Vereinbarung zur Auftragsverarbeitung

zwischen der

Crismo GmbH

Prenzlauer Allee 186, 10405 Berlin, Deutschland

(im Folgenden: „Auftragsverarbeiter“)

und

Kunde

Adresse

(im Folgenden: „Verantwortlicher“)

(beide nachfolgend gemeinsam „Parteien“)

Hintergrund und Zweck der Vereinbarung

Diese Vereinbarung wird hinsichtlich der Nutzung von Crismo-Produkten (SaaS Variante) auf Grundlage von separate(n) Softwarenutzungsvereinbarung(en) (jeweils einzeln oder gemeinsam im Folgenden als „Hauptvertrag“ bezeichnet) geschlossen. Die Parteien sind mit dem Hauptvertrag ein Auftragsverarbeitungsverhältnis gemäß Art. 28 DSGVO eingegangen. Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis nach geltendem Recht zu konkretisieren, schließen die Parteien die nachfolgende Vereinbarung im Angesicht der Tatsache, dass der Verantwortliche laut Art. 4 Z. 7 DSGVO und der Auftragsverarbeiter laut Art. 4 Z. 8 DSGVO definiert sind.

1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand des Hauptvertrages sind und bei deren Verrichtung personenbezogene Daten durch den Auftragsverarbeiter oder einen Subunternehmer verarbeitet werden, nachdem sie zuvor vom Verantwortlichen in jedweder Form an den Auftragsverarbeiter übermittelt wurden (diese Art personenbezogener Daten wird im Nachfolgenden als „Daten“ bezeichnet). Diese Vereinbarung samt Anhängen gilt ausdrücklich nicht für den Fall, dass der Verantwortliche den Auftragsverarbeiter anweist, seine Daten auf Servern außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (EWR) zu speichern. Für eine solche Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums bedarf es einer gesonderten schriftlichen Vereinbarung zwischen den Parteien. Die optionale Nutzung der KI-Funktion „Crismo AI“ durch den Verantwortlichen wird hiervon nicht berührt und richtet sich nach Anhang 3.

2 Gegenstand, Dauer und Zweck der Verarbeitung

(1) Der Gegenstand und die Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten sind im Hauptvertrag dargelegt.

(2) Folgende Datenarten oder -kategorien sind Gegenstand der Erhebung, Verarbeitung und/oder Nutzung durch den Auftragsverarbeiter: Nutzerdaten (Name, Vorname, vollständige Anschrift, E-Mail-Adresse, Unternehmensbezeichnung), Zugangs- und Authentifizierungsdaten (z. B. Benutzername, gehashtes Passwort, Single-Sign-On-Anmeldedaten), IP-Adresse des Zugriffs, Geschäftsprozessdiagramme / Organigramme / Diagramme samt erweiterter Attribute, Kommentierungen der Geschäftsprozessdiagramme/Organigramme/Diagramme, Inhalte beliebiger durch den Verantwortlichen freiwillig übermittelter Daten, Workflow-Statusinformationen, Prozess-Logdaten inklusive enthaltener Geschäftsdaten.

(3) Der Kreis, der durch den Umgang mit ihren Daten Betroffenen, umfasst: Verantwortlichenseite: Anwender des Systems (Modellierungsnutzer, eingeladene Personen, Hub-Nutzer), ggf. weitere Personen, deren Daten in den Nutzdaten enthalten sind (Geschäftsprozessdiagramme/Organigramme/Workflows, Dateien, übermittelte Prozess-Logdaten inklusive enthaltener Geschäftsdaten).

(4) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO ist nicht Gegenstand dieser Vereinbarung. Der Verantwortliche stellt sicher, dass er im Rahmen der Nutzung der Crismo-Produkte keine derartigen Daten überträgt, es sei denn, die Parteien vereinbaren dies gesondert in Textform.

3 Verantwortlichkeiten der Parteien und Weisungsbefugnis

(1) Der Verantwortliche ist insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter verantwortlich. Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen.

(2) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten. Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete Anordnung des Verantwortlichen in Textform. Die Weisungen werden zunächst durch den Hauptvertrag definiert und können durch den Verantwortlichen in weiterer Folge durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(3) Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(4) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

(5) Auskünfte an Dritte oder an den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Zustimmung in Textform durch den Verantwortlichen erteilen. Soweit ein Betroffener sich zwecks Ausübung seiner Rechte (insbesondere Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch) unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner

Möglichkeiten und in angemessenem Umfang durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Personen.

(6) Der Auftragsverarbeiter unterstützt in einem angemessenen Umfang den Verantwortlichen bei der Erfüllung seiner Pflichten nach Art. 32 bis 36 DSGVO, insbesondere umfasst dies die Unterstützung bei der Datenschutz-Folgenabschätzung. Für Unterstützungsleistungen, die nicht im Hauptvertrag enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

(7) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet grundsätzlich in Mitgliedsstaaten der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Hiervon unberührt bleibt ein im Einzelfall erforderlicher, eng begrenzter Zugriff durch Support- oder Wartungspersonal eines Subunternehmers aus einem Drittstaat (z. B. zur kurzfristigen Störungsbehebung), sofern hierfür geeignete Garantien im Sinne von Art. 46 DSGVO (insbesondere EU-Standardvertragsklauseln) vereinbart sind und der Zugriff auf das zur Aufgabenerfüllung erforderliche Minimum beschränkt bleibt. Eine darüberhinausgehende Verlagerung der Verarbeitung in einen anderen Staat bedarf der vorherigen Zustimmung des Verantwortlichen. Die optionale Nutzung der KI-Funktion „Crismo AI“ richtet sich abweichend hiervon nach Anhang 3.

(8) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(9) Der Auftragsverarbeiter hat, entsprechend der gesetzlichen Vorgaben, einen Datenschutzbeauftragten zu bestellen, der mit der Ausübung der einschlägigen Aufgaben betraut ist. Der Datenschutzbeauftragte des Auftragsverarbeiters ist unter der E-Mail-Adresse contact@crismo.io zu erreichen.

(10) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden, sofern sie sich auf dieses Auftragsverarbeitungsverhältnis beziehen.

4 Sicherheitsmaßnahmen und Kontrollrechte

(1) Die Parteien vereinbaren die in Anhang 1 zu dieser Vereinbarung definierten technischen und organisatorischen Maßnahmen gemäß Art. 28 (3) lit. c) DSGVO, in Verbindung mit Art. 32 DSGVO. Soweit der Verantwortliche die optionale KI-Funktion „Crismo AI“ nutzt, gelten ergänzend die in Anhang 3 genannten Maßnahmen.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang 1 festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Sofern hierfür eine Überprüfung erforderlich ist, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer, welcher in keinem direkten oder indirekten Konkurrenzverhältnis zum Auftragsverarbeiter steht, in dessen Geschäftsbetrieb

durchgeführt wird, wird diese vom Auftragsverarbeiter ermöglicht und deren Durchführung in angemessenem Umfang unterstützt, wobei darauf zu achten ist, dass die Störung des Geschäftsbetriebs des Auftragsverarbeiters durch die Überprüfung auf das nötige Minimum beschränkt bleibt. Der Nachweis der Umsetzung geeigneter Maßnahmen ersetzt vorgenannte Überprüfung, sofern die Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragte, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht wird.

(4) Die in Absatz (3) genannte Überprüfung kann jederzeit nach vorheriger terminlicher Absprache mit dem Auftragsverarbeiter zu den üblichen Geschäftszeiten durchgeführt werden, jedoch nicht öfter als einmal pro Jahr, sofern kein Verdacht auf eine Verletzung dieser Vereinbarung besteht.

5 Mitteilung bei Verstößen durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, bei tatsächlichen Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Die Unterrichtung erfolgt unverzüglich, in der Regel innerhalb von 48 Stunden nach Bekanntwerden des Vorfalls, damit der Verantwortliche etwaige gesetzliche Meldefristen, insbesondere nach Art. 33 DSGVO, einhalten kann.

(2) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

6 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher, nach Aufforderung des Verantwortlichen, jedoch spätestens mit Beendigung des Hauptvertrages, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Gleichermaßen können Sicherheitskopien auch länger als entsprechend der in Absatz (2) genannten Fristen vorgehalten werden, wenn deren Löschung außerhalb der routinemäßigen Löschzyklen einen unverhältnismäßigen Aufwand für den Auftragsverarbeiter bedeuten würde. Jedenfalls darf die Vorhaltezeit von Sicherheitskopien nach Ende des Hauptvertrages einen Zeitraum von 6 (sechs) Monaten nicht überschreiten.

7 Subunternehmer

(1) Zusätzlich zu den in Anhang 2 genannten, wird der Auftragsverarbeiter keine Dritten zur Datenverarbeitung („Subunternehmer“) ohne die vorherige schriftliche Genehmigung des Verantwortlichen hinzuziehen. Die Hinzuziehung des in Anhang 3 genannten Subunternehmers für die optionale KI-Funktion „Crismo AI“ richtet sich nach Anhang 3. Ungeachtet dessen genehmigt der Verantwortliche die Hinzuziehung neuer Subunternehmer, sofern

a) der Auftragsverarbeiter den Verantwortlichen mindestens 30 (dreißig) Tage im Voraus über solche Subunternehmer in Kenntnis setzt;

b) der Auftragsverarbeiter sicherstellt, dass seine vertraglichen Vereinbarungen mit solchen Subunternehmern derart gestaltet sind, dass das Datenschutzniveau mindestens der vorliegenden Vereinbarung zur Auftragsverarbeitung entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden, insbesondere im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung; und

c) solche Subunternehmer die vertraglich vereinbarte Datenverarbeitung grundsätzlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vornehmen; ein im Einzelfall erforderlicher, eng begrenzter Zugriff aus einem Drittstaat (insbesondere zu Support- oder Wartungszwecken) ist zulässig, sofern hierfür geeignete Garantien im Sinne von Art. 46 DSGVO vereinbart sind.

Werden die vorstehenden Bestimmungen a) bis c) nicht erfüllt, kann der Verantwortliche gegen die Hinzuziehung neuer Subunternehmen binnen 14 (vierzehn) Tagen nach Erhalt der in a) beschriebenen Benachrichtigung Einspruch erheben. Die Parteien werden sich in diesem Fall um eine einvernehmliche Lösung bemühen. Kommt innerhalb von weiteren 30 (dreißig) Tagen keine Einigung zustande, ist der Verantwortliche berechtigt, denjenigen Teil des Hauptvertrages, dessen Erbringung die Nutzung des betreffenden Subunternehmens voraussetzt, mit einer Frist von 30 (dreißig) Tagen zum Monatsende zu kündigen.

(2) Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikations- und Wartungsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Hinsichtlich der Überprüfungsrechte des Verantwortlichen gegenüber Subunternehmen hat der Auftragsverarbeiter vertraglich mit dem Subunternehmen sicherzustellen, dass die Anforderungen aus Abschnitt 4 (3) dieser Vereinbarung im selben Umfang gelten.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

(5) Sofern die vertragsgegenständliche Crismo Software Funktionalitäten beinhaltet, die auf Diensten von Dritten basieren und diese vom Verantwortlichen nach eigenem Ermessen aktiviert werden können, wird im Falle der Nutzung dieser Funktionalitäten ausschließlich der jeweilige Dritte zum Vertragspartner des Verantwortlichen, keinesfalls jedoch der Auftragsverarbeiter. Diesfalls gelten allein die Nutzungsbedingungen sowie Datenschutzbestimmungen des Dritten. Die vorliegende Vereinbarung zur Auftragsvereinbarung gilt nicht für die Nutzung dieser Funktionalitäten durch den Verantwortlichen.

8 Sonstige Bestimmungen

(1) Sofern in dieser Vereinbarung nicht anders vorgesehen, reicht die Textform (E-Mail) als Formerfordernis für alle Erklärungen, insbesondere Mitteilungen. Änderungen und Ergänzungen dieser Vereinbarung bedürfen ebenfalls der Textform (E-Mail).

(2) Die drei Anhänge „Technisch-organisatorische Maßnahmen“, „Bestehende Subunternehmerverhältnisse“ und „Crismo AI (optional)“ sind Bestandteile dieser Vereinbarung.

(3) Diese Vereinbarung zur Auftragsverarbeitung ersetzt zuvor gegebenenfalls zwischen den Parteien geschlossene Vereinbarungen zur Auftragsdatenverarbeitung nach § 11 BDSG im Ganzen.

(4) Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag hat diese Vereinbarung in datenschutzrechtlichen Belangen Vorrang.

(5) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

9 Unterschriften

Diese Vereinbarung zur Auftragsverarbeitung wird von den Parteien bzw. deren ordnungsgemäß bevollmächtigten Vertretern zu dem/den nachstehend genannten Datum/Daten unterzeichnet.

Crismo GmbH	**Kunde**
Ort, Datum:	Ort, Datum:
Unterschrift:	Unterschrift:
Name (in Druckschrift):	Name (in Druckschrift):
Position/Titel:	Position/Titel:

Anhang 1 – Technische und organisatorische Maßnahmen (TOMs)

A. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

A.1 Zutritts- und Zugangskontrolle

Der physische und logische Zugang zu den Systemen des Auftragsverarbeiters ist wie folgt abgesichert:

– Rechenzentren für Produktions- und Backupsysteme verfügen über zeitgemäße physische Zugangsschutzmechanismen, u. a. Wachschutz, Videoüberwachung und elektronische Zugangssysteme inkl. Protokollierung.

– Datenträger sind auf Datenträgerebene mit sicheren, dem Stand der Technik entsprechenden Passwörtern und zeitgemäßen Verschlüsselungsverfahren verschlüsselt; Rechenzentrumsmitarbeiter mit Hardwarezugriff haben dadurch keinen Zugriff auf die Daten selbst und kennen auch keine Zugangsdaten zu den durch den Auftragsverarbeiter betriebenen Systemen.

– Für den administrativen Zugriff werden ausschließlich Passwörter mit einer Mindestlänge von 20 Zeichen sowie gesicherte Verbindungen (mindestens SSH, 2048 Bit oder gleichwertig) verwendet; Systempasswörter werden alle zwölf Monate aus Sicherheitsgründen geändert, für die administrative Verbindung zu den Servern ist zusätzlich ein zweiter Faktor erforderlich.

– Die für die SaaS-Lösungen verwendeten öffentlichen IP-Adressen erlauben ausschließlich den Zugriff über die Anwendungsprotokolle HTTP, HTTPS und SMTP.

A.2 Zugriffskontrolle

Der Zugriff auf Daten und Systeme ist nach dem Need-to-know- und Least-Privilege-Prinzip beschränkt:

– Zugriffsrechte werden ausschließlich auf Basis der jeweiligen Job-Verantwortlichkeiten vergeben; der Zugriff auf die Administrationsoberfläche für Support-Mitarbeiter ist durch eine zweifache Authentifizierung (HTTP- und Applikationsebene) sowie eine gesicherte Verbindung geschützt. Alle Mitarbeiter mit Datenzugriff werden im Umgang mit den Daten geschult.

– Autorisierungen werden nur auf Basis gültiger Nutzername-/Passwort-Kombinationen oder vom Verantwortlichen explizit erstellter Authentifizierungsschlüssel (z. B. per Freigabe-Funktion oder Zertifikat) erteilt. Passwörter werden ausschließlich verschlüsselt (aktueller Hash-Algorithmus + Salt) gespeichert, sodass sie – auch für Mitarbeiter des Auftragsverarbeiters – in keiner lesbaren Form einsehbar sind. Auf Wunsch des Verantwortlichen kann zusätzlich eine Single-Sign-on-Integration aktiviert werden.

– Die Weitergabe von Informationen aus den Rechenzentren an Dritte bedarf stets der Zustimmung des Auftragsverarbeiters, soweit nicht zwingendes Recht etwas anderes bestimmt.

– Backups werden nach aktuellen Industriestandards mit sicherer Schlüssellänge asymmetrisch verschlüsselt, örtlich getrennt gespeichert und nur stark eingeschränkt zugänglich gemacht; die Schlüssel werden physisch getrennt aufbewahrt.

A.3 Trennungskontrolle

Die Trennung der Daten verschiedener Kunden ist wie folgt sichergestellt:

– Die Software-Architektur folgt einem Multi-Tenant-Konzept: Jeder Kunde erhält einen vollständig von allen anderen Kunden getrennten Arbeitsbereich („Tenant“), was technisch durch ein globales Berechtigungssystem für sämtliche Repository-Objekte und Nutzerdaten abgebildet wird – dies gilt entsprechend, sofern ein Kunde mehrere Arbeitsbereiche zu unterschiedlichen Zwecken nutzt.

– Jeder Kunde erhält einen abgeschlossenen Bereich, auf den ausschließlich von ihm autorisierte Nutzer zugreifen können. Der Auftragsverarbeiter selbst greift zu keinem Zeitpunkt auf die Daten eines Arbeitsbereichs zu, es sei denn, der Verantwortliche autorisiert im Rahmen eines Support-Falls eigenständig und zeitlich begrenzt einen Mitarbeiter des Auftragsverarbeiters.

– Sämtliche im Crismo-Repository abgelegten Objekte und Artefakte – einschließlich serverseitig erzeugter Cache-Kopien wie Diagramm-Vorschaugrafiken – unterliegen einem durchgängigen, systembedingt nicht umgehbaren Berechtigungssystem.

– Die einzige Möglichkeit, dieses Berechtigungssystem zu umgehen, wäre ein direkter Zugriff auf die lokal gehaltene Datenbank. Ein solcher Zugriff ist ausschließlich den Hauptverantwortlichen (oder deren Vertretern) für den technischen Betrieb und die Wartung der Produktivsysteme möglich; diese sind verpflichtet, außerhalb von Wartungszwecken keinen Zugriff auf die Daten zu nehmen.

B. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

B.1 Weitergabekontrolle

Die Integrität der Daten bei Übertragung und Weitergabe wird wie folgt sichergestellt:

– Die Weitergabe von Informationen aus den Rechenzentren an Dritte bedarf der Zustimmung des Auftragsverarbeiters.

– Der Zugriff auf die Dienste des Auftragsverarbeiters ist generell nur über eine Anmeldung auf Benutzerebene möglich; ohne diese kann auf keine Daten zugegriffen werden. Der Zugriff per API ist ebenfalls nur per Benutzeranmeldung oder einem vom Benutzer verwalteten API-Schlüssel möglich – dies gilt auch für Mitarbeiter des Auftragsverarbeiters und Servicetechniker. Gegen automatisierte Angriffe bestehen Schutzmaßnahmen (u. a. Brute-Force-Protection).

– Der clientseitige Zugriff auf die Cloud-Systeme ist nach Industriestandards mit aktuellen Algorithmen (AES-256 Bit und PFS oder gleichwertig) abgesichert und verschlüsselt. Aktualität und Sicherheit der eingesetzten Algorithmen und Technologien werden regelmäßig überprüft und bei bekannten Sicherheitsproblemen angepasst; eine Verschlechterung des Sicherheitsniveaus ist ausgeschlossen.

– Der administrative Zugriff ist unter Abschnitt A.1 (Zutritts- und Zugangskontrolle) beschrieben; hier kommen konsequent verschlüsselte Verbindungen nach Industriestandards sowie ein zweiter Faktor für die Authentifizierung zum Einsatz.

– Werden Daten vom Verantwortlichen an Crismo übergeben, hat der Verantwortliche für einen ausreichenden Schutz bei der Übertragung zu sorgen (z. B. verschlüsselte Archive mit telefonisch übermitteltem Passwort). Der Auftragsverarbeiter stellt hierfür einen gesicherten elektronischen Übergabeort bereit; empfohlen wird eine Verschlüsselung mit mindestens 256 Bit AES. Die Übergabe physischer Datenträger ist nicht vorgesehen.

B.2 Eingabekontrolle

Eingabe-, Änderungs- und Löschoperationen werden anwendungsseitig nicht abschaltbar und nicht umgehbar protokolliert; der Verantwortliche kann auf Anfrage Einsicht in das erzeugte Protokoll erhalten. Aus technischen Gründen kann eine Protokoll-Historie nur für die jeweils letzten 12 Monate zugesichert werden.

C. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

C.1 Verfügbarkeitskontrolle

Die Verfügbarkeit und Belastbarkeit der Systeme wird u. a. durch folgende Maßnahmen sichergestellt:

– Sämtliche Daten werden in einem Intervall von drei Stunden (oder kürzer) auf örtlich getrennte Backup-Server gesichert; vor der Übertragung kommt ein asynchrones Verschlüsselungsverfahren auf Basis aktueller Industriestandards direkt auf den Daten zum Einsatz.

– Für eine Entschlüsselung im Disaster-Recovery-Fall ist ein gesonderter, unter physischem Verschluss mehrfach vorgehaltener privater Schlüssel erforderlich.

– Zusätzlich zur Datei-Verschlüsselung erfolgt die Übertragung auf den örtlich verteilten Backup-Server über eine verschlüsselte Leitung nach aktuellen Industriestandards; sämtliche Schlüssel haben eine Mindestlänge von 20 Zeichen.

– Auf den Servern kommen generell eine Antivirus-/Antimalware-Lösung sowie ein Rootkitschutz zum Einsatz.

– Zur Sicherung der Datenintegrität und zur Vermeidung von Datenverlust werden auf den Serversystemen generell redundante RAID-Speichersysteme oder gleichwertige Lösungen eingesetzt.

– Die gesamte Softwareentwicklung einschließlich Fehlerbeseitigung unterliegt einem Qualitätssicherungsprozess mit systematischem Testing; automatisierte Tests prüfen insbesondere, ob veränderte oder neue Komponenten innerhalb der erwarteten Parameter arbeiten.

D. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Der Auftragsverarbeiter setzt, soweit möglich, Pseudonymisierung als technische Maßnahme ein:

– Innerhalb der Cloud-Umgebung erfolgt aus Sicherheits- und Wartungsgründen ein Logging. Sämtliche Nutzerdaten werden dabei pseudonymisiert, sofern die sicherheitstechnischen Maßnahmen dem nicht entgegenstehen – beispielsweise werden bei der Überwachung der Authentifizierung E-Mail-Adressen zur Angriffserkennung benötigt. Der Zugriff auf Logs ist zweckgebunden und auf einen explizit autorisierten Personenkreis beschränkt.

– Personenbezogene Daten, die der Verantwortliche in Crismo-Systemen hochlädt, müssen unter Umständen vom Verantwortlichen selbst pseudonymisiert werden.

E. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

E.1 Bewertung und Evaluierung

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig überprüft:

– Die Systeme des Auftragsverarbeiters werden quartalsweise durch Vulnerability-Scanner untersucht und regelmäßig externen Penetrationstests unterzogen; die Ergebnisse fließen direkt in den Entwicklungsprozess ein, notwendige Anpassungen werden umgehend vorgenommen.

– Vom Auftragsverarbeiter verwendete Rechenzentren unterliegen regelmäßigen Überprüfungen durch deren jeweilige IT-Sicherheitsabteilung.

E.2 Auftragskontrolle

Die zweckgebundene Verarbeitung im Auftrag wird wie folgt sichergestellt:

– Der Verantwortliche beauftragt den Auftragsverarbeiter ausschließlich mit dem Hosting und Betrieb des im Hauptvertrag vereinbarten Produkts; der Auftragsverarbeiter sichert zu, die Daten nicht zu anderen als den dort festgelegten Zwecken zu verarbeiten.

– Die betroffenen Mitarbeiter des Auftragsverarbeiters sowie die einbezogenen Subunternehmer sind hinsichtlich des Zweckbezugs und der Weisungen des Auftraggebers instruiert und entsprechend verpflichtet.

– Ausnahmen bedürfen ggf. der Genehmigung durch den Verantwortlichen.

Anhang 2 – „Bestehende Subunternehmerverhältnisse“

Subunternehmer	Dienstleistung	Standort / Rechenzentren	Rechtsgrundlage
Google Cloud EMEA Ltd / Google Ireland Ltd (Firebase / Google Cloud Platform)	Bereitstellung von Server- und Speicherinfrastruktur für den Plattformbetrieb (Rechenzentrumsdienstleistungen)	EU (Belgien, Niederlande, Finnland)	Google Cloud DPA + EU-Standardvertragsklauseln
Mixpanel, Inc.	Analyse der Produktnutzung (pseudonymisierte Ereignis-/Nutzungsdaten); Datenübertragung über EU-Endpunkt api-eu.mixpanel.com	EU-Endpunkt (Unternehmen mit Hauptsitz in den USA)	EU-Standardvertragsklauseln / EU-U.S. Data Privacy Framework

Hinweis: Die für die SaaS-Lösung des Auftragsverarbeiters verwendeten Rechenzentren befinden sich innerhalb der EU (Belgien, Niederlande, Finnland).

Anhang 3 – „Crismo AI (optional)“

(1) Dieser Anhang gilt ausschließlich für die optionale KI-Funktion „Crismo AI“ (Claude-Integration) und nur, soweit und solange der Verantwortliche diese Funktion aktiv nutzt. Nutzt der Verantwortliche diese Funktion nicht, finden dieser Anhang und die nachfolgenden Regelungen auf ihn keine Anwendung; insbesondere kommt der in diesem Anhang genannte Subunternehmer für ihn nicht zur Anwendung.

(2) Für die Erbringung der KI-Funktion „Crismo AI“ zieht der Auftragsverarbeiter den nachfolgenden Subunternehmer hinzu:

Subunternehmer	Dienstleistung	Standort / Rechenzentren	Rechtsgrundlage
Anthropic, PBC	Bereitstellung der KI-Modell-Funktionalität für die optionale KI-Funktion „Crismo AI“ (Verarbeitung von Nutzereingaben und -ausgaben durch Claude)	USA	EU-Standardvertragsklauseln (Modul 2/3, Durchführungsbeschluss (EU) 2021/914)

(3) Für die Verarbeitung im Rahmen von „Crismo AI“ gelten ergänzend zu Anhang 1 die folgenden Maßnahmen:

– Übertragungssicherheit: Die Übermittlung von Eingaben und Ausgaben zwischen der Crismo-Plattform und Claude (Anthropic) erfolgt ausschließlich über eine TLS-verschlüsselte Verbindung nach dem Stand der Technik.

– Datenminimierung: An Claude werden ausschließlich die Daten übermittelt, die für die jeweils genutzte Crismo-AI-Funktion tatsächlich erforderlich sind; ein darüberhinausgehender Datenexport findet nicht statt.

– Zugriffskontrolle: Die Auslösung von Crismo-AI-Funktionen unterliegt denselben Berechtigungs- und Zugriffskontrollen wie die übrige Nutzung der Crismo-Plattform gemäß Anhang 1, Abschnitt A.2; nur hierfür autorisierte Nutzer können die Funktion aktivieren.

– Aufbewahrung bei Anthropic: Eingaben und Ausgaben werden bei Anthropic entsprechend der jeweils aktuellen Standard-Aufbewahrungsfrist von Anthropic für die genutzte Schnittstelle gespeichert, sofern nicht eine Zero-Data-Retention-Konfiguration vereinbart ist; die jeweils aktuelle Frist ist der Dokumentation von Anthropic zu entnehmen.

– Kein Training auf Kundendaten: Anthropic nutzt die über die API übermittelten Daten nach den geltenden Anthropic-Nutzungsbedingungen standardmäßig nicht zum Training eigener KI-Modelle. Auf Anfrage kann für den Verantwortlichen eine Zero-Data-Retention-Konfiguration mit entsprechend verkürzten Aufbewahrungsfristen vereinbart werden.

– Umgang mit Ausgaben: Von Claude erzeugte Ausgaben, die der Verantwortliche innerhalb der Crismo-Plattform speichert (z. B. in einem Diagramm oder Workflow), werden ab diesem Zeitpunkt wieder als gewöhnliche, durch den Auftragsverarbeiter verarbeitete Daten behandelt und unterliegen den allgemeinen Maßnahmen aus Anhang 1.

(4) Jede Änderung des in diesem Anhang genannten Subunternehmers erfolgt nach den in Abschnitt 7 dieser Vereinbarung genannten Voraussetzungen und Verfahren (Vorankündigung, Einspruchsrecht, Kündigungsrecht).