Sicherheitsübersicht für Croco

Version: 1.0

Stand: 13. Juli 2026

Anbieter: CrossLink GmbH

---

1. Zweck dieser Sicherheitsübersicht

Diese Sicherheitsübersicht beschreibt zentrale technische und organisatorische Sicherheitsmaßnahmen im Zusammenhang mit der Plattform **Croco**.

Sie dient Mandanten, Interessenten und deren Datenschutz-, IT- und Sicherheitsverantwortlichen als verständliche Übersicht über grundlegende Sicherheitsprinzipien von Croco.

Diese Sicherheitsübersicht ergänzt die Allgemeinen Geschäftsbedingungen, die Servicebeschreibung, die Datenschutzerklärung, den Auftragsverarbeitungsvertrag und die Nutzungsrichtlinien.

Sie stellt keine Verfügbarkeitsgarantie, kein Service Level Agreement und keine abschließende technische Dokumentation dar.

---

2. Plattformbeschreibung

Croco ist eine cloudbasierte Kommunikations- und Kollaborationsplattform für Unternehmen und Organisationen.

Die Plattform unterstützt insbesondere:

- Mandantenverwaltung,
- Domainverwaltung,
- Benutzerverwaltung,
- Rollen und Berechtigungen,
- Kommunikationskontexte,
- Direktnachrichten,
- Gruppen und Kanäle,
- domainübergreifende Kommunikation,
- Dateien und Medien,
- Sprach- und Videokommunikation,
- mobile Apps für Android und iOS,
- Push-Benachrichtigungen.

Croco ist mandantenbasiert aufgebaut. Der Mandant ist die rechtliche und organisatorische Einheit. Innerhalb eines Mandanten können eine oder mehrere Domains betrieben werden. Domains sind die höchsten Kommunikationseinheiten innerhalb von Croco.

---

3. Sicherheitsprinzipien

CrossLink orientiert sich beim Betrieb von Croco an folgenden Grundprinzipien:

- Trennung von Mandanten,
- Trennung von Domains,
- Zugriff nur nach Berechtigung,
- rollenbasierte Zugriffskontrolle,
- kontextbezogene Kommunikation,
- Datenminimierung,
- sichere Übertragung,
- Schutz administrativer Zugänge,
- Missbrauchsprävention,
- nachvollziehbare Verantwortlichkeiten,
- kontinuierliche technische Weiterentwicklung.

Der Mandant bleibt für die sichere Nutzung innerhalb seines Mandantenkontos verantwortlich, insbesondere für Benutzer, Rollen, Berechtigungen, Endgeräte, externe Identitätsanbieter und interne Sicherheitsrichtlinien.

---

4. Hosting und Infrastruktur

Croco wird von CrossLink selbst betrieben.

Die zugrunde liegende Infrastruktur wird nach derzeitigem Stand im Rechenzentrumsumfeld der **Infomaniak Network SA** in der Schweiz betrieben.

Die Schweiz gilt nach Angemessenheitsentscheidung der Europäischen Kommission als Land mit angemessenem Datenschutzniveau.

CrossLink kann technische Infrastruktur, Systemarchitektur oder eingesetzte Dienstleister ändern, sofern vertragliche und datenschutzrechtliche Anforderungen eingehalten werden.

---

5. Mandanten- und Domaintrennung

Croco verwendet ein Mandantenmodell.

Ein Mandant ist die rechtliche und organisatorische Einheit, über die Abonnement, Rechnung, Domains und zentrale Einstellungen verwaltet werden.

Domains sind die höchsten Kommunikationseinheiten innerhalb eines Mandanten.

Die Plattform ist darauf ausgelegt, Daten, Benutzer, Rollen, Berechtigungen und Kommunikationskontexte logisch nach Mandanten und Domains zu trennen.

Der Mandant kann mehrere Domains verwenden, zum Beispiel für:

- Abteilungen,
- Standorte,

- Tochtergesellschaften,
- Marken,
- Projekte,
- Kundengruppen,
- interne und externe Kommunikationsbereiche.

---

6. Rollen und Berechtigungen

Croco stellt ein Rollen- und Berechtigungssystem bereit.

Berechtigungen können insbesondere auf folgenden Ebenen bestehen:

- Mandantenebene,
- Domainebene,
- Ebene einzelner Kommunikationskontexte.

Der Mandant kann Benutzer mit unterschiedlichen Rollen ausstatten, insbesondere mit Verwaltungsrollen, Domainrollen oder Rollen innerhalb einzelner Chats, Gruppen oder Kanäle.

Der Mandant ist selbst dafür verantwortlich, Rollen und Berechtigungen sorgfältig zu vergeben, regelmäßig zu überprüfen und nicht mehr benötigte Rechte zu entfernen.

