Vereinbarung über eine Auftragsverarbeitung

Art. 28 Abs. 3 DSGVO · ILMENO Agent Sync · Vorlage Version 1.0 · Stand: 3. November 2026

abgeschlossen zwischen

dem **Verantwortlichen**
[Name bzw. Firma]
[Anschrift]
[E-Mail für Mitteilungen nach dieser Vereinbarung]
(im Folgenden „Auftraggeber“)

und

dem **Auftragsverarbeiter**
CROPT GmbH, Ursprungweg 42b, 8045 Graz, Österreich
FN 572509a · ATU77768845 · vertreten durch den Geschäftsführer Martin Schmeisser
office@ilmeno.com
(im Folgenden „Auftragnehmer“)

1. Gegenstand der Vereinbarung

1.1 Gegenstand der Auftragsverarbeitung ist der Betrieb der optionalen Server-Funktion **„Agent Sync“** der iOS-App ILMENO für den Auftraggeber: Die App des Auftraggebers lädt auf dessen ausdrückliche Aktivierung hin einen Spiegel seiner offenen Aufgaben auf den Server `api.ilmeno.com`, damit ein vom Auftraggeber beauftragter Software-Agent diese über eine Schnittstelle lesen, neue Aufgaben einstellen und bestehende als erledigt markieren kann. Der Auftragnehmer speichert diese Daten und stellt sie der App und dem Agenten des Auftraggebers bereit; er wertet sie nicht aus. Spiegel und Agent-Einträge sind Ende-zu-Ende verschlüsselt (Anlage ./1); der Auftragnehmer hält den Schlüssel nicht und kann die Inhalte nicht lesen.

1.2 Diese Vereinbarung ist als Ergänzung zu den Nutzungsbedingungen von ILMENO und der Datenschutzerklärung zu verstehen und geht ihnen für die hier geregelte Verarbeitung vor.

1.3 Folgende Datenkategorien unterliegen der Auftragsverarbeitung:

- **Aufgabeninhalte** des Auftraggebers: Titel, erster Schritt, Schritte, Notizen/Inhalt, Bereich, Tags, Fristen, Wiederholungsregeln, Zeitpräferenzen, Status, Zeitstempel — als Freitext des Auftraggebers, der personenbezogene Daten Dritter enthalten kann (etwa Namen von Kunden, Auftrags- und Terminangaben);
- **Tag-Vokabular** des Auftraggebers (Namen, Beschreibungen, Farben seiner Bereiche und Tags);
- **technische Daten**: IP-Adresse des Geräts bzw. des Agenten, SHA-256-Hash des Zugangs-Tokens, Zeitstempel, Byte-Größen.

Nicht übertragen werden erledigte Aufgaben, Standortdaten, Kalender, Anhänge und Kontakte. Aufgabeninhalte und Tag-Vokabular erreichen den Auftragnehmer ausschließlich verschlüsselt; im Klartext verarbeitet er nur die technischen Daten.

1.4 Folgende Kategorien betroffener Personen unterliegen der Auftragsverarbeitung: der Auftraggeber selbst und seine Beschäftigten; Kund:innen, Interessent:innen, Lieferant:innen, Ansprechpartner:innen und sonstige Kontakte des Auftraggebers, soweit in Aufgaben genannt.

1.5 Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand. Der Auftraggeber erfasst keine Gesundheits-, Religions-, Biometrie- oder sonstigen Art.-9-Daten Dritter in Aufgaben, die über Agent Sync gespiegelt werden, oder kürzt sie so, dass kein Rückschluss möglich ist. Empfehlung zur Datensparsamkeit: Für Aufgaben mit Kundenbezug genügen in der Regel Kürzel oder Auftragsnummern; die Zuordnung bleibt im System des Auftraggebers.

2. Dauer der Vereinbarung

Die Vereinbarung ist auf unbestimmte Zeit geschlossen. Sie endet, ohne dass es einer Kündigung bedarf, wenn der Auftraggeber Agent Sync in der App dauerhaft ausschaltet oder die Nutzung von ILMENO beendet. Beide Parteien können sie außerdem jederzeit in Textform

kündigen; der Auftragnehmer kündigt nur unter Einhaltung einer Frist von einem Monat, außer aus wichtigem Grund. Punkt 3.8 (Löschung) gilt über das Ende hinaus.

3. Pflichten des Auftragnehmers

3.1 Weisungsbindung. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen des Auftraggebers. Die Weisungen sind durch diese Vereinbarung und die Bedienung der Funktion festgelegt: *Einschalten* von Agent Sync ist die Weisung zur Speicherung des Spiegels und zur Bereitstellung an den vom Auftraggeber mit Token und Schlüssel ausgestatteten Agenten; *Ausschalten* oder „Zugang erneuern" ist die Weisung zur sofortigen Löschung. Weitergehende Einzelweisungen erteilt der Auftraggeber in Textform an office@ilmeno.com. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke, insbesondere nicht zur Analyse, Profilbildung, Produktverbesserung oder zum Training von KI-Modellen. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, informiert er — sofern gesetzlich zulässig — den Auftraggeber unverzüglich und verweist die Behörde an diesen.

3.2 Vertraulichkeit. Der Auftragnehmer erklärt rechtsverbindlich, dass alle mit der Datenverarbeitung befassten Personen vor Aufnahme der Tätigkeit schriftlich zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; die Verpflichtung bleibt nach Beendigung der Tätigkeit aufrecht. Derzeit hat beim Auftragnehmer ausschließlich der Geschäftsführer im Rahmen der Serverwartung Zugang zu den Systemen.

3.3 Sicherheit der Verarbeitung. Der Auftragnehmer erklärt rechtsverbindlich, dass er die in **Anlage ./1** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO ergriffen hat. Die Maßnahmen unterliegen dem technischen Fortschritt; der Auftragnehmer darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird, und teilt wesentliche Änderungen auf Anfrage mit.

3.4 Rechte der betroffenen Personen. Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Personen nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch, automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen erfüllen kann, und übermittelt ihm die dafür notwendigen Informationen. Praktisch gilt: Auskunft, Berichtigung und Löschung einzelner Angaben nimmt

der Auftraggeber selbst in der App vor — der Server-Spiegel folgt der App beim nächsten Abgleich automatisch; die Löschung des gesamten Spiegels bewirkt er durch Ausschalten der Funktion. Darüber hinausgehende Unterstützung erbringt der Auftragnehmer auf Weisung binnen fünf Werktagen. Wird ein Antrag einer betroffenen Person an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen hält, leitet der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiter und teilt dies dem Antragsteller mit.

3.5 Unterstützung nach Art. 32 bis 36 DSGVO. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Datensicherheit, Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung betroffener Personen, Datenschutz-Folgenabschätzung, vorherige Konsultation). Diese Unterstützungspflicht umfasst jedenfalls: Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten, die den Spiegel oder die Agent-Inbox betrifft, **unverzüglich, in der Regel binnen 48 Stunden nach Kenntnis**, in Textform an die oben genannte E-Mail-Adresse mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt; fehlende Angaben reicht er nach. Als Verletzung gilt insbesondere ein unbefugter Zugriff auf den Server oder die Offenlegung der Datenbankdatei. Der Verlust eines Tokens oder Schlüssels auf Seiten des Auftraggebers oder seines Agenten ist keine vom Auftragnehmer zu meldende Verletzung; der Auftraggeber kann den Zugang jederzeit in der App erneuern, was den Spiegel löscht. Bei einer Datenschutz-Folgenabschätzung oder Konsultation stellt der Auftragnehmer die ihm vorliegenden Informationen über die Verarbeitung zur Verfügung.

3.6 Verarbeitungsverzeichnis. Der Auftragnehmer führt für die vorliegende Auftragsverarbeitung ein Verzeichnis nach Art. 30 Abs. 2 DSGVO.

3.7 Einsichtnahme und Kontrolle. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht der Einsichtnahme und Kontrolle eingeräumt, auch durch von ihm beauftragte, zur Vertraulichkeit verpflichtete Dritte. Der Auftragnehmer stellt die Informationen zur Verfügung, die zur Kontrolle der Einhaltung dieser Vereinbarung notwendig sind: die Dokumentation in Anlage ./1, die öffentliche technische Beschreibung (ilmeno.com/api, api.ilmeno.com/tools/sync-api.md) und auf Anfrage Auskünfte sowie Konfigurationsauszüge in Textform. Inspektionen der Datenverarbeitungseinrichtungen kündigt der Auftraggeber mindestens zwei Wochen vorab an; sie erfolgen grundsätzlich durch Fernzugriff auf Dokumente und Konfigurationsauszüge, da der virtuelle Server in einem Rechenzentrum des in Anlage ./2 genannten Betreibers läuft, dessen physische Sicherheit durch dessen Zertifizierungen

nachgewiesen wird. Jede Partei trägt den Aufwand einer Kontrolle selbst; für anlasslose Kontrollen über eine jährliche hinaus kann der Auftragnehmer angemessenen Aufwandsersatz verlangen.

3.8 Löschung und Rückgabe. Das Ausschalten von Agent Sync oder „Zugang erneuern“ in der App löscht Spiegel und Agent-Inbox auf dem Server sofort und unwiederbringlich. Spiegel ohne Aktualisierung seit 180 Tagen und von der App nicht abgeholte Inbox-Einträge älter als 90 Tage löscht der Server täglich automatisch. Nach Beendigung dieser Vereinbarung löscht der Auftragnehmer alle verbleibenden personenbezogenen Daten des Auftraggebers unverzüglich und bestätigt die Löschung auf Anfrage in Textform. Eine Herausgabe ist in der Regel nicht erforderlich, weil die App des Auftraggebers stets den vollständigen, maßgeblichen Datenbestand hält; verlangt der Auftraggeber sie dennoch, erhält er die Daten in dem Format, in dem der Auftragnehmer sie erhalten hat (verschlüsselte JSON-Umschläge), oder — soweit der Auftragnehmer sie lesen kann — in einem gängigen Format. Server-Protokolle (Anlage ./1) enthalten keine Inhalte und werden nach 30 Tagen gelöscht.

3.9 Hinweis auf rechtswidrige Weisungen. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Ansicht ist, eine Weisung verstoße gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Ort der Durchführung der Datenverarbeitung

Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der Europäischen Union durchgeführt, und zwar auf einem virtuellen Server im Rechenzentrum Falkenstein (Deutschland) des in Anlage ./2 genannten Betreibers. Eine Verarbeitung in einem Drittland findet nur in dem in Anlage ./2 beschriebenen Fall statt (KI-Einordnung des Titels einer vom Agenten ohne Bereich eingestellten Aufgabe durch Anthropic, USA) und nur, wenn der Auftraggeber die Cloud-KI und „KI bei Importen“ in der App eingeschaltet hat; er kann diesen Fall jederzeit in der App oder durch Anweisung seines Agenten (immer einen Bereich mitgeben) ausschließen.

5. Sub-Auftragsverarbeiter

Der Auftragnehmer ist befugt, die in **Anlage ./2** angeführten Sub-Auftragsverarbeiter (Art. 28 Abs. 2 DSGVO) heranzuziehen. Beabsichtigte Änderungen (Hinzuziehung oder Ersetzung) teilt

der Auftragnehmer dem Auftraggeber mindestens 30 Tage vor dem Wirksamwerden in Textform an die oben genannte E-Mail-Adresse mit; der Auftraggeber kann binnen dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Kommt keine Einigung zustande, kann der Auftraggeber Agent Sync beenden; die Daten werden nach Punkt 3.8 gelöscht. Der Auftragnehmer schließt mit den Sub-Auftragsverarbeitern die erforderlichen Vereinbarungen im Sinne des Art. 28 Abs. 4 DSGVO und stellt sicher, dass sie dieselben Verpflichtungen eingehen, die ihm aufgrund dieser Vereinbarung obliegen. Kommen Sub-Auftragsverarbeiter ihren Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung ihrer Pflichten. Nebenleistungen ohne Zugriff auf Inhalte (Erreichbarkeits-Überwachung durch Abruf einer Statusseite ohne personenbezogene Daten, Telekommunikation) sind keine Sub-Auftragsverarbeitung.

6. Schlussbestimmungen

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO; im Innenverhältnis haftet jede Partei für den Schaden, den sie durch eine ihr zurechenbare Verletzung dieser Vereinbarung oder der DSGVO verursacht hat. Änderungen und Ergänzungen bedürfen der Textform. Sollte eine Bestimmung unwirksam sein, bleibt die Vereinbarung im Übrigen wirksam; die Parteien ersetzen die unwirksame Bestimmung durch eine, die dem datenschutzrechtlichen Zweck am nächsten kommt. Es gilt österreichisches Recht; Gerichtsstand ist, soweit zulässig, Graz.

[Ort] , am [Datum]

Für den Auftraggeber:

.....
[Name samt Funktion im Unternehmen]

Graz, am [Datum]

Für den Auftragnehmer (CROPT GmbH):

.....
Martin Schmeisser, Geschäftsführer

Anlage ./1: Technisch-organisatorische Maßnahmen

Stand 3. November 2026, auf dem Produktivsystem geprüft. Gliederung nach dem Muster der WKO; angegeben sind die tatsächlich umgesetzten Maßnahmen.

A. Vertraulichkeit

- **Zutrittskontrolle:** Der Server ist ein virtueller Server im Rechenzentrum Falkenstein (Deutschland) der Hetzner Online GmbH; physischer Zutritt ausschließlich durch den Betreiber nach dessen ISO-27001-zertifizierten Verfahren. Der Auftragnehmer hat keinen physischen Zugang.
- **Zugangskontrolle:** Serverzugang nur per SSH mit Schlüssel (Passwort-Login deaktiviert), personalisiertes Konto; Verwaltungs-Oberflächen (Statistik, Metriken) passwortgeschützt und ohne Aufgabeninhalte; Zugangsdaten im Passwort-Manager; automatische Bildschirmsperre auf dem Arbeitsgerät.
- **Zugriffskontrolle (Schnittstelle):** Jeder Spiegel ist an einen zufälligen 256-Bit-Zugangs-Token gebunden, den die App erzeugt und nur im iOS-Schlüsselbund des Auftraggebers hält; der Server kennt ausschließlich den SHA-256-Hash. Zugriff hat nur, wer den Token vorweist. Mailboxen verschiedener Nutzer sind strikt getrennt (Zugriff ausschließlich über den Token-Hash, keine Listen-Funktion).
- **Zugriffskontrolle (System):** Die Datenbank gehört dem Dienstkonto `ilmeno`; Verzeichnis und Dateien sind nur für dieses Konto lesbar (Modus 0700/0600). Der Dienst läuft mit systemd-Härtung (`ProtectSystem=strict` , `ProtectHome` , `NoNewPrivileges` , `PrivateTmp` , eingeschränkte Adressfamilien). Berechtigungen werden jährlich überprüft.
- **Verschlüsselung der Inhalte (Ende-zu-Ende):** Spiegel und Agent-Einträge werden auf dem Gerät des Auftraggebers bzw. durch seinen Agenten mit AES-256-GCM verschlüsselt (256-Bit-Schlüssel, von der App erzeugt, nur im iOS-Schlüsselbund des Auftraggebers und bei seinem Agenten). Der Server erhält den Schlüssel zu keinem Zeitpunkt, speichert und liefert ausschließlich Chiffrat und prüft nur Form und Größe des Umschlags; unverschlüsselte Einträge weist er ab. Metadaten im Klartext: Größe, Zeitpunkte, IP-Adressen, Anzahl wartender Einträge.
- **Pseudonymisierung:** Server-Protokolle enthalten Route, gekürzten Hash der IP-Adresse, gekürzten Token-Hash und Byte-Größen — nie Inhalte, nie Klartext-Token. Aufbewahrung 30 Tage, danach automatische Löschung; kein Versand an Dritte.

- **Klassifikation:** Aufgabeninhalte gelten als vertraulich; sie werden ausschließlich verschlüsselt gespeichert und nie protokolliert.

B. Datenintegrität

- **Weitergabekontrolle:** Ausschließlich HTTPS (TLS, automatisch verwaltete Zertifikate); unverschlüsselter Zugriff ist nicht möglich. Inhalte sind zusätzlich Ende-zu-Ende verschlüsselt (A).
- **Eingabekontrolle:** Jeder Upload ersetzt den Spiegel vollständig (kein Zusammenführen auf dem Server); Agent-Einträge werden auf Form und Größe geprüft (32 KB je Eintrag, 200 offene Einträge, 2 MB je Spiegel) und erst nach Bestätigung durch die App gelöscht; Raten-Begrenzung je IP (300 Anfragen/Stunde, 3000/Tag). Jede schreibende Anfrage wird mit Zeitstempel, Route und Token-Hash protokolliert.

C. Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle:** Erreichbarkeits-Überwachung durch einen externen Dienst, der ausschließlich eine Statusseite ohne personenbezogene Daten abruft; Firewall des Betreibers und des Systems; automatische Sicherheitsaktualisierungen des Betriebssystems. **Keine Sicherungskopien des Spiegels** — bewusst: Das Gerät des Auftraggebers hält den maßgeblichen Datenbestand und stellt den Spiegel beim nächsten App-Start automatisch wieder her. Ein Verlust des Servers bedeutet keinen Datenverlust, aber auch keine Daten-Kopien an weiteren Orten.
- **Wiederherstellbarkeit:** Gewährleistet durch das Gerät des Auftraggebers (Quelle der Wahrheit); der Server wird aus dem versionierten Quellcode über eine automatisierte Pipeline mit Gesundheitsprüfung und automatischem Rückfall auf die vorige Version neu ausgeliefert.

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Datenschutz-Management:** Ein-Personen-Betrieb; Verfahrensdokumentation in dieser Anlage, in der Datenschutzerklärung (Abschnitt 3.5) und in der technischen Spezifikation; jährliche Überprüfung der Maßnahmen.
- **Incident-Response:** Meldeweg nach Punkt 3.5; Server-Protokolle der letzten 30 Tage als Analysegrundlage; Zugang kann durch Sperrung des Tokens bzw. Löschung der Mailbox sofort entzogen werden.

- **Datenschutzfreundliche Voreinstellungen:** Agent Sync ist standardmäßig aus; Ende-zu-Ende-Verschlüsselung ist nicht abschaltbar; der Spiegel enthält nur offene Aufgaben, keine erledigten, keine Standort-, Kalender- oder Kontaktdaten.
- **Auftragskontrolle:** Eindeutige Vertragsgestaltung (diese Vereinbarung); keine Verarbeitung zu eigenen Zwecken; Sub-Auftragsverarbeiter nur nach Anlage ./2 mit Vereinbarungen nach Art. 28 Abs. 4 DSGVO.

Anlage ./2: Sub-Auftragsverarbeiter

Sub-Auftragsverarbeiter gemäß Punkt 5 der Vereinbarung:

Unternehmen, Anschrift, Kontakt	Kurzbeschreibung der Leistung	Ort
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland www.hetzner.com	Hosting des virtuellen Servers `api.ilmeno.com`, auf dem Spiegel (nur Chiffrat) und Agent-Inbox gespeichert sind. Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO mit Hetzner.	Rechenzentrum Falkenstein, Deutschland (EU)
Anthropic, PBC 548 Market Street PMB 90375, San Francisco, CA 94104, USA www.anthropic.com	KI-Einordnung des *Titels* einer vom Agenten ohne Bereich eingestellten Aufgabe (Zuordnung zu Bereich/Tags, Vorschlag eines ersten Schritts) — **nur wenn der Auftraggeber in der App Cloud-KI und „KI bei Importen“ eingeschaltet hat**. Die Übermittlung geht vom Gerät des Auftraggebers über den Proxy des Auftragnehmers, nicht aus dem Spiegel. Rechtsgrundlage der Drittlandübermittlung: EU-Standardvertragsklauseln (Modul 2) im Anthropic-DPA; Transfer-Impact-Assessment des Auftragnehmers liegt vor; keine Nutzung zum Modelltraining.	USA

Keine weiteren Sub-Auftragsverarbeiter. Der Auftraggeber kann die Anthropic-Verarbeitung für Agent Sync vollständig ausschließen, indem er in der App „KI bei Importen“ → „API (Agent Sync)“ ausschaltet oder seinen Agenten anweist, immer einen Bereich (`contextTag`) mitzugeben.