

Verschwiegenheitsvereinbarung nach § 203 StGB (DE) / österreichischem Berufs- und Strafrecht (AT) / Art. 321 StGB (CH)

Dokument: Standalone-Verschwiegenheitsvereinbarung (Berufsgeheimnisträger) · **Stand:** 13. Jul 2026 · Nur die deutsche Fassung ist verbindlich.

Verschwiegenheitsvereinbarung über die Mitwirkung an Berufsgeheimnissen (§ 203 StGB)

zwischen

[Name des Auftraggebers / der Kanzlei / Praxis], [Anschrift] – nachfolgend „Auftraggeber“ (Berufsgeheimnisträger) –

und

EZTO TECHNOLOGIES GmbH, Am Brand 41, 55116 Mainz – nachfolgend „EZTO“ (mitwirkende Person/ Hilfsperson) –

– gemeinsam die „Parteien“ –

Kurz gesagt (*unverbindliche Orientierung — maßgeblich ist der Vertragstext*): Im § 203-Modus laufen nur EU-kontrollierte Modelle · keine dauerhafte Speicherung bei den Modellanbietern (Zero Data Retention) · Websuche ist deaktiviert · Ihre Mandats-/Patientendaten liegen in einem eigenen, isolierten Bereich (Tenant) · **Ihre Pflichten:** diese Vereinbarung unterzeichnen, den § 203-Modus aktivieren, geschützte Geheimnisse nur im geschützten Tenant verarbeiten und Ihre eigenen Mitarbeiter verpflichten.

Wer ist wer: „Auftraggeber“ ist der Berufsgeheimnisträger — Sie als Kunde im Sinne der AGB und Verantwortlicher im Sinne des AVV.

Präambel

1. EZTO stellt dem Auftraggeber die KI-Orchestrierungs- und Governance-Plattform „Zentre“ als Software-as-a-Service bereit. Die Einzelheiten der Verarbeitung personenbezogener Daten regelt der zwischen den Parteien geschlossene Auftragsverarbeitungsvertrag (AVV/DPA); die allgemeinen Leistungsbedingungen regeln die AGB.
2. Der Auftraggeber unterliegt einer strafbewehrten beruflichen Verschwiegenheitspflicht (Deutschland: § 203 StGB; Österreich: je nach Beruf § 80 WTBG 2017, § 9 RAO bzw. – insbesondere für Gesundheitsberufe – § 121 öStGB; Schweiz: Art. 321 schweizerisches StGB). Soweit der Auftraggeber Zentre zur Verarbeitung geschützter Geheimnisse einsetzt, wird EZTO als sonstige mitwirkende Person (Deutschland: § 203 Abs. 3 StGB), als Dienstleister bzw. Hilfskraft nach dem jeweiligen österreichischen Berufsrecht (Österreich) oder als Hilfsperson (Schweiz: Art. 321 CH-StGB) tätig.
3. Diese Vereinbarung setzt die berufsrechtlichen Vorgaben zur Einbindung von Dienstleistern um, insbesondere § 43e BRAO i. V. m. § 2 BORA (Rechtsanwälte) und § 62a StBerG (Steuerberater) in Deutschland sowie die entsprechenden berufsrechtlichen Vorgaben in Österreich und der Schweiz, und ergänzt den AVV/DPA. Für Sachverhalte des Geheimnisschutzes gehen die Regelungen dieser Vereinbarung dem AVV/DPA und den AGB vor.

