CovaSyn

SIG Lite (CovaSyn-Fassung)

Stand: 2026-08-04

Vorausgefüllte Antworten zu den Themenfeldern eines SIG-Lite-Fragebogens. Jede Antwort beschreibt den tatsächlichen Stand. Wo etwas nicht vorhanden ist, steht das dort, zusammen mit dem, was es ausgleicht.

Diese Fassung wird aus einer einzigen gepflegten Antwortbibliothek erzeugt. Eine Änderung wirkt gleichzeitig in allen Fassungen. Angaben beschreiben den tatsächlichen Stand; wo etwas nicht besteht, steht das ausdrücklich dort.

SIG A · Risiko- und Sicherheitsorganisation

Besteht ein dokumentiertes Informationssicherheits-Managementsystem?

Status: Teilweise

Die Sicherheitsleitlinien, das Zugriffskonzept, das Löschkonzept und der Notfallplan sind dokumentiert und werden jährlich überprüft. Eine ISO-27001-Zertifizierung besteht nicht; sie ist mit dokumentierter Anwendbarkeitserklärung in Vorbereitung. CovaSyn ist ein kleines Unternehmen, die Verantwortung liegt namentlich bei der Geschäftsführung.

Nachweis: Trust-Seite, Abschnitt Compliance-Posture

Bestehen Zertifizierungen (ISO 27001, SOC 2, TISAX)?

Status: Nein

Nein. ISO 27001 ist in Vorbereitung, SOC 2 ist nicht geplant, TISAX ist für unseren Markt nicht einschlägig. Wir behaupten keine Zertifizierung, die wir nicht haben. Eine Zertifizierung nehmen wir in Angriff, sobald ein konkreter Kundenvertrag sie verlangt und trägt.

Gibt es eine Change-Notification-Policy für Modell- und Werkzeugänderungen?

Status: Ja

Ja. Werkzeugversionen sind gepinnt, gleiche Eingabe ergibt reproduzierbar die gleiche Ausgabe. Änderungen an numerischen Werkzeugen oder an einem eingesetzten Sprachmodell, die das Ergebnis beeinflussen können, werden mindestens 30 Tage vor Wirksamkeit angekündigt, mit Angabe des betroffenen Werkzeugs und der erwarteten Wirkung. Bei validierten Kundenprozessen ist das die Grundlage Ihrer Change-Control.

Nachweis: Changelog auf covasyn.com, Enterprise-Rahmenvertrag

SIG D · Zugriffssteuerung

Wird Single Sign-On unterstützt?

Status: Ja

Ja, SAML 2.0 für Enterprise-Kunden, erprobt mit Microsoft Entra ID, Okta und Google Workspace. Nutzer werden beim ersten Anmelden anhand der verifizierten Unternehmensdomain automatisch der Organisation zugeordnet. SCIM zur automatischen Deprovisionierung ist auf Anfrage möglich.

Nachweis: SSO-Anleitung für Ihre IT

Wie ist der administrative Zugriff auf Produktionssysteme geregelt?

Status: Teilweise

Der administrative Zugriff auf die Anwendungsumgebung erfolgt ausschließlich über SSH mit hinterlegten Schlüsselpaaren, eine Anmeldung mit Passwort ist für das Verwaltungskonto abgeschaltet. Es gibt keinen geteilten Sammelaccount und keine weiteren Anmeldekonten auf dem System. Offen benannt: derzeit ist genau ein Schlüssel hinterlegt, ein zweiter benannter Zugang wird eingerichtet. Der Zugriff auf Kundendaten

erfolgt ausschließlich anlassbezogen zur Störungsbehebung, Anmeldungen werden systemseitig protokolliert.

Werden Zugriffe protokolliert und sind die Protokolle exportierbar?

Status: Ja

Ja. Jeder Werkzeugaufruf wird mit Zeitpunkt, Werkzeug, Version, Ergebnisstatus und Schlüsselkennung protokolliert. Die Protokolle sind als CSV oder JSON exportierbar. Ausgaben tragen einen SHA-256-Hash, nachträgliche Änderungen an einem Protokolleintrag fallen beim erneuten Hashen auf.

SIG G · Betrieb, Netz und Verschlüsselung

Wo werden die Daten gehostet?

Status: Ja

In Deutschland, bei der Hetzner Online GmbH. Die Datenhaltung erfolgt im EU-Raum, es gibt keine Spiegelung außerhalb der EU. Auf Wunsch ist ein Betrieb als Container auf Ihrer eigenen Infrastruktur möglich.

Ist die Übertragung verschlüsselt, und wie sind Daten im Ruhezustand geschützt?

Status: Ja

Der Transport läuft ausschließlich über TLS 1.2 oder höher, HSTS ist aktiv. Im Ruhezustand sind die Datenträger verschlüsselt; Zugangsdaten und Schlüssel werden nur als Hash beziehungsweise in getrennter Konfiguration gehalten und nie im Klartext protokolliert.

