwendet werden, außer soweit dies im Einzelfall erforderlich, rechtlich zulässig und angemessen abgesichert ist.

3. PHYSISCHE SICHERHEIT

3.1. Soweit die physische Infrastruktur durch professionelle Rechenzentrums- oder Cloud-Anbieter betrieben wird, stützt sich der Anbieter auf deren physische Sicherheitsmaßnahmen.

3.2. Diese sollen insbesondere umfassen:

a) physische Zugangskontrollen;

b) Besuchermanagement;

c) Schutz vor unbefugtem Zutritt;

d) Stromversorgungs- und Umgebungsüberwachung;

e) Brand- und Ausfallschutz;

f) kontrollierte Entsorgung von Datenträgern.

3.3. Der Anbieter selbst betreibt grundsätzlich keine frei zugänglichen Produktionsserver in eigenen Büroräumlichkeiten.

4. IDENTITY AND ACCESS MANAGEMENT

- 4.1. Zugriffe auf produktive Systeme werden nach dem Need-to-know- und Least-Privilege-Prinzip vergeben.
- 4.2. Administrative Berechtigungen werden auf Personen beschränkt, die diese für ihre Aufgaben benötigen.
- 4.3. Administrative Konten werden grundsätzlich personenbezogen vergeben.
- 4.4. Berechtigungen werden bei Rollenänderungen oder Ausscheiden von Mitarbeitern zeitnah angepasst bzw. entzogen.
- 4.5. Berechtigungen privilegierter Benutzer werden alle 6 Monate überprüft.

5. KUNDENSEITIGE ZUGRIFFSSTEUERUNG

- 5.1. Convillance unterstützt rollen- bzw. berechtigungsbezogene Zugriffskontrollen entsprechend der Produktkonfiguration.
- 5.2. Der Kunde ist verantwortlich für:
 - a) die Auswahl autorisierter Benutzer;
 - b) korrekte Rollenvergabe;
 - c) regelmäßige Überprüfung seiner Benutzer;
 - d) unverzügliches Deaktivieren nicht mehr benötigter Accounts;
 - e) Schutz kundenseitiger Zugangsdaten.

6. VERSCHLÜSSELUNG

- 6.1. Die Übertragung von Daten zwischen Benutzer und Convillance erfolgt über zeitgemäße verschlüsselte Transportprotokolle. Mindeststandard: TLS 1.3
- 6.2. Produktive Daten werden im Ruhezustand durch angemessene technische Schutzmechanismen der eingesetzten Infrastruktur geschützt. Encryption at Rest: AES-256

- 6.3. Kryptographische Schlüssel werden durch geeignete technische Verfahren verwaltet und vom Zugriff unberechtigter Personen geschützt.

7. NETZWERK- UND SYSTEMSCHUTZ

- 7.1. Der Anbieter setzt angemessene Maßnahmen zum Schutz der produktiven Infrastruktur ein:

- a) Netzwerksegmentierung bzw. logische Trennung;
- b) Firewall- oder vergleichbare Cloud-Sicherheitskontrollen;
- c) restriktive administrative Zugänge;
- d) abgesicherte Remote-Zugänge;
- e) automatisierte Monitoring-Funktionen;
- f) regelmäßige Aktualisierung relevanter Systemkomponenten.

- 7.2. Nicht erforderliche Dienste und Schnittstellen werden deaktiviert oder eingeschränkt.

8. SECURE SOFTWARE DEVELOPMENT LIFECYCLE

- 8.1. Der Anbieter unterhält einen dokumentierten Entwicklungs- und Release-Prozess.

- 8.2. Dieser umfasst risikobasiert insbesondere:

- a) definierte Anforderungen;
- b) Versionsverwaltung;
- c) Code Review bzw. angemessene Vier-Augen-Prüfungen;
- d) Trennung von Entwicklungs- und Produktionsumgebungen;
- e) Softwaretests vor produktiven Releases;
- f) kontrollierte Deployment-Prozesse;
- g) Change-Dokumentation;
- h) Verfahren für dringende Sicherheitsänderungen.

- 8.3. Änderungen am Produktivsystem dürfen nur durch hierzu berechnigte Personen oder kontrollierte Deployment-Prozesse erfolgen.

9. VULNERABILITY MANAGEMENT

9.1. Der Anbieter unterhält einen risikobasierten Prozess zur Identifikation und Behandlung technischer Schwachstellen.

- a) Dependency- und Vulnerability-Scanning;
- b) Security Advisories;
- c) Patch Management;
- d) Code- bzw. Application-Security-Tests.