CrossLink empfiehlt das Prinzip der minimal erforderlichen Berechtigung: Benutzer sollten nur jene Rechte erhalten, die sie für ihre Aufgabe benötigen.

---

7. Kommunikationskontexte

Kommunikationskontexte sind abgegrenzte Bereiche innerhalb von Croco, in denen Benutzer Informationen austauschen können.

Dazu zählen insbesondere:

- Direktnachrichten,
- Gruppen,
- Kanäle,
- themenbezogene Bereiche,
- vergleichbare Kommunikationsformen.

Der Zugriff auf Inhalte eines Kommunikationskontextes richtet sich nach der Teilnahme und den Berechtigungen innerhalb dieses Kommunikationskontextes.

Mandantenadministratoren und Domainadministratoren erhalten nicht automatisch Zugriff auf alle Kommunikationsinhalte.

Administratoren können Kommunikationsinhalte nur einsehen, wenn sie berechtigter Teilnehmer des jeweiligen Kommunikationskontextes sind oder durch eine innerhalb von Croco vorgesehene und berechtigte Handlung Teilnehmer werden.

Es besteht keine allgemeine zentrale Funktion, mit der Administratoren beliebige Kommunikationsinhalte

außerhalb eines Kommunikationskontextes einsehen oder entschlüsseln können.

---

8. Domainübergreifende Kommunikation

Croco kann Kommunikation zwischen unterschiedlichen Domains ermöglichen.

Domainübergreifende Kommunikation erfolgt nur, soweit sie technisch vorgesehen und durch die beteiligten Parteien freigegeben wurde.

Freigaben können insbesondere durch Kontaktanfragen, Einladungen oder andere innerhalb von Croco vorgesehene Mechanismen erfolgen.

Jede Domain bleibt für ihre eigenen Benutzer, Rollen, Berechtigungen und Kommunikationsinhalte verantwortlich.

Der Mandant ist dafür verantwortlich, sicherzustellen, dass Benutzer nur solche Informationen mit anderen Domains teilen, deren Weitergabe zulässig und gewünscht ist.

---

9. Authentifizierung

Croco kann die Anmeldung über OAuth oder vergleichbare externe Authentifizierungsverfahren unterstützen.

Dabei können externe Identitätsanbieter eingebunden werden.

Der Mandant ist dafür verantwortlich, externe Identitätsanbieter sicher zu konfigurieren und Benutzerzugänge ordnungsgemäß zu verwalten.

CrossLink ist nicht verantwortlich für Sicherheitsvorfälle, Fehlkonfigurationen oder Sperrungen, die auf externe Authentifizierungsdienste oder vom Mandanten verwaltete Identitätssysteme zurückzuführen sind.

---

10. Zugriffsschutz

CrossLink beschränkt den Zugriff auf Systeme und Daten auf berechtigte Personen.

Interne Zugriffe erfolgen nur, soweit sie für Betrieb, Wartung, Sicherheit, Fehleranalyse, Support oder Vertragserfüllung erforderlich sind.

Mögliche Zugriffsschutzmaßnahmen umfassen:

- rollenbasierte Zugriffsbeschränkungen,
- administrative Zugriffskontrollen,
- Protokollierung sicherheitsrelevanter Ereignisse,
- Begrenzung interner Zugriffsrechte,
- Trennung von Zuständigkeiten,
- Schutz administrativer Zugänge.

Der Mandant ist ergänzend dafür verantwortlich, eigene Benutzerkonten, Administratorrechte und Endgeräte abzusichern.

11. Übertragungssicherheit

CrossLink setzt angemessene Maßnahmen ein, um Daten während der Übertragung zu schützen.

Dazu zählen insbesondere verschlüsselte Übertragungswege, soweit dies technisch vorgesehen und branchenüblich ist.

Der Mandant ist dafür verantwortlich, sichere Endgeräte, aktuelle Browser, geschützte Netzwerke und geeignete interne Sicherheitsmaßnahmen zu verwenden.

---

12. Dateien und Medien

Croco ermöglicht abhängig vom Tarif das Hochladen und Teilen von Dateien und Medien.

Je nach Tarif gelten unterschiedliche Speichergrenzen und maximale Dateigrößen.

Der Mandant ist verantwortlich dafür, dass hochgeladene Dateien:

- rechtmäßig sind,
- keine Rechte Dritter verletzen,
- keine Schadsoftware enthalten,
- keine unbefugt offengelegten vertraulichen Informationen enthalten,
- keine personenbezogenen Daten ohne Rechtsgrundlage enthalten.

CrossLink kann Dateien einschränken, blockieren oder entfernen, wenn konkrete Hinweise auf Rechtsverletzungen, Sicherheitsrisiken oder Missbrauch bestehen.

---

13. Mobile Apps

Croco kann als mobile App für Android und iOS bereitgestellt werden.