Werden Sicherheitsupdates und Abhängigkeiten regelmäßig geprüft?

Status: Ja

Ja. Bei jedem Codestand laufen automatisiert Typprüfung, Testlauf, Abhängigkeitsprüfung und eine Suche nach versehentlich eingecheckten Geheimnissen. Ein roter Lauf verhindert die Auslieferung.

SIG I · Vorfallbehandlung

Wie werden Sicherheitsvorfälle behandelt und gemeldet?

Status: Ja

Es besteht ein dokumentierter Meldeweg mit benannten Verantwortlichen. Betroffene Kunden werden unverzüglich informiert, spätestens innerhalb von 24 Stunden nach Feststellung eines Vorfalls mit möglichem Bezug zu ihren Daten. Die Meldefrist nach Art. 33 DSGVO gegenüber der Aufsichtsbehörde (72 Stunden) ist Teil des Ablaufs. Sicherheitsmeldungen von außen nehmen wir über security@covasyn.com entgegen.

Nachweis: security.txt nach RFC 9116, Sicherheitsseite

Werden Verfügbarkeit und Fehler überwacht?

Status: Ja

Ja, mit selbst betriebener Verfügbarkeitsmessung und Fehlererfassung, Alarmierung per E-Mail. Die Fehlererfassung ist so gebaut, dass sie ausdrücklich keine Anfrageinhalte, keine Suchparameter und keine hochgeladenen Inhalte erfasst. Eine zugesagte Verfügbarkeitsquote nennen wir erst, wenn sie über 30 Tage gemessen ist; eine belegte Zahl ist mehr wert als eine versprochene.

SIG K · Betriebskontinuität

Wie sind Sicherungskopien und Wiederherstellung geregelt?

Status: Teilweise

Die Datenbank wird täglich um 03:00 UTC automatisiert gesichert, die Vorhaltung beträgt 7 Tage. Zusätzlich entsteht vor jedem Ausrollen eine Momentaufnahme. Zielwerte: Wiederherstellungszeit unter 8 Stunden,

maximaler Datenverlust 24 Stunden. Offen benannt: die Sicherungen liegen derzeit verschlüsselt auf demselben Wirtssystem wie der Produktivbetrieb, eine räumlich getrennte Kopie und ein turnusmäßig protokollierter Wiederherstellungstest sind in Umsetzung. Für Enterprise-Kunden vereinbaren wir abweichende Vorhaltefristen und eine getrennte Ablage vertraglich.

Was passiert bei Ausfall oder Wegfall des Anbieters?

Status: Teilweise

CovaSyn ist ein kleines Unternehmen, das benennen wir offen. Zwei Personen haben administrativen Vollzugriff, ein Betriebshandbuch liegt vor, und Ihre Daten sind jederzeit vollständig exportierbar. Für Enterprise-Kunden ist der Betrieb auf eigener Infrastruktur die belastbarste Absicherung; die dafür nötigen Unterlagen sind Vertragsbestandteil.

SIG P · Datenschutz

Werden Kundendaten zum Training von Modellen verwendet?

Status: Nein

Nein. Hochgeladene Strukturen, Sequenzen und Dateien werden ausschließlich zur Bearbeitung der jeweiligen Anfrage verarbeitet und niemals zum Training eigener oder fremder Modelle verwendet. Diese Zusage steht vertraglich im Auftragsverarbeitungsvertrag, nicht nur auf der Website. Für eingesetzte Modellanbieter gelten Verträge, die Training auf übermittelten Daten ausschließen.

Nachweis: AVV § Zweckbindung, Trust-Seite

Wie ist die Mandantentrennung umgesetzt?

Status: Ja

Jeder Datensatz ist einem Account zugeordnet, und die Datenbank erzwingt die Trennung auf Zeilenebene (Row Level Security), nicht nur die Anwendung. Ein Zugriff über einen fremden Account liefert keine Zeilen, nicht eine gefilterte Ansicht. Für Enterprise-Kunden ist zusätzlich ein Einzelmandanten-Betrieb oder der Betrieb auf eigener Infrastruktur möglich.

Nachweis: Trust-Seite, technische Beschreibung auf Anfrage

Werden Daten auf Verlangen gelöscht, und wie sind die Fristen?

Status: Ja

Ja. Auf Verlangen löschen wir Kundendaten innerhalb von 30 Tagen, einschließlich der Sicherungskopien im Rahmen ihres Rotationszyklus (längstens 7 Tage). Nach Vertragsende werden Verarbeitungsdaten binnen 90 Tagen gelöscht. Ausgenommen sind gesetzlich aufbewahrungspflichtige Rechnungsdaten (10 Jahre nach HGB und AO), die keine Analyseinhalte enthalten.