10. LOGGING UND MONITORING

10.1. Für sicherheits- und systemrelevante Vorgänge werden angemessene Logs geführt.

- a) administrative Zugriffe;
- b) Authentifizierungsereignisse;
- c) technische Fehler;
- d) sicherheitsrelevante Systemereignisse;
- e) Deployment- und Systemänderungen.

10.2. Systemzeiten werden soweit praktikabel über geeignete Zeitquellen synchronisiert.

11. AUDIT TRAIL UND DATENINTEGRITÄT

11.1. Soweit entsprechende Produktfunktionen eingesetzt werden, dokumentiert Convillance relevante Bearbeitungs- bzw. Systemaktivitäten in einem Audit Trail.

11.2. Der Anbieter trifft angemessene Maßnahmen, damit protokollierte Audit-Trail-Einträge nicht durch gewöhnliche Endnutzer unkontrolliert verändert werden können.

11.3. Umfang und Aufbewahrung des fachlichen Audit Trails richten sich nach Produktfunktion und vereinbarter Konfiguration.

12. BACKUP

- 12.1. Der Anbieter führt angemessene regelmäßige Sicherungen der für die Wiederherstellung von Convillance erforderlichen Daten durch.
- 12.2. Backups werden logisch bzw. technisch so geschützt, dass ein einzelner gewöhnlicher Benutzerzugriff nicht ohne Weiteres zu einer Manipulation aller Sicherungskopien führt.

13. BEHANDLUNG VON SICHERHEITSVorfällen

- 13.1. Der Anbieter verfügt über einen dokumentierten Prozess zur Behandlung von Sicherheitsvorfällen.
- 13.2. Dieser umfasst:
 - a) Erkennung;
 - b) interne Eskalation;
 - c) Analyse;
 - d) Eindämmung;
 - e) Behebung;
 - f) Wiederherstellung;
 - g) Dokumentation;
 - h) gegebenenfalls Root-Cause-Analyse und CAPA.
- 13.3. Vertragsrelevante Meldepflichten gegenüber dem Kunden richten sich nach AGB, AVV und SLA.

14. MALWARE UND ENDPOINT SECURITY

- 14.1. Arbeitsplätze und Systeme mit administrativem Zugriff auf Convillance werden durch angemessene Endpoint- und Malware-Schutzmaßnahmen abgesichert.
- 14.2. Dazu gehören:
 - a) automatische Sicherheitsupdates;
 - b) Endpoint Protection;

- c) Festplattenverschlüsselung;
- d) Gerätesperre;
- e) restriktive lokale Administratorrechte.

15. SICHERHEIT BEI MITARBEITENDEN

- 15.1. Mitarbeitende mit relevantem Systemzugriff werden sorgfältig ausgewählt, unterliegen Vertraulichkeitsverpflichtungen, erhalten nur erforderliche Zugriffsrechte und werden zu Datenschutz und Informationssicherheit geschult.
- 15.2. Background Checks werden durchgeführt, soweit dies für die jeweilige Rolle angemessen und nach anwendbarem Arbeits- und Datenschutzrecht zulässig ist.
- 15.3. Relevante Mitarbeiter erhalten mindestens jährlich bzw. bei wesentlichen Änderungen Schulungen bzw. Awareness-Maßnahmen zu:
 - a) Datenschutz;
 - b) Informationssicherheit;
 - c) Phishing und Social Engineering;
 - d) Passwort- und Zugangssicherheit;
 - e) Incident Reporting;
 - f) Umgang mit vertraulichen Informationen.

16. MANDANTENTRENNUNG

- 16.1. Kundendaten werden innerhalb der SaaS-Architektur durch geeignete logische Zugriffskontrollen voneinander getrennt.
- 16.2. Benutzer eines Kunden können nicht auf Daten anderer Kunden zugreifen.

17. DATENMINIMIERUNG UND LÖSCHUNG

- 17.1. Der Anbieter stellt technische Prozesse zur Verfügung bzw. unterhält interne Verfahren, um Daten entsprechend den vertraglichen und konfigurierten Löscho- bzw. Anonymisierungsregeln zu behandeln.
- 17.2. Zugriff auf gelöschte produktive Daten ist nach Abschluss des Löschvorgangs nicht mehr möglich.
- 17.3. Backup-Daten werden im Rahmen des definierten Backup-Lebenszyklus überschrieben.

18. REGELMÄßIGE ÜBERPRÜFUNG

- 18.1. Die technischen und organisatorischen Maßnahmen werden unter Berücksichtigung von:
 - a) technischer Entwicklung;
 - b) Bedrohungslage;
 - c) Verarbeitungstätigkeit;
 - d) Kundennutzung;
 - e) regulatorischen Anforderungen
 regelmäßig überprüft und gegebenenfalls angepasst.

Stand: Jänner 2025 / Convilance_TOM_V2_2025-01