§ 1 Begriffsbestimmungen

1. „Geschützte Geheimnisse“ sind fremde Geheimnisse i. S. d. § 203 StGB bzw. der entsprechenden Verschwiegenheitspflichten (z. B. § 80 WTBG 2017, §§ 121, 122 öStGB, Art. 321 CH-StGB), die dem Auftraggeber in Ausübung seines Berufes anvertraut oder sonst bekannt geworden sind und die der Auftraggeber im Rahmen der Nutzung von Zentre verarbeitet (einschließlich der Tatsache des Bestehens eines Mandats-/Behandlungsverhältnisses).
2. „Mitwirkende Personen“ sind EZTO sowie weitere von EZTO eingesetzte Personen und Stellen (insbesondere Beschäftigte, Subprozessoren und KI-Provider), die an der Erbringung der Leistung mitwirken und dabei Zugang zu geschützten Geheimnissen erhalten können.
3. „§ 203-Modus“ ist die in Anlage 2 beschriebene Konfiguration für die Verarbeitung geschützter Geheimnisse: EU-Hosting, EU-basiertes Routing, Zero Data Retention, deaktivierte Websuche sowie Beschränkung ausschließlich auf zugelassene EU-kontrollierte bzw. von Cortecs in der EU selbst betriebene Modelle. Endpunkte von Anbietern mit Nicht-EU-Konzernobergesellschaft stehen im § 203-Modus nicht zur Verfügung. Die Verarbeitung geschützter Geheimnisse erfolgt in einem vom Normalbetrieb getrennten Tenant (§ 7 Abs. 6).

§ 2 Verpflichtung zur Verschwiegenheit

1. EZTO verpflichtet sich, über alle geschützten Geheimnisse, die ihr im Rahmen der Leistungserbringung zugänglich werden, Stillschweigen zu bewahren und sie weder unbefugt zu offenbaren noch zu verwerten.
2. EZTO verwendet geschützte Geheimnisse ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und auf dokumentierte Weisung des Auftraggebers. Eine Nutzung zu eigenen Zwecken, insbesondere zum Training, Fine-Tuning oder zur Verbesserung eigener oder fremder KI-Modelle, ist ausgeschlossen.
3. Die Verpflichtung gilt zeitlich unbegrenzt und besteht auch nach Beendigung des Vertragsverhältnisses fort.

§ 3 Belehrung über die strafrechtlichen Folgen

1. Der Auftraggeber belehrt EZTO hiermit, dass der Bruch der Verschwiegenheit oder die Verwertung fremder Geheimnisse durch EZTO für die mitwirkenden Personen strafbar ist (§ 203 Abs. 4 Satz 1 StGB, § 204 StGB) und mit Freiheitsstrafe bis zu einem Jahr, im Fall des § 204 StGB mit Freiheitsstrafe bis zu zwei Jahren, oder mit Geldstrafe geahndet werden kann. Die Strafdrohung erhöht sich auf Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, wenn die Person gegen Entgelt oder in Bereicherungsabsicht – auch zugunsten Dritter – oder in Schädigungsabsicht handelt (§ 203 Abs. 6 StGB).
2. Der Auftraggeber belehrt EZTO vorsorglich, dass sich mitwirkende Personen strafbar machen, wenn sie sich einer weiteren mitwirkenden Person bedienen, die die Verschwiegenheit bricht, und nicht dafür Sorge getragen haben, dass diese zur Geheimhaltung verpflichtet wurde (§ 203 Abs. 4 Satz 2 Nr. 2 StGB).
3. „Offenbaren“ im Sinne des § 203 StGB umfasst bereits das Verschaffen der Möglichkeit der Kenntnisnahme durch unbefugte Dritte. Eine entsprechende Strafbarkeit bzw. Sanktionierung kann sich in Österreich – je nach Beruf – aus § 121 öStGB (insbesondere Gesundheitsberufe), § 122 öStGB oder dem Berufsrecht (z. B. § 80 Abs. 5 WTBG 2017) und in der Schweiz aus Art. 321 schweizerisches StGB ergeben.
4. Bestandteil dieser Belehrung ist der Wortlaut der einschlägigen Vorschriften (§§ 203, 204 StGB; § 43e BRAO; § 62a StBerG) in der bei Abschluss geltenden Fassung; dieser wird der Ausfertigung dieser

Vereinbarung als Anlage beigefügt. EZTO belehrt die von ihr zur Leistungserbringung eingesetzten Personen entsprechend.