Nachweis: Löschkonzept, AVV

Werden personenbezogene Daten in Drittländer übermittelt?

Status: Teilweise

Ja, in Teilen. Die Rechenwerkzeuge selbst laufen auf unserer Infrastruktur in der EU. Zwei Funktionen binden jedoch ein Sprachmodell von Anthropic mit Verarbeitung in den USA ein, und dabei werden Inhalte übermittelt: der Chat-Assistent im Strukturededitor (übermittelt die gezeichnete Struktur, den Gesprächsverlauf und die Ergebnisse der aufgerufenen Werkzeuge) sowie die Auswertungsfunktion im Bereich für Kampagnenanalyse (übermittelt Ergebniszusammenfassungen und statistische Auswertungen, keine Rohstrukturen). Die Übermittlung ist über Standardvertragsklauseln abgesichert, Anthropic ist in der Unterauftragsverarbeiter-Liste aufgeführt. Alle übrigen Werkzeuge, einschließlich Retrosynthese, Spektrenvorhersage und Toxikologie, arbeiten ohne Sprachmodell und ohne Drittlandübermittlung. Enterprise-Kunden können die Plattform vollständig auf eigener Infrastruktur betreiben, dann entfällt jede Übermittlung.

Nachweis: Unterauftragsverarbeiter-Liste, AVV Anlage, Architekturbeschreibung auf Anfrage

Wem gehören die Rechte an hochgeladenen Inhalten und den Ergebnissen?

Status: Ja

Die Rechte an Ihren Eingaben und an den erzeugten Ergebnissen verbleiben vollständig bei Ihnen. CovaSyn erwirbt daran keine Nutzungsrechte über die Erbringung der Leistung hinaus. Das ist im Rahmenvertrag ausdrücklich geregelt.

Nachweis: Enterprise-Rahmenvertrag, Abschnitt Rechte

SIG U · Künstliche Intelligenz

Sind die Ergebnisse deterministisch oder probabilistisch?

Status: Ja

Die numerischen Werkzeuge sind deterministisch: gepinnte Versionen, gleiche Eingabe ergibt reproduzierbar die gleiche Ausgabe, auch Wochen später. Ein Sprachmodell steht gegebenenfalls davor, um die Aufgabe zu verstehen, nicht im Rechenweg. Diese Trennung ist der Grund, warum die Ergebnisse prüfbar sind.

Welche Modellanbieter werden eingesetzt und was passiert mit den Daten dort?

Status: Ja

Wir setzen ein Sprachmodell von Anthropic (Claude) an genau zwei Stellen ein, beide klar abgegrenzt: im Chat-Assistenten des Strukturеditors und in der Auswertungsfunktion der Kampagnenanalyse. Übermittelt werden dort die jeweils bearbeitete Struktur, der Gesprächsverlauf und Ergebnisse der aufgerufenen Werkzeuge beziehungsweise statistische Auswertungen. Die Verarbeitung findet in den USA statt, abgesichert über Standardvertragsklauseln; nach den Geschäftsbedingungen des Anbieters für Geschäftskunden findet kein Training auf übermittelten Inhalten statt. Alle anderen Werkzeuge, also Retrosynthese, Spektrenvorhersage, Toxikologie, Stabilität und Chromatographie, nutzen eigene, auf chemische Aufgaben spezialisierte Modelle auf unserer Infrastruktur in der EU und übermitteln nichts an Dritte. Sie erkennen die beiden Ausnahmen daran, dass es sich um dialogbasierte Funktionen handelt, nicht um Rechenwerkzeuge. Eine Änderung der Anbieterliste kündigen wir mit Widerspruchsmöglichkeit an.

Nachweis: Unterauftragsverarbeiter-Liste

SIG V · Regulatorik und Verträge

Wie ist die Software nach GAMP 5 einzuordnen, und liefern Sie ein validiertes System?

Status: Teilweise

Die Einordnung ist GAMP 5 Kategorie 4 (konfiguriertes Produkt), beim Kunden wird kein individueller Code entwickelt. Wir liefern kein validiertes System, sondern die Unterlagen, mit denen Sie validieren: Vorlagen für Lastenheft, Funktionsspezifikation sowie Installations-, Funktions- und Leistungsqualifizierung. Validierung ist der Prozess in Ihrem Haus, keine Eigenschaft, die eine Software beim Kauf mitbringt. Das ist in der Pharmawelt der Normalfall.

Nachweis: Validierungspaket im Enterprise-Tarif

Wird ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO angeboten?

Status: Ja

Ja, mit Anlage zu den technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und mit der Unterauftragsverarbeiter-Liste. Der Vertrag wird auf Anfrage vor dem Preisgespräch zur Verfügung gestellt.

Nachweis: AVV auf Anfrage