Auftragsverarbeitungsvertrag (AVV) für Croco

Version: 1.0

Stand: 13. Juli 2026

Anbieter / Auftragsverarbeiter: CrossLink GmbH

---

1. Präambel

Dieser Auftragsverarbeitungsvertrag („AVV“) regelt die Verarbeitung personenbezogener Daten durch die **CrossLink GmbH** („CrossLink“ oder „Auftragsverarbeiter“) im Auftrag des jeweiligen Mandanten („Mandant“ oder „Verantwortlicher“) im Zusammenhang mit der Nutzung der Plattform **Croco**.

Croco ist eine cloudbasierte Kommunikations- und Kollaborationsplattform für Unternehmen und Organisationen. Der Mandant nutzt Croco zur Kommunikation und Zusammenarbeit innerhalb eines Mandanten, innerhalb von Domains sowie – soweit freigegeben – zwischen unterschiedlichen Domains.

Soweit CrossLink personenbezogene Daten im Auftrag des Mandanten verarbeitet, erfolgt diese Verarbeitung nach Maßgabe dieses AVV, der Datenschutz-Grundverordnung („DSGVO“), der AGB, der Servicebeschreibung und der Weisungen des Mandanten.

Dieser AVV ergänzt die Allgemeinen Geschäftsbedingungen für Croco. Bei Widersprüchen zwischen diesem AVV und den AGB gehen die Regelungen dieses AVV in Bezug auf die Verarbeitung personenbezogener Daten im Auftrag vor.

---

2. Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch CrossLink im Auftrag des Mandanten im Rahmen der Bereitstellung, des Betriebs, der Wartung, der Sicherung und des Supports von Croco.

Die Verarbeitung betrifft insbesondere personenbezogene Daten, die der Mandant, dessen Administratoren, Benutzer oder Kommunikationspartner innerhalb von Croco eingeben, übermitteln, speichern, teilen oder sonst verarbeiten.

2.2 Dauer

Die Dauer der Verarbeitung entspricht der Laufzeit des Vertrags über die Nutzung von Croco.

Nach Vertragsende werden personenbezogene Daten nach Maßgabe der AGB, der Servicebeschreibung, dieses AVV und gesetzlicher Vorgaben gelöscht oder anonymisiert.

Sofern keine gesetzlichen Aufbewahrungspflichten, berechtigten Interessen oder abweichenden Vereinbarungen entgegenstehen, werden Kundendaten spätestens **180 Tage nach Vertragsende** gelöscht oder anonymisiert.

---

3. Art und Zweck der Verarbeitung

3.1 Art der Verarbeitung

CrossLink verarbeitet personenbezogene Daten insbesondere durch:

- Erheben,
- Erfassen,
- Organisieren,
- Ordnen,
- Speichern,
- Anpassen,
- Verändern,
- Auslesen,
- Abfragen,
- Verwenden,
- Offenlegen durch Übermittlung,
- Bereitstellen,
- Abgleichen,
- Verknüpfen,
- Einschränken,
- Löschen,
- Vernichten.

3.2 Zweck der Verarbeitung

Die Verarbeitung erfolgt ausschließlich zum Zweck der Bereitstellung und des Betriebs von Croco.

Dazu zählen insbesondere:

- Einrichtung und Verwaltung von Mandanten,
- Einrichtung und Verwaltung von Domains,
- Verwaltung von Benutzern,
- Verwaltung von Rollen und Berechtigungen,
- Bereitstellung von Kommunikationskontexten,
- Übermittlung und Speicherung von Nachrichten,
- Verarbeitung von Dateien und Medien,
- Ermöglichung domainübergreifender Kommunikation,
- Bereitstellung von Sprach- und Videofunktionen,
- Bereitstellung mobiler Apps,
- Zustellung von Push-Benachrichtigungen,
- Authentifizierung und Zugriffskontrolle,

- Sicherheit und Missbrauchsprävention,
- Fehleranalyse,
- Support,
- Wartung,
- technische Weiterentwicklung,
- Datenexport,
- Löschung und Anonymisierung nach Vertragsende.

CrossLink verarbeitet personenbezogene Daten nicht für eigene Zwecke, soweit CrossLink als Auftragsverarbeiter handelt.