Bei Nutzung der mobilen Apps können zusätzliche technische Daten verarbeitet werden, insbesondere:

- Geräteinformationen,
- App-Version,
- Betriebssysteminformationen,
- technische Diagnosedaten,
- Push-Token,
- Zustellinformationen.

Benutzer sollten mobile Endgeräte durch geeignete Maßnahmen schützen, insbesondere durch Gerätesperre, aktuelle Betriebssysteme, sichere App-Installationen und Schutz vor unbefugtem Zugriff.

---

14. Push-Benachrichtigungen

Croco kann Push-Benachrichtigungen verwenden.

Für Push-Benachrichtigungen werden je nach Plattform externe Push-Dienste eingesetzt:

- **Firebase Cloud Messaging (FCM)** für Android,
- **Apple Push Notification service (APNs)** für iOS.

Dabei können insbesondere Push-Token, Geräteinformationen, App-Informationen, Zustellinformationen und je nach Konfiguration Inhalte oder Teile von Push-Benachrichtigungen verarbeitet werden.

CrossLink ist bemüht, Push-Benachrichtigungen datensparsam zu gestalten.

Datenschutzfreundlich ist eine Konfiguration, bei der Push-Benachrichtigungen nur neutrale Hinweise enthalten, zum Beispiel „Neue Nachricht in Croco“, und eigentliche Kommunikationsinhalte erst nach Öffnen der App geladen werden.

---

15. Backups und Wiederherstellung

CrossLink kann Backups und Sicherungskopien erstellen, um den Systembetrieb, die Sicherheit und die technische Wiederherstellbarkeit von Croco zu unterstützen.

Backups dienen primär dem Schutz des Systembetriebs.

Sie sind nicht als individuelle Archivierungs- oder Wiederherstellungsfunktion für einzelne Mandanten, Domains, Nachrichten, Dateien oder Kommunikationskontexte vorgesehen.

Ein Anspruch auf Wiederherstellung einzelner Daten aus Backups besteht nur, wenn dies ausdrücklich vereinbart wurde.

Der Mandant sollte Daten rechtzeitig exportieren, soweit er diese außerhalb von Croco benötigt oder gesetzlichen, vertraglichen oder internen Aufbewahrungspflichten unterliegt.

---

16. Datenexport

Croco kann Funktionen zum Export von Kundendaten bereitstellen.

Der konkrete Umfang, das Format und die technische Verfügbarkeit von Exportfunktionen richten sich nach den jeweils bereitgestellten Funktionen der Plattform, der Servicebeschreibung oder einer gesonderten Vereinbarung.

Der Mandant ist dafür verantwortlich, Daten rechtzeitig zu exportieren, insbesondere vor Vertragsende.

CrossLink schuldet ohne gesonderte Vereinbarung keine individuelle Migration, Konvertierung oder Aufbereitung von Daten für Systeme Dritter.

---

17. Löschung nach Vertragsende

Nach Vertragsende werden Kundendaten nach Maßgabe der AGB, der Datenschutzerklärung und des Auftragsverarbeitungsvertrags gelöscht oder anonymisiert.

Sofern keine gesetzlichen Aufbewahrungspflichten, berechtigten Interessen oder abweichenden

Vereinbarungen entgegenstehen, werden Kundendaten spätestens 180 Tage nach Vertragsende gelöscht oder anonymisiert.

Daten in Backups können nach Maßgabe technischer Backup-Zyklen später überschrieben oder gelöscht werden.

Rechnungsdaten, Vertragsdaten und steuerlich relevante Unterlagen können aufgrund gesetzlicher Aufbewahrungspflichten länger gespeichert werden.

---

18. Protokollierung und Sicherheitsereignisse

CrossLink kann technische Protokolle und Sicherheitsereignisse verarbeiten, soweit dies für Betrieb, Sicherheit, Fehleranalyse, Missbrauchsprävention oder rechtliche Verteidigung erforderlich ist.

Dazu können insbesondere gehören:

- Anmeldeereignisse,
- fehlgeschlagene Anmeldeversuche,
- technische Fehler,
- Systemereignisse,
- sicherheitsrelevante Ereignisse,
- IP-Adressen,
- Geräte- und Browserinformationen,
- Zeitstempel.

CrossLink führt keine allgemeine inhaltliche Überwachung von Kommunikationsinhalten durch.

---

19. Missbrauchsprävention

CrossLink kann Maßnahmen zur Erkennung, Verhinderung und Begrenzung von Missbrauch einsetzen.

Missbrauch kann insbesondere umfassen:

- Spam,
- Phishing,
- Schadsoftware,
- Angriffe auf Systeme,
- Umgehung von Schutzmaßnahmen,
- unzulässige Automatisierung,
- übermäßige Nutzung,
- Verletzung von Rechten Dritter,
- rechtswidrige Inhalte.

