CUBERA

Technische und Organisatorische Massnahmen

Cubera Solutions AG
General-Wille-Strasse 96
CH-8706 Feldmeilen
www.cubera.ch

Präambel

Die Cubera Solutions AG, General-Wille-Strasse 96, CH-8706 Feldmeilen, entwickelt und betreibt Software für ihre Kundinnen und Kunden.

Soweit dabei Personendaten bearbeitet werden, handelt Cubera als Auftragsbearbeiterin. Verantwortliche bleibt die Kundin; sie entscheidet allein, welche Personendaten zu welchem Zweck bearbeitet werden. Gegenstand, Umfang und Dauer der Bearbeitung sowie die eingesetzten Unterauftragnehmer sind je Lösung im Vertrag über die Auftragsbearbeitung bezeichnet.

Cubera betreibt keine eigenen Rechenzentren. Die produktive Verarbeitung erfolgt in Rechenzentren spezialisierter Anbieter, welche über eigene Nachweise zur physischen Sicherheit verfügen.

Die nachstehenden Massnahmen dienen dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der bearbeiteten Informationen. Sie gelten für alle Mitarbeitenden und Beauftragten von Cubera, für die von Cubera betriebenen Systeme sowie für die eingesetzten Unterauftragnehmer.

Cubera betreibt ein Informationssicherheits-Managementsystem, das nach ISO/IEC 27001:2022 zertifiziert ist. Die Massnahmen werden mindestens jährlich sowie bei wesentlichen Änderungen der Bedrohungslage, der Technologie oder der rechtlichen Anforderungen überprüft und dem Stand der Technik angepasst; das Schutzniveau wird dabei nicht unterschritten.

Eine ausführliche Beschreibung der Massnahmen stellt Cubera auf Anfrage als Sicherheitsauskunft zur Verfügung.

1 Vertraulichkeit

Zutrittskontrolle

Der Zutritt zu den Geschäftsräumen ist auf berechtigte Personen beschränkt und über Schliessmittel geregelt, deren Ausgabe und Rückgabe dokumentiert wird. Ausser den Arbeitsgeräten der Mitarbeitenden unterhält Cubera keine eigenen Verarbeitungsanlagen.

Zugangskontrolle

Die Authentisierung erfolgt, wo technisch möglich, über einen zentralen Identitätsdienst. Für Zugriffe über den zentralen Identitätsdienst auf schützenswerte Daten und für administrative Zugriffe wird eine Mehrfaktor-Authentisierung verlangt; der Zugang zu Servern erfolgt schlüsselbasiert. Für Zugangsdaten gilt eine verbindliche Richtlinie; nicht personengebundene Zugangsdaten werden in einem zentralen, verschlüsselten Passwortverwaltungssystem geführt und bedarfsgerecht freigegeben, technische Geheimnisse der Anwendungen in einer dafür vorgesehenen Secret-Verwaltung. Arbeitsgeräte sind vollständig verschlüsselt und mit automatischer Bildschirmsperre versehen.

Zugriffskontrolle

Zugriffe werden nach dem Grundsatz der geringsten Berechtigung und nach dem Erforderlichkeitsprinzip erteilt. Administrative Zugriffe sind auf einen definierten Personenkreis beschränkt und werden getrennt von den normalen Benutzerkonten verwaltet. Berechtigungen werden periodisch überprüft und bereinigt.

Trennungskontrolle

Daten und Systeme verschiedener Kundinnen und Kunden werden logisch getrennt. Produktions-, Test- und Entwicklungsumgebungen sind technisch getrennt; der Einsatz von Produktivdaten ausserhalb der Produktion ist geregelt und auf begründete Fälle beschränkt.

Verschlüsselung

Übertragungen über öffentliche Netze erfolgen durchgängig verschlüsselt über TLS in einer aktuellen Version. Ruhende Daten werden auf Speicher- und Sicherungsmedien verschlüsselt. Schlüssel und Geheimnisse werden getrennt von den Daten in zugriffsbeschränkten Speichern verwahrt und beim Austritt Berechtigter sowie bei Verdacht auf Kompromittierung widerrufen oder erneuert.

Personal

Mitarbeitende werden vor der Anstellung auf ihre Eignung geprüft und schriftlich zur Vertraulichkeit verpflichtet; die Verpflichtung besteht über das Ende des Arbeitsverhältnisses hinaus. Ein verbindlicher Verhaltenskodex ist in Kraft. Mitarbeitende werden regelmässig zu Informationssicherheit und Datenschutz geschult; die Durchführung wird dokumentiert. Bei Austritt werden Berechtigungen entzogen und die Rückgabe der Arbeitsmittel dokumentiert.

2 Integrität

Weitergabekontrolle

Schützenswerte Daten werden ausschliesslich verschlüsselt übermittelt. Der Fernzugriff auf betriebene Systeme erfolgt nur über verschlüsselte Verbindungen und mit starker Authentisierung, über Mehrfaktor-Authentisierung oder schlüsselbasiert. Für die Vernichtung von Daten und Datenträgern besteht ein dokumentiertes Verfahren; ausgemusterte Datenträger werden nachweislich unbrauchbar gemacht oder sicher gelöscht.