---

4. Kategorien personenbezogener Daten

Im Rahmen der Nutzung von Croco können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden:

4.1 Benutzer- und Kontodaten

- Name,
- E-Mail-Adresse,
- Benutzerkennung,
- Profilinformationen,
- Profilbild oder Avatar, sofern hochgeladen,
- Spracheinstellungen,
- Kontoeinstellungen,
- Zugehörigkeit zu Mandanten und Domains,
- Rollen,
- Berechtigungen,
- Einladungsstatus,
- Aktivierungsstatus,
- Erstellungs- und Änderungszeitpunkte.

4.2 Kommunikationsdaten

- Nachrichten,
- Direktnachrichten,
- Gruppenkommunikation,
- Kanalnachrichten,
- Reaktionen,
- Kommentare,

- Erwähnungen,
- Teilnehmerinformationen,
- Zeitstempel,
- Informationen über Kommunikationskontexte,
- Informationen zu Kontaktanfragen zwischen Domains,
- Informationen zu domainübergreifender Kommunikation.

4.3 Dateien und Medien

- hochgeladene Dateien,
- Dateinamen,
- Dateitypen,
- Dateigrößen,
- Medieninhalte,
- Anhänge,
- technische Metadaten zu Dateien,
- Informationen über Upload, Download oder Freigabe, soweit technisch verarbeitet.

4.4 Rollen- und Berechtigungsdaten

- Mandantenrollen,
- Domainrollen,
- Rollen innerhalb von Kommunikationskontexten,
- individuelle Berechtigungen,
- Berechtigungsänderungen,
- Administratorzuweisungen,
- Freigaben,
- Zugriffsinformationen.

4.5 Authentifizierungs- und Sicherheitsdaten

- Login-Daten,
- Authentifizierungsstatus,
- OAuth-Daten, soweit erforderlich,
- technische Sitzungsdaten,
- Geräteinformationen,
- IP-Adressen,
- Sicherheitsereignisse,
- fehlgeschlagene Anmeldeversuche,
- Zugriffshistorie, soweit technisch verarbeitet,

- Push-Token,
- App-Informationen.

4.6 Technische Betriebsdaten

- Logdaten,
- Fehlerprotokolle,
- Systemereignisse,
- Performance-Daten,
- Verbindungsdaten,
- Zustellinformationen,
- Browser- und Geräteinformationen,
- App-Versionen,
- Betriebssysteminformationen,
- technische Diagnoseinformationen.

4.7 Supportdaten

- Inhalt von Supportanfragen,
- Kontaktdaten der anfragenden Person,
- technische Beschreibungen,
- Screenshots oder Dateien, sofern übermittelt,
- Kommunikationsverlauf,
- Bearbeitungsstatus,
- interne Supportnotizen.

---

5. Kategorien betroffener Personen

Die Verarbeitung kann insbesondere personenbezogene Daten folgender Kategorien betroffener Personen betreffen:

- Benutzer des Mandanten,
- Mandantenadministratoren,
- Domainadministratoren,
- Mitarbeiter des Mandanten,
- freie Mitarbeiter des Mandanten,
- Dienstleister des Mandanten,
- Kunden des Mandanten,
- Kommunikationspartner des Mandanten,
- Benutzer anderer Domains bei domainübergreifender Kommunikation,

- Ansprechpartner des Mandanten,
- Supportkontakte,
- sonstige Personen, deren Daten durch den Mandanten oder dessen Benutzer in Croco verarbeitet werden.

---

6. Weisungen des Mandanten

6.1 Weisungsgebundenheit

CrossLink verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Mandanten, soweit CrossLink als Auftragsverarbeiter handelt.

Als Weisungen gelten insbesondere:

- dieser AVV,
- die AGB,
- die Servicebeschreibung,
- die Konfiguration durch den Mandanten,
- die Nutzung von Croco durch berechtigte Benutzer,
- individuelle schriftliche Vereinbarungen,
- dokumentierte Support- oder Administrationsanfragen.

6.2 Weisungen innerhalb von Croco

Der Mandant kann Weisungen auch durch technische Konfiguration innerhalb von Croco erteilen, insbesondere durch:

- Einrichtung von Domains,
- Anlage von Benutzern,
- Vergabe von Rollen und Berechtigungen,
- Erstellung von Kommunikationskontexten,
- Freigabe domainübergreifender Kommunikation,
- Upload von Dateien,
- Löschung von Daten,
- Nutzung von Exportfunktionen,
- Deaktivierung oder Entfernung von Benutzern.

6.3 Unzulässige Weisungen

CrossLink ist nicht verpflichtet, Weisungen auszuführen, die offensichtlich gegen geltendes Recht verstoßen.

Ist CrossLink der Ansicht, dass eine Weisung gegen Datenschutzrecht oder sonstiges Recht verstößt, wird CrossLink den Mandanten darauf hinweisen, soweit dies rechtlich zulässig ist.

CrossLink kann die Ausführung einer Weisung aussetzen, bis der Mandant die Weisung bestätigt, ändert oder zurücknimmt.

6.4 Weisungen außerhalb des vereinbarten Leistungsumfangs

Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, insbesondere individuelle Datenmigrationen, Sonderauswertungen, manuelle Datenbearbeitungen oder individuelle Lösch- und Wiederherstellungsmaßnahmen, bedürfen einer gesonderten Vereinbarung.

CrossLink kann hierfür eine angemessene Vergütung verlangen.

---

7. Pflichten von CrossLink

CrossLink verpflichtet sich, personenbezogene Daten im Auftrag des Mandanten nur nach Maßgabe dieses AVV und der dokumentierten Weisungen des Mandanten zu verarbeiten.

CrossLink verpflichtet sich insbesondere:

- personenbezogene Daten vertraulich zu behandeln,
- nur befugten Personen Zugriff zu gewähren,
- angemessene technische und organisatorische Maßnahmen zu treffen,
- den Mandanten bei der Erfüllung datenschutzrechtlicher Pflichten angemessen zu unterstützen,
- Unterauftragsverarbeiter nur nach Maßgabe dieses AVV einzusetzen,
- Datenschutzverletzungen nach Maßgabe dieses AVV mitzuteilen,
- personenbezogene Daten nach Vertragsende nach Maßgabe dieses AVV zu löschen oder zurückzugeben,
- dem Mandanten erforderliche Informationen zur Verfügung zu stellen, um die Einhaltung dieses AVV nachweisen zu können.

---

8. Pflichten des Mandanten

Der Mandant bleibt Verantwortlicher im Sinne der DSGVO.

Der Mandant ist insbesondere verantwortlich für:

- die Rechtmäßigkeit der Verarbeitung personenbezogener Daten,
- das Vorliegen geeigneter Rechtsgrundlagen,
- die Information betroffener Personen,
- die Bearbeitung von Betroffenenrechten,
- die Rechtmäßigkeit von Kommunikationsinhalten,
- die Konfiguration von Rollen und Berechtigungen,
- die Auswahl und Verwaltung von Benutzern,
- die Freigabe domainübergreifender Kommunikation,
- die Einhaltung interner Lösch- und Aufbewahrungspflichten,
- die Prüfung, ob Croco für seine Zwecke geeignet ist,
- die Beachtung besonderer Branchen- oder Berufsgeheimnisse, soweit anwendbar.

Der Mandant darf in Croco nur solche personenbezogenen Daten verarbeiten, zu deren Verarbeitung er

berechtigt ist.

---

9. Vertraulichkeit

CrossLink stellt sicher, dass Personen, die personenbezogene Daten im Auftrag des Mandanten verarbeiten, zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Zugriff auf personenbezogene Daten wird auf jene Personen beschränkt, die diesen Zugriff zur Erfüllung ihrer Aufgaben benötigen.

Die Vertraulichkeitspflicht gilt auch nach Beendigung der Tätigkeit der jeweiligen Person fort.

---

10. Technische und organisatorische Maßnahmen

CrossLink trifft angemessene technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die Maßnahmen sind in **Anlage 2 – Technische und organisatorische Maßnahmen** beschrieben.

CrossLink kann technische und organisatorische Maßnahmen weiterentwickeln, anpassen oder ersetzen, sofern das vereinbarte Schutzniveau dadurch nicht wesentlich unterschritten wird.

Der Mandant nimmt zur Kenntnis, dass er selbst für ergänzende Maßnahmen in seinem Verantwortungsbereich zuständig ist, insbesondere:

- sichere Endgeräte,
- sichere Netzwerke,
- Verwaltung von Benutzerkonten,
- Vergabe von Rollen und Berechtigungen,
- interne Datenschutzrichtlinien,
- Schulung von Benutzern,
- Kontrolle externer Identitätsanbieter.

---

11. Unterauftragsverarbeiter

11.1 Allgemeine Genehmigung

Der Mandant erteilt CrossLink eine allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern, soweit diese für die Bereitstellung, den Betrieb, die Sicherheit, Wartung, Support oder Zustellung von Funktionen von Croco erforderlich sind.

Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage 3 – Unterauftragsverarbeiter** aufgeführt.

11.2 Verpflichtung von Unterauftragsverarbeitern

CrossLink verpflichtet Unterauftragsverarbeiter auf Datenschutzpflichten, die den Pflichten aus diesem AVV im Wesentlichen entsprechen.

CrossLink bleibt gegenüber dem Mandanten für die Erfüllung der Pflichten der Unterauftragsverarbeiter verantwortlich, soweit die DSGVO dies vorsieht.

11.3 Änderungen bei Unterauftragsverarbeitern

CrossLink informiert den Mandanten über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern.

Die Information kann insbesondere per E-Mail, innerhalb von Croco, über eine Unterauftragsverarbeiterliste oder über eine sonstige geeignete Mitteilung erfolgen.

Der Mandant kann aus wichtigem datenschutzrechtlichem Grund gegen eine Änderung Einspruch erheben.

Der Einspruch muss innerhalb einer angemessenen Frist erfolgen, sofern CrossLink in der Mitteilung keine andere Frist nennt.

Kann zwischen den Parteien keine angemessene Lösung gefunden werden, kann jede Partei das betroffene Vertragsverhältnis nach Maßgabe der AGB kündigen.

---

12. Drittlandübermittlungen

Eine Verarbeitung personenbezogener Daten außerhalb des Europäischen Wirtschaftsraums erfolgt nur, soweit hierfür eine geeignete Rechtsgrundlage besteht.

Dies kann insbesondere der Fall sein bei:

- einem Angemessenheitsbeschluss der Europäischen Kommission,
- Standardvertragsklauseln,
- verbindlichen internen Datenschutzvorschriften,
- gesetzlichen Ausnahmen,
- sonstigen geeigneten Garantien nach der DSGVO.

Croco wird nach derzeitigem Stand von CrossLink selbst betrieben. Die zugrunde liegende Infrastruktur wird im Rechenzentrumsumfeld der Infomaniak Network SA in der Schweiz betrieben.

Die Schweiz verfügt nach derzeitigem Stand über ein von der Europäischen Kommission anerkanntes angemessenes Datenschutzniveau.

Für Push-Benachrichtigungen können personenbezogene Daten an Google bzw. Apple übermittelt werden. Dies kann je nach technischer Verarbeitung und Standort der jeweiligen Anbieter auch Drittlandbezüge auslösen.

---

13. Unterstützung bei Betroffenenrechten

CrossLink unterstützt den Mandanten im Rahmen des Zumutbaren und Erforderlichen bei der Erfüllung von Pflichten zur Wahrung der Rechte betroffener Personen.

Dies betrifft insbesondere:

- Auskunft,
- Berichtigung,
- Löschung,
- Einschränkung der Verarbeitung,
- Datenübertragbarkeit,
- Widerspruch,
- Widerruf von Einwilligungen, soweit relevant.

Soweit eine betroffene Person CrossLink unmittelbar kontaktiert und die Anfrage Daten betrifft, die CrossLink im Auftrag des Mandanten verarbeitet, wird CrossLink die Anfrage nach Möglichkeit an den Mandanten weiterleiten.

CrossLink beantwortet solche Anfragen nicht eigenständig inhaltlich, sofern CrossLink hierzu nicht gesetzlich verpflichtet ist.

Unterstützungsleistungen, die über die vertraglich geschuldete Plattformfunktionalität hinausgehen, können gesondert vergütet werden.

---

14. Unterstützung bei Datenschutz-Folgenabschätzungen und Konsultationen

CrossLink unterstützt den Mandanten im Rahmen des Zumutbaren und Erforderlichen bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen mit Aufsichtsbehörden, soweit sich die Unterstützung auf die von CrossLink erbrachte Auftragsverarbeitung bezieht.

Der Mandant bleibt selbst dafür verantwortlich, zu prüfen, ob eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation erforderlich ist.

Unterstützungsleistungen, die über die Bereitstellung vorhandener Informationen hinausgehen, können gesondert vergütet werden.

---

15. Verletzungen des Schutzes personenbezogener Daten

15.1 Mitteilung durch CrossLink

CrossLink informiert den Mandanten unverzüglich, nachdem CrossLink eine Verletzung des Schutzes personenbezogener Daten festgestellt hat, die personenbezogene Daten betrifft, die CrossLink im Auftrag des Mandanten verarbeitet.

15.2 Inhalt der Mitteilung

Die Mitteilung enthält, soweit CrossLink die Informationen vorliegen und dies zumutbar ist, insbesondere:

- Art der Datenschutzverletzung,
- betroffene Datenkategorien,

- betroffene Personengruppen,
- ungefähre Anzahl betroffener Personen, soweit bekannt,
- wahrscheinliche Folgen,
- bereits ergriffene oder vorgeschlagene Maßnahmen,
- Kontaktstelle für Rückfragen.

Informationen können schrittweise bereitgestellt werden, wenn nicht alle Informationen sofort verfügbar sind.

15.3 Verantwortung des Mandanten

Der Mandant bleibt verantwortlich für die Prüfung, ob eine Meldung an eine Aufsichtsbehörde oder eine Benachrichtigung betroffener Personen erforderlich ist.

CrossLink unterstützt den Mandanten im Rahmen des Zumutbaren und Erforderlichen.

---

16. Nachweise und Prüfungen

16.1 Nachweise

CrossLink stellt dem Mandanten auf Anfrage geeignete Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus diesem AVV nachzuweisen.

Dies kann insbesondere erfolgen durch:

- Beschreibung technischer und organisatorischer Maßnahmen,
- Sicherheitsübersicht,
- Unterauftragsverarbeiterliste,
- Zertifikate, soweit vorhanden,
- Auditberichte, soweit vorhanden,
- schriftliche Auskünfte.

16.2 Prüfungen durch den Mandanten

Der Mandant ist berechtigt, die Einhaltung dieses AVV im angemessenen Umfang zu prüfen.

Prüfungen müssen rechtzeitig angekündigt werden, dürfen den Betrieb von CrossLink nicht unangemessen beeinträchtigen und müssen Vertraulichkeits- und Sicherheitsanforderungen beachten.

Vor-Ort-Prüfungen sind nur zulässig, wenn der Mandant ein berechtigtes Interesse darlegt und die erforderlichen Informationen nicht auf andere zumutbare Weise bereitgestellt werden können.

CrossLink kann eine angemessene Vergütung für Prüfungen verlangen, die über gesetzlich erforderliche oder vertraglich übliche Nachweise hinausgehen.

16.3 Schutz anderer Mandanten

Prüfungen dürfen keine Daten, Systeme, Geschäftsgeheimnisse oder Sicherheitsinformationen anderer Mandanten offenlegen oder gefährden.

CrossLink kann Zugang zu Informationen, Systemen oder Räumen verweigern oder beschränken, soweit dies zum Schutz anderer Mandanten, der Sicherheit, von Geschäftsgeheimnissen oder gesetzlicher Pflichten erforderlich ist.

---

17. Löschung und Rückgabe personenbezogener Daten

Nach Beendigung des Vertrags löscht oder anonymisiert CrossLink personenbezogene Daten nach Maßgabe der AGB, der Servicebeschreibung und dieses AVV.

Sofern keine gesetzlichen Aufbewahrungspflichten, berechtigten Interessen oder abweichenden Vereinbarungen entgegenstehen, werden Kundendaten spätestens **180 Tage nach Vertragsende** gelöscht oder anonymisiert.

Der Mandant kann Kundendaten vor Vertragsende exportieren, soweit Croco entsprechende Exportfunktionen bereitstellt.

Eine individuelle Datenmigration, Aufbereitung oder Konvertierung in bestimmte Zielformate wird nur geschuldet, wenn dies ausdrücklich vereinbart wurde.

Daten in Backups werden nach Maßgabe technischer Backup-Zyklen gelöscht oder überschrieben. Backups dienen primär dem Systemschutz und nicht der individuellen Archivierung einzelner Daten für den Mandanten.

---

18. Berichtigung, Einschränkung und Löschung während der Vertragslaufzeit

Der Mandant kann personenbezogene Daten während der Vertragslaufzeit selbst berichtigen, löschen oder einschränken, soweit Croco entsprechende Funktionen bereitstellt.

Soweit eine Bearbeitung durch CrossLink erforderlich ist und nicht über die Plattformfunktionen erfolgen kann, unterstützt CrossLink den Mandanten im Rahmen des Zumutbaren und Erforderlichen.

CrossLink kann für manuelle Sonderleistungen eine angemessene Vergütung verlangen, soweit keine gesetzliche Pflicht zur unentgeltlichen Unterstützung besteht.

---

19. Mobile Apps und Push-Benachrichtigungen

CrossLink stellt Croco auch als mobile App für Android und iOS bereit.

Zur Zustellung von Push-Benachrichtigungen können externe Push-Dienste verwendet werden:

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

Dabei können insbesondere folgende Daten verarbeitet werden:

- Push-Token,
- Geräteinformationen,
- App-Version,

- Betriebssysteminformationen,
- Zustellinformationen,
- technische Kommunikationsdaten,
- Inhalte oder Teile von Push-Benachrichtigungen, soweit technisch erforderlich oder konfiguriert.

CrossLink ist bemüht, Push-Benachrichtigungen datensparsam zu gestalten.

Der Mandant nimmt zur Kenntnis, dass Push-Benachrichtigungen über die Infrastruktur der jeweiligen Plattformanbieter zugestellt werden.

Soweit Push-Benachrichtigungen Nachrichtenvorschauen oder personenbezogene Inhalte enthalten, können diese Inhalte an die jeweiligen Push-Dienste übermittelt werden. Datenschutzfreundlicher ist eine Konfiguration, bei der Push-Benachrichtigungen nur neutrale Hinweise enthalten und eigentliche Kommunikationsinhalte erst nach Öffnen der App geladen werden.

---

20. Kommunikationsinhalte und Administratorzugriff

Kommunikationsinhalte werden innerhalb von Kommunikationskontexten verarbeitet.

Der Zugriff auf Kommunikationsinhalte richtet sich nach Teilnahme und Berechtigung innerhalb des jeweiligen Kommunikationskontextes.

Mandantenadministratoren und Domainadministratoren erhalten nicht allein aufgrund ihrer administrativen Rolle 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.

---

21. Berichtigung und Information bei Fehlern

CrossLink informiert den Mandanten, wenn CrossLink feststellt, dass personenbezogene Daten im Auftrag des Mandanten unrichtig, unvollständig oder fehlerhaft verarbeitet wurden und dies für den Mandanten relevant ist.

Der Mandant bleibt verantwortlich für die inhaltliche Richtigkeit der von ihm oder seinen Benutzern in Croco eingegebenen Daten.

---

22. Rückfragen und Datenschutzkontakt

Anfragen zum Datenschutz und zu diesem AVV können an folgende Kontaktadresse gerichtet werden:

CrossLink GmbH

[Adresse]

Österreich

E-Mail: [Datenschutz-E-Mail-Adresse]

Web: https://crosslink.at

Anlage 1 – Beschreibung der Verarbeitung

1. Gegenstand der Verarbeitung

Bereitstellung, Betrieb, Wartung, Support und Absicherung der Plattform Croco als cloudbasierte Kommunikations- und Kollaborationsplattform für Unternehmen und Organisationen.

2. Zweck der Verarbeitung

- digitale Kommunikation,
- Zusammenarbeit,
- Benutzerverwaltung,
- Domainverwaltung,
- Rollen- und Berechtigungsverwaltung,
- Verwaltung von Kommunikationskontexten,
- domainübergreifende Kommunikation,
- Datei- und Medienaustausch,
- Sprach- und Videokommunikation,
- mobile Nutzung,
- Push-Benachrichtigungen,
- Sicherheit,
- Support,
- Fehleranalyse,
- Datenexport,
- Löschung nach Vertragsende.

3. Art der personenbezogenen Daten

- Stammdaten,
- Kontaktdaten,
- Benutzerkontodaten,
- Rollen- und Berechtigungsdaten,
- Kommunikationsdaten,
- Kommunikationsinhalte,
- Dateien und Medien,
- technische Metadaten,

- Authentifizierungsdaten,
- Logdaten,
- Sicherheitsdaten,
- Supportdaten,
- Push-Token,
- Geräteinformationen.

4. Kategorien betroffener Personen

- Benutzer,
- Administratoren,
- Mitarbeiter des Mandanten,
- Kunden des Mandanten,
- Dienstleister des Mandanten,
- Kommunikationspartner,
- Benutzer anderer Domains,
- Ansprechpartner,
- Supportkontakte,
- sonstige Personen, deren Daten in Croco verarbeitet werden.

5. Dauer der Verarbeitung

Für die Dauer des Vertrags über die Nutzung von Croco.

Nach Vertragsende Löschung oder Anonymisierung spätestens nach 180 Tagen, sofern keine gesetzlichen Aufbewahrungspflichten, berechtigten Interessen oder abweichenden Vereinbarungen entgegenstehen.

Anlage 2 – Technische und organisatorische Maßnahmen

1. Zutrittskontrolle

Maßnahmen zur Verhinderung unbefugten physischen Zutritts zu Systemen, mit denen personenbezogene Daten verarbeitet werden.

Mögliche Maßnahmen:

- Betrieb in professioneller Rechenzentrumsumgebung,
- physische Zutrittskontrollen des Rechenzentrumsbetreibers,
- beschränkter Zugang zu Server- und Betriebsumgebungen,
- dokumentierte Verantwortlichkeiten.

2. Zugangskontrolle

Maßnahmen zur Verhinderung unbefugter Nutzung von Systemen.

Mögliche Maßnahmen:

- Benutzerkonten,
- Authentifizierung,
- rollenbasierte Zugriffskontrolle,
- Administratorberechtigungen nur für berechtigte Personen,
- Schutz administrativer Zugänge,
- Protokollierung sicherheitsrelevanter Ereignisse,
- Deaktivierung nicht mehr benötigter Zugänge.

3. Zugriffskontrolle

Maßnahmen, die sicherstellen, dass berechtigte Benutzer nur auf Daten zugreifen können, für die sie berechtigt sind.

Mögliche Maßnahmen:

- Mandantenmodell,
- Domaintrennung,
- Kommunikationskontexte,
- Rollen und Berechtigungen,
- Kontextbezogene Zugriffsbeschränkungen,
- keine allgemeine zentrale Lesefunktion für beliebige Kommunikationsinhalte,
- Trennung von Mandantendaten.

4. Weitergabekontrolle

Maßnahmen zur Kontrolle der Übermittlung personenbezogener Daten.

Mögliche Maßnahmen:

- verschlüsselte Übertragungswege,
- Zugriffsbeschränkungen,
- kontrollierte domainübergreifende Kommunikation,
- Kontaktanfragen zwischen Domains,
- Einsatz vertraglich gebundener Unterauftragsverarbeiter,
- Dokumentation eingesetzter Dienste.

5. Eingabekontrolle

Maßnahmen zur Nachvollziehbarkeit von Eingaben, Änderungen oder Löschungen, soweit technisch vorgesehen.

Mögliche Maßnahmen:

- Zeitstempel,
- Benutzerzuordnung,
- technische Protokolle,

- Änderungsinformationen,
- Sicherheitslogs,
- Systemereignisse.

6. Auftragskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten nur entsprechend Weisung verarbeitet werden.

Mögliche Maßnahmen:

- AVV,
- dokumentierte Weisungen,
- rollenbasierte Verarbeitung,
- interne Berechtigungsbeschränkung,
- Verpflichtung von Unterauftragsverarbeitern,
- Vertraulichkeitsverpflichtungen.

7. Verfügbarkeitskontrolle

Maßnahmen zum Schutz gegen zufällige Zerstörung oder Verlust.

Mögliche Maßnahmen:

- Backups zum Systemschutz,
- Wartung und Sicherheitsupdates,
- technische Überwachung,
- Fehleranalyse,
- Wiederherstellungsmaßnahmen für den Systembetrieb,
- Schutz vor Missbrauch und Angriffen.

8. Trennungsgebot

Maßnahmen zur getrennten Verarbeitung von Daten unterschiedlicher Mandanten.

Mögliche Maßnahmen:

- Mandantenbasierte Datenstruktur,
- Domainbasierte Kommunikationseinheiten,
- Zugriffsbeschränkungen,
- Rollen- und Berechtigungssystem,
- logische Trennung von Kundendaten.

9. Datenschutzfreundliche Voreinstellungen

Mögliche Maßnahmen:

- beschränkte Standardberechtigungen,
- kontextbezogene Teilnahme,

- kontrollierte domainübergreifende Kommunikation,
- datensparsame Push-Benachrichtigungen, soweit konfiguriert,
- Zugriff nur für berechtigte Teilnehmer.

10. Regelmäßige Überprüfung

CrossLink überprüft und verbessert technische und organisatorische Maßnahmen nach eigenem Ermessen und entsprechend technischer, organisatorischer und sicherheitsbezogener Anforderungen.

Anlage 3 – Unterauftragsverarbeiter

Zum Zeitpunkt dieser Fassung sind insbesondere folgende Unterauftragsverarbeiter bzw. Dienste relevant:

Anbieter	Zweck	Mögliche Datenkategorien	Sitz / Verarbeitung
Infomaniak Network SA	Rechenzentrums- und Infrastrukturumgebung für den selbst betriebenen Croco-Dienst	Kundendaten, Kommunikationsdaten, Dateien, technische Daten, Logdaten	Schweiz
Google Ireland Limited / Google LLC	Firebase Cloud Messaging für Android-Push-Benachrichtigungen	Push-Token, Geräteinformationen, App-Informationen, Zustellinformationen, ggf. Inhalte von Push-Benachrichtigungen	EU / USA / global, abhängig von Google-Verarbeitung
Apple Distribution International Ltd. / Apple Inc.	Apple Push Notification service für iOS-Push-Benachrichtigungen	Push-Token, Geräteinformationen, App-Informationen, Zustellinformationen, ggf. Inhalte von Push-Benachrichtigungen	EU / USA / global, abhängig von Apple-Verarbeitung

CrossLink kann diese Liste aktualisieren, wenn neue Unterauftragsverarbeiter eingesetzt oder bestehende ersetzt werden.

Anlage 4 – Weisungen des Mandanten

Als dokumentierte Weisungen des Mandanten gelten insbesondere:

- Abschluss dieses AVV,
- Abschluss des Vertrags über Croco,
- Nutzung der Plattformfunktionen,
- Einrichtung von Mandanten, Domains und Benutzern,
- Vergabe von Rollen und Berechtigungen,
- Erstellung von Kommunikationskontexten,
- Upload und Löschung von Daten,
- Freigabe domainübergreifender Kommunikation,
- Nutzung von Exportfunktionen,

- Supportanfragen,
- schriftliche oder elektronische Weisungen des Mandanten.

Weisungen müssen eindeutig, rechtmäßig und durch eine berechtigte Person erteilt werden.

Anlage 5 – Löschung und Rückgabe

Nach Vertragsende kann der Mandant Kundendaten exportieren, soweit Croco entsprechende Exportfunktionen bereitstellt.

CrossLink löscht oder anonymisiert Kundendaten spätestens 180 Tage nach Vertragsende, sofern keine gesetzlichen Aufbewahrungspflichten, berechtigten Interessen oder abweichenden Vereinbarungen entgegenstehen.

Backups werden nach Maßgabe technischer Backup-Zyklen überschrieben oder gelöscht.

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

Eine individuelle Wiederherstellung oder Migration von Daten wird nur geschuldet, wenn dies ausdrücklich vereinbart wurde.