Bei konkreten Hinweisen kann CrossLink Inhalte, Benutzer, Kommunikationskontexte, Domains oder Mandanten einschränken, sperren oder entfernen, soweit dies erforderlich und angemessen ist.

20. Wartung und Sicherheitsupdates

CrossLink kann Wartungsarbeiten, Sicherheitsupdates und technische Änderungen durchführen.

Wartungsarbeiten können zu vorübergehenden Einschränkungen führen.

Planbare Wartungsarbeiten werden nach Möglichkeit so durchgeführt, dass Auswirkungen auf Mandanten möglichst gering bleiben.

Sicherheitsrelevante Maßnahmen können auch kurzfristig und ohne vorherige Ankündigung erfolgen, wenn dies zum Schutz von Croco, Mandanten, Benutzern oder Dritten erforderlich ist.

---

21. Verfügbarkeit

Croco wird nach bestem Bemühen bereitgestellt.

Eine bestimmte Mindestverfügbarkeit, garantierte Reaktionszeit, garantierte Behebungszeit oder ein verbindliches Service Level Agreement besteht nur, wenn dies ausdrücklich schriftlich vereinbart wurde.

Technische Störungen können insbesondere entstehen durch:

- Wartungsarbeiten,
- Sicherheitsmaßnahmen,
- Netzwerkprobleme,
- Ausfälle von Rechenzentrumsinfrastruktur,
- Störungen bei Drittanbietern,
- Angriffe auf IT-Systeme,
- höhere Gewalt.

---

22. Verantwortung des Mandanten

Der Mandant ist für die sichere Nutzung von Croco innerhalb seines Mandantenkontos verantwortlich.

Dies umfasst insbesondere:

- Auswahl und Verwaltung von Benutzern,
- Vergabe von Rollen und Berechtigungen,
- regelmäßige Überprüfung administrativer Rechte,
- Schutz von Zugangsdaten,
- sichere Endgeräte,
- sichere Netzwerke,
- Verwaltung externer Identitätsanbieter,
- interne Datenschutz- und Sicherheitsrichtlinien,
- Schulung von Benutzern,

- rechtmäßige Nutzung domainübergreifender Kommunikation,
- rechtzeitiger Datenexport.

Sicherheitsmaßnahmen von CrossLink ersetzen nicht die internen Sicherheits- und Organisationspflichten des Mandanten.

---

23. Sicherheitsvorfälle

Der Mandant sollte CrossLink unverzüglich informieren, wenn konkrete Anhaltspunkte für einen Sicherheitsvorfall bestehen.

Dies gilt insbesondere bei:

- Verdacht auf unbefugten Zugriff,
- kompromittierten Zugangsdaten,
- Fehlkonfigurationen mit Sicherheitsrelevanz,
- unbefugter Offenlegung von Daten,
- Schadsoftware,
- missbräuchlicher Nutzung,
- Angriffen auf Croco oder Benutzer.

CrossLink wird Sicherheitsvorfälle im eigenen Verantwortungsbereich prüfen und angemessene Maßnahmen ergreifen.

Soweit personenbezogene Daten betroffen sind, gelten ergänzend die Datenschutzerklärung und der Auftragsverarbeitungsvertrag.

---

24. Unterauftragsverarbeiter und Drittanbieter

Für Betrieb, Infrastruktur oder bestimmte Funktionen können Dienstleister oder Drittanbieter eingesetzt werden.

Nach derzeitigem Stand sind insbesondere relevant:

- Infomaniak Network SA für Rechenzentrums- und Infrastrukturumgebung,
- Google / Firebase Cloud Messaging für Android-Push-Benachrichtigungen,
- Apple Push Notification service für iOS-Push-Benachrichtigungen.

Weitere Informationen ergeben sich aus der Datenschutzerklärung und dem Auftragsverarbeitungsvertrag.

---

25. Kein Ersatz für Kundenaudit

Diese Sicherheitsübersicht dient der allgemeinen Information.

Sie ersetzt keine individuelle Sicherheitsprüfung, kein Audit, keine Datenschutz-Folgenabschätzung und keine rechtliche Bewertung durch den Mandanten.

Der Mandant ist selbst dafür verantwortlich zu prüfen, ob Croco für seine technischen, organisatorischen,

rechtlichen und branchenspezifischen Anforderungen geeignet ist.

---

26. Änderungen dieser Sicherheitsübersicht

CrossLink kann diese Sicherheitsübersicht aktualisieren, wenn sich technische, organisatorische, rechtliche oder sicherheitsbezogene Umstände ändern.

Die jeweils aktuelle Fassung wird über die Website von CrossLink, innerhalb von Croco oder auf anderem geeigneten Weg bereitgestellt.

Wesentliche Änderungen können dem Mandanten zusätzlich mitgeteilt werden.