Eingabe- und Änderungskontrolle

Änderungen an produktiven Systemen unterliegen einem dokumentierten, risikobasierten Änderungsverfahren; Freigaben und die Behandlung von Notfalländerungen sind geregelt. Sicherheitsrelevante Ereignisse werden protokolliert; die Protokolle sind gegen unbefugte Veränderung geschützt und werden zweckgebunden aufbewahrt.

3 Verfügbarkeit und Belastbarkeit

Datensicherung und Wiederherstellung

Für produktive Systeme bestehen automatische Datensicherungen. Sicherungen werden getrennt von den Produktivdaten aufbewahrt; Sicherungen, die Cubera selbst betreibt, werden verschlüsselt. Bei verwalteten Diensten sichert der Anbieter nach seinen eigenen Nachweisen. Die Wiederherstellbarkeit wird periodisch geprüft.

Betrieb

Verfügbarkeit, Auslastung und Störungen werden überwacht; Störungen lösen eine Alarmierung aus. Für Ausfälle und Notfälle bestehen dokumentierte Wiederanlaufverfahren, und Stellvertretungen sind geregelt. Ein redundanter Aufbau sowie zugesicherte Wiederherstellungsziele werden, soweit vereinbart, im jeweiligen Betriebsvertrag festgelegt.

Schutz vor Schadsoftware und Angriffen

Arbeitsgeräte und relevante Systeme verfügen über Schutzmechanismen gegen Schadsoftware. Ein vorgeschalteter Schutz gegen Überlastangriffe sowie eine Anwendungs-Firewall kommen zum Einsatz, soweit vertraglich vereinbart.

4 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

Informationssicherheits-Management

Cubera verfügt über eine dokumentierte Sicherheitsorganisation mit einer benannten Verantwortung für Informationssicherheit und Datenschutz. Grundlage bilden eine von der Geschäftsleitung verabschiedete Informationssicherheitsleitlinie sowie themenspezifische Richtlinien, ein Inventar der Informationswerte mit Eigentümerschaft und Schutzbedarf sowie ein Risikoregister mit zugewiesenen Massnahmen. Die Wirksamkeit wird anhand eines Kennzahlenprogramms und dokumentierter, wiederkehrender Auswertungen beurteilt und in der Managementbewertung behandelt.

Vorfallbehandlung

Für Informationssicherheits- und Datenschutzvorfälle besteht ein dokumentierter Prozess. Vorfälle werden in einem zentralen Register erfasst, klassifiziert und bis zum Abschluss nachverfolgt. Verletzungen der Datensicherheit werden der Verantwortlichen unverzüglich gemeldet, spätestens innert 24 Stunden nach Kenntnis, mit den zur Beurteilung und zur Erfüllung ihrer Meldepflichten erforderlichen Angaben. Die Erstmeldung enthält die zu diesem Zeitpunkt verfügbaren Angaben; weitere Angaben werden unverzüglich nachgereicht.

Schwachstellen und Aktualisierungen

Die eingesetzten Softwarekomponenten werden fortlaufend auf bekannte Schwachstellen überwacht. Festgestellte Schwachstellen werden nach Schweregrad und Ausnutzbarkeit priorisiert und einer Behebung zugeführt. Sicherheitsrelevante Aktualisierungen der Infrastruktur werden regelmässig eingespielt; kritische Schwachstellen werden ausserhalb des ordentlichen Rhythmus behandelt. Sicherheitslücken können Cubera über security@cubera.ch gemeldet werden; das Vorgehen regelt die veröffentlichte Coordinated Vulnerability Disclosure Policy.

Sichere Entwicklung

Für die Softwareentwicklung besteht eine verbindliche Richtlinie. Quellcode wird in einer Versionsverwaltung geführt, Änderungen werden vor der Übernahme überprüft, und Geheimnisse werden nicht im Quellcode geführt. Der Einsatz von Systemen der künstlichen Intelligenz ist durch eine Richtlinie geregelt und auf freigegebene Werkzeuge beschränkt; die Eingabe von Kundendaten in nicht freigegebene Dienste ist untersagt.

Datenhaltung und Löschung

Informationen werden nach einer verbindlichen Richtlinie klassifiziert; Personendaten werden ausschliesslich auf dafür freigegebenen Systemen gespeichert. Löschung und Rückgabe von Kundendaten nach Beendigung eines Auftrags richten sich nach dem jeweiligen Vertrag über die Auftragsbearbeitung.

Auftragskontrolle

Unterauftragnehmer werden vor dem Einsatz nach Sicherheits- und Datenschutzkriterien beurteilt und vertraglich auf ein Schutzniveau verpflichtet, welches dem vorliegenden entspricht. Cubera bevorzugt Anbieter mit Verarbeitungsstandorten in der Schweiz oder im Europäischen Wirtschaftsraum. Änderungen der eingesetzten Unterauftragnehmer werden der Verantwortlichen vorab mitgeteilt.

Prüfrecht

Die Verantwortliche kann die Einhaltung dieser Massnahmen nach vorheriger Ankündigung, während der ordentlichen Geschäftszeiten und ohne unangemessene Beeinträchtigung des Betriebs überprüfen. Cubera kann den Nachweis durch das Zertifikat nach ISO/IEC 27001, aktuelle Berichte oder die Sicherheitsauskunft erbringen. Reichen diese Nachweise im Einzelfall nicht aus, bleiben weitergehende Prüfungen einschliesslich Inspektionen vorbehalten. Die Kostentragung richtet sich nach dem jeweiligen Vertrag.