§ 4 Verpflichtung der Beschäftigten

1. EZTO stellt sicher, dass alle ihr unterstellten Personen, die Zugang zu geschützten Geheimnissen erhalten können, vor Aufnahme der Tätigkeit in Textform zur Verschwiegenheit nach Maßgabe dieser Vereinbarung verpflichtet und über die strafrechtlichen Folgen belehrt werden. Ein Muster der Verpflichtungserklärung ergibt sich aus Anlage 1.
2. EZTO weist die Erfüllung dieser Pflicht dem Auftraggeber auf Anfrage durch eine zusammenfassende Bestätigung nach; das Muster der Verpflichtungserklärung (Anlage 1) wird auf Wunsch bereitgestellt. Personenbezogene Einzelnachweise erfolgen nur nach gesonderter Vereinbarung oder soweit berufsrechtlich zwingend erforderlich.

§ 5 Weitere mitwirkende Personen (Flow-down)

1. Soweit EZTO weitere mitwirkende Personen (insbesondere Subprozessoren und KI-Provider) einsetzt, die Zugang zu geschützten Geheimnissen erhalten können, verpflichtet EZTO diese zuvor in Textform gleichwertig zur Verschwiegenheit und Belehrung nach dieser Vereinbarung.
2. Im § 203-Modus werden ausschließlich Modellanbieter eingesetzt, die nach Anlage 2 zugelassen sind und die sich einer entsprechenden Verschwiegenheitsverpflichtung unterworfen haben. Anbieter, die einer solchen Verpflichtung nicht unterliegen, werden technisch ausgeschlossen.
3. Kann eine weitere mitwirkende Person nicht gleichwertig verpflichtet werden, so wird sie für die Verarbeitung geschützter Geheimnisse nicht eingesetzt.

§ 6 Erforderlichkeit, Zugriffsbeschränkung, Sicherheit

1. Ein Zugriff auf geschützte Geheimnisse erfolgt nur, soweit dies für die Leistungserbringung erforderlich ist (Need-to-know), möglichst zeitlich begrenzt, freigegeben und protokolliert.
2. EZTO trifft angemessene technische und organisatorische Maßnahmen nach dem Stand der Technik (Art. 32 DSGVO; Einzelheiten gemäß AVV/DPA und dessen TOM-Anlage), insbesondere Transportverschlüsselung (TLS 1.2 oder höher), Verschlüsselung ruhender Daten/Artefakte (AES-256 (mindestens)), rollenbasierte Zugriffskontrolle, Mandantentrennung und Zugriffsprotokollierung. EZTO betreibt ein an ISO/IEC 27001 ausgerichtetes ISMS und befindet sich derzeit im Zertifizierungsprozess nach ISO/IEC 27001; Nachweise erbringt EZTO über das Standard-Nachweispaket gemäß AVV Anlage 2 (Trust Center); das ISO/IEC-27001-Zertifikat stellt EZTO nach Erteilung im Trust Center bereit. Das Sicherheitsniveau wird dabei nicht geringer angesetzt als für eigene vertrauliche Informationen von EZTO.

§ 7 Datenstandort und § 203-Modus

1. Hosting und produktive Verarbeitung erfolgen im § 203-Modus ausschließlich innerhalb der EU/des EWR (Hosting: Scaleway, Region Paris/fr-par). Zero Data Retention ist aktiviert. Eine Nutzung von Inhalten zum Modell-Training ist vertraglich ausgeschlossen; bei von Cortecs selbst in der EU betriebenen Modellen erhält der Modellhersteller technisch keinen Zugriff auf Inferenzdaten, bei externen EU-Anbietern gelten deren vertragliche Zero-Data-Retention-Zusagen.
2. Im § 203-Modus werden ausschließlich EU-kontrollierte bzw. von Cortecs in der EU selbst betriebene Endpunkte eingesetzt (Anlage 2). Modellanbieter, die einer Nicht-EU-Jurisdiktion unterliegen, sind technisch deaktiviert.

3. Die Aktivierung des § 203-Modus gilt als dokumentierte Weisung.
4. Die Aufnahme zusätzlicher Modellanbieter oder Modellversionen, die die Anforderungen der Absätze 1 und 2 erfüllen, in Anlage 2 ist ohne gesonderte Ankündigung zulässig. Die Entfernung oder der Ersatz zugelassener Modellanbieter sowie sonstige Änderungen der Konfiguration des § 203-Modus werden dem Auftraggeber mindestens 30 Tage vor Wirksamwerden in Textform angekündigt; ein Ersatz erfolgt nur durch mindestens gleichwertige Anbieter, die die Anforderungen der Absätze 1 und 2 erfüllen. Widerspricht der Auftraggeber innerhalb der Ankündigungsfrist, steht ihm ein Sonderkündigungsrecht zum Wirksamwerden der Änderung zu. Anlage 2 wird mit Stand-Datum geführt; die bei Abschluss dieser Vereinbarung geltende Fassung wird der Ausfertigung beigelegt. Die jeweils aktuelle Anlage 2 ist im Trust Center abrufbar; frühere Fassungen sind mit Stand-Datum im Trust Center abrufbar.
5. Web-Suche: Im § 203-Modus ist die Websuche-Funktion deaktiviert. Geschützte Geheimnisse dürfen nicht als Suchanfrage eingegeben werden.
6. Mandatstrennung durch separaten Tenant: Für die Verarbeitung geschützter Geheimnisse wird eine vom Normalbetrieb getrennte, dedizierte und logisch isolierte Umgebung (separater Tenant) bereitgestellt. Eine physisch getrennte Umgebung (Private Cloud/On-Premises) kann als Enterprise-Option gesondert vereinbart werden. Der § 203-Tenant verfügt über eine eigene, isolierte Wissensbasis (RAG-Index/ Vektorspeicher), eigene Datenhaltung sowie eine dedizierte Modell- und Routing-Konfiguration; die Verschlüsselung erfolgt mandantenbezogen im Rahmen der TOM. Eine gemeinsame Wissensbasis mit dem Normal-Tenant besteht nicht; ein Datentransfer und eine tenantübergreifende Suche zwischen § 203-Tenant und Normal-Tenant sind durch technische Zugriffskontrollen unterbunden. Ein etwaiger Wechsel zwischen Tenants ist ein reiner Identitäts-/Navigationswechsel (z. B. via Single Sign-On) ohne Übertragung von Inhalten. Der aktive Tenant wird dem Nutzer eindeutig angezeigt.

§ 8 Mitteilungspflichten

1. EZTO informiert den Auftraggeber unverzüglich über jede tatsächliche oder drohende unbefugte Kenntnisnahme geschützter Geheimnisse.
2. Über rechtlich bindende Offenlegungsersuchen Dritter oder von Behörden in Bezug auf geschützte Geheimnisse informiert EZTO den Auftraggeber – soweit rechtlich zulässig – unverzüglich und vor einer etwaigen Offenlegung; Offenlegungen werden auf das rechtlich zwingend erforderliche Minimum beschränkt.

§ 9 Pflichten und Verantwortung des Auftraggebers

1. Der Auftraggeber bleibt allein verantwortlich für die Zulässigkeit der Offenbarung geschützter Geheimnisse gegenüber EZTO, für die sorgfältige Auswahl und – im Rahmen des Zumutbaren – Überwachung von EZTO sowie für die Beschränkung der eingegebenen Daten auf das Erforderliche (Datenminimierung, Need-to-know).
2. Der Auftraggeber stellt sicher, dass geschützte Geheimnisse ausschließlich im § 203-Tenant (im § 203-Modus) verarbeitet werden; die Einordnung, ob Daten ein geschütztes Geheimnis darstellen, obliegt dem Auftraggeber. Im Zweifel ist der § 203-Tenant zu verwenden. Mandatsfreie/interne Vorgänge ohne geschützte Geheimnisse können im Normal-Tenant verarbeitet werden.
3. Der Auftraggeber verpflichtet seine eigenen Beschäftigten und Nutzer eigenverantwortlich zur Verschwiegenheit.

§ 10 Laufzeit und Beendigung

1. Diese Vereinbarung gilt für die Dauer des Hauptvertrags. Die Verschwiegenheitspflichten gelten zeitlich unbegrenzt fort.

2. Der Auftraggeber kann diese Vereinbarung und den Hauptvertrag aus wichtigem Grund mit sofortiger Wirkung beenden, wenn die Einhaltung der gesetzlichen Vorgaben (insbesondere § 203 StGB, § 43e BRAO/§ 2 BORA bzw. § 62a StBerG; in Österreich die einschlägigen berufs- und strafrechtlichen Vorgaben, z. B. § 80 WTBG 2017, §§ 121, 122 öStGB; in der Schweiz Art. 321 schweizerisches StGB) nicht mehr gewährleistet ist; entsprechendes berufsrechtliches Beendigungsrecht bleibt unberührt.

§ 11 Verhältnis zu anderen Vereinbarungen

Diese Vereinbarung ergänzt den AVV/DPA und die AGB. Bei Widersprüchen gehen für Sachverhalte des Geheimnisschutzes die Regelungen dieser Vereinbarung vor; im Übrigen gelten AVV/DPA und AGB.

§ 12 Schlussbestimmungen

1. Änderungen und Ergänzungen bedürfen mindestens der Textform; dies gilt auch für die Aufhebung dieses Formerfordernisses. Diese Vereinbarung kann elektronisch (Textform/elektronische Signatur) geschlossen werden; EZTO stellt dem Auftraggeber nach Abschluss eine vollständige Ausfertigung einschließlich der zum Abschlusszeitpunkt geltenden Anlagen (insbesondere Anlage 2 und Gesetzeswortlaut) als Dokument bereit. Im Fall einer Übertragung des Hauptvertrags nach Ziff. 16 der AGB tritt der Rechtsnachfolger in diese Vereinbarung ein; die Übertragung ist nur zulässig, wenn der Rechtsnachfolger die Pflichten nach §§ 4 und 5 übernimmt und die Verpflichtung und Belehrung der bei ihm mitwirkenden Personen vor deren erstem Zugriff auf geschützte Geheimnisse sichergestellt ist.
2. Es gilt deutsches Recht. Gerichtsstand ist – soweit zulässig – Mainz. Zwingende berufs- und strafrechtliche Vorgaben des Sitzstaates des Auftraggebers (insbesondere in Österreich und der Schweiz) bleiben unberührt.
3. Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem wirtschaftlichen Zweck am nächsten kommt.

Auftraggeber — Ort, Datum: _____ Unterschrift: _____

EZTO TECHNOLOGIES GmbH — Ort, Datum: _____ Unterschrift: _____

Anlage 1 — Verpflichtungserklärung der Beschäftigten (Muster)

Hiermit werde ich, [Name], als mitwirkende Person zur Verschwiegenheit verpflichtet. Mir ist bekannt, dass

- ich über alle fremden Geheimnisse, die mir im Rahmen meiner Tätigkeit für die EZTO TECHNOLOGIES GmbH zugänglich werden, Stillschweigen zu bewahren habe und sie weder offenbaren noch verwerten darf;
- die unbefugte Offenbarung nach § 203 Abs. 4 StGB (Deutschland) strafbar ist – und entsprechend nach österreichischem Recht (je nach Beruf §§ 121, 122 öStGB, § 80 WTBG 2017) bzw. Art. 321 schweizerisches StGB (Schweiz) – und bereits das Verschaffen der Möglichkeit der Kenntnisnahme erfasst;
- diese Pflicht über die Beendigung meiner Tätigkeit hinaus fortbesteht.

Ort, Datum: _____ Unterschrift: _____

Anlage 2 — § 203-Modus: zugelassene Modellanbieter

Konfigurationsgrundsatz: Im § 203-Modus sind in Cortecs (Cortecs GmbH, Wien) ausschließlich die nachstehend zugelassenen, in der EU betriebenen Endpunkte freigeschaltet; alle übrigen Anbieter sind

technisch gesperrt. Die Aktivierung des § 203-Modus gilt als dokumentierte Weisung. Maßgeblich ist, wer während der Inferenz auf die Daten zugreifen kann: Bei offenen Modellen, die Cortecs selbst in der EU betreibt, erhält der Modellhersteller keinen Zugriff.

Zugelassene Modellanbieter — EU-kontrolliert

Ausschließlich EU-kontrollierte bzw. von Cortecs in der EU selbst betriebene Modelle; kein Anbieter mit Nicht-EU-Mutterkonzern.

Modell / Anbieter	Sitz	Hosting	ZDR
Mistral (Large, Medium, Codestral, Devstral, Nemo)	Frankreich (EU)	EU	Ja
Offene Modelle, von Cortecs in der EU betrieben (Llama, Qwen, DeepSeek, Gemma, Phi, gpt-oss)	Betrieb durch Cortecs (EU)	EU	Ja
EU-Inferenz-Provider (STACKIT, IONOS, OVH, Scaleway, AKI.IO)	Deutschland / EU	EU	Ja

Ausgeschlossen: Sämtliche Endpunkte von Anbietern mit Nicht-EU-Konzernobergesellschaft (auch EU-gehostete Endpunkte) sowie Anbieter ohne EU-Endpunkt, ohne Zero Data Retention oder ohne Verschwiegenheits-Flow-down.

Confidentiality Agreement under Section 203 StGB (DE) / Austrian professional and criminal law (AT) / Article 321 CH-StGB

English convenience translation. Only the German version is legally binding.

Document: standalone confidentiality agreement (professional secrecy holders) · **Last updated:** 13 Jul 2026

Confidentiality Agreement on Involvement in Professional Secrets (Section 203 StGB)

between

[Name of the customer / law firm / practice], [address] – hereinafter “Customer” (professional secrecy holder) –

and

EZTO TECHNOLOGIES GmbH, Am Brand 41, 55116 Mainz – hereinafter “EZTO” (contributing person/auxiliary person) –

– together the “Parties” –

In brief (*non-binding orientation — the contract text prevails*): In Section 203 mode, only EU-controlled models run · no permanent storage at the model providers (zero data retention) · web search is deactivated · your mandate/patient data resides in its own isolated area (tenant) · **Your duties:** sign this agreement, activate Section 203 mode, process protected secrets only in the protected tenant, and bind your own staff.

Who is who: the “Customer” is the professional secrecy holder — you as the customer under the GTC and the controller under the DPA.

Preamble

1. EZTO provides the Customer with the AI orchestration and governance platform “Zentre” as software-as-a-service. The details of the processing of personal data are governed by the Data Processing Agreement (DPA) concluded between the Parties; the General Terms and Conditions (AGB) govern the general service terms.
2. The Customer is subject to a criminally sanctioned professional duty of confidentiality (Germany: Section 203 StGB; Austria: depending on the profession, Section 80 WTBG 2017, Section 9 RAO or – in particular for health professions – Section 121 öStGB; Switzerland: Article 321 of the Swiss Criminal Code). To the extent the Customer uses Zentre to process protected secrets, EZTO acts as an “other contributing person” within the meaning of Section 203 (3) StGB, as a service provider or auxiliary under the applicable Austrian professional law (Austria), or as an auxiliary person (Switzerland: Article 321 CH-StGB).
3. This Agreement implements the professional-law requirements for engaging service providers, in particular Section 43e BRAO in conjunction with Section 2 BORA (lawyers) and Section 62a StBerG (tax advisors) in Germany, as well as the corresponding professional-law requirements in Austria and Switzerland, and supplements the DPA. For matters of secret protection, the provisions of this Agreement prevail over the DPA and the terms of service.

Section 1 Definitions

1. “Protected secrets” are third-party secrets within the meaning of Section 203 StGB or the corresponding confidentiality duties (e.g., Section 80 WTBG 2017, Sections 121, 122 öStGB, Article 321 CH-StGB) that have been entrusted to or otherwise become known to the Customer in the exercise of its profession and that the Customer processes when using Zentre (including the fact of the existence of a mandate/ treatment relationship).
2. “Contributing persons” are EZTO as well as other persons and entities engaged by EZTO (in particular employees, subprocessors, and AI providers) who participate in the provision of the service and may thereby gain access to protected secrets.
3. “Section 203 mode” is the configuration described in Annex 2 for the processing of protected secrets: EU hosting, EU-based routing, zero data retention, deactivated web search, and restriction exclusively to authorized EU-controlled models or models operated by Cortecs in the EU itself. Endpoints of providers with a non-EU ultimate parent are not available in Section 203 mode. The processing of protected secrets takes place in a tenant separated from normal operation (Section 7 (6)).

Section 2 Confidentiality obligation

1. EZTO undertakes to maintain secrecy regarding all protected secrets that become accessible to it in the course of providing the service, and neither to disclose nor exploit them without authorization.
2. EZTO uses protected secrets exclusively to provide the contractually agreed services and on the documented instruction of the Customer. Any use for its own purposes, in particular for training, fine-tuning, or improving its own or third-party AI models, is excluded.
3. The obligation applies without time limit and continues after termination of the contractual relationship.

Section 3 Instruction about the criminal consequences

1. The Customer hereby instructs EZTO that a breach of confidentiality or the exploitation of third-party secrets by EZTO is punishable for the contributing persons (§ 203 (4) sentence 1 StGB, § 204 StGB) by imprisonment of up to one year, in the case of § 204 StGB up to two years, or a fine. The penalty increases to imprisonment of up to two years or a fine where the person acts for remuneration or with intent to enrich themselves or a third party, or to harm another (§ 203 (6) StGB).
2. The Customer instructs EZTO, as a precaution, that contributing persons are liable to prosecution if they engage a further contributing person who breaches confidentiality and they have not ensured that such person was bound to secrecy (§ 203 (4) sentence 2 no. 2 StGB).
3. “Disclosure” within the meaning of § 203 StGB already includes enabling unauthorized third parties to take note of the information. Corresponding criminal liability or sanctions may arise in Austria – depending on the profession – from Section 121 öStGB (in particular health professions), Section 122 öStGB, or professional law (e.g., Section 80(5) WTBG 2017), and in Switzerland from Article 321 of the Swiss Criminal Code.
4. The wording of the relevant provisions (§§ 203, 204 StGB; § 43e BRAO; § 62a StBerG) in the version in effect at conclusion forms part of this instruction and is appended to the executed copy of this Agreement as an annex. EZTO instructs the persons it engages for the provision of the services accordingly.

Section 4 Obligation of employees

1. EZTO ensures that all persons subordinate to it who may gain access to protected secrets are, before taking up their activity, bound to confidentiality in text form in accordance with this Agreement and

instructed about the criminal consequences. A template of the confidentiality undertaking is set out in Annex 1.

2. EZTO demonstrates fulfilment of this obligation to the Customer upon request by way of a summary confirmation; the template undertaking (Annex 1) is provided on request. Person-specific individual evidence is provided only by separate agreement or to the extent mandatorily required under professional law.

Section 5 Other contributing persons (flow-down)

1. To the extent EZTO engages other contributing persons (in particular subprocessors and AI providers) who may gain access to protected secrets, EZTO binds them beforehand in text form to equivalent confidentiality and instruction in accordance with this Agreement.
2. In Section 203 mode, only model providers that are authorized in accordance with Annex 2 and that have submitted to a corresponding confidentiality obligation are used. Providers not subject to such an obligation are technically excluded.
3. If another contributing person cannot be bound equivalently, it is not used for the processing of protected secrets.

Section 6 Necessity, access restriction, security

1. Access to protected secrets takes place only to the extent necessary for the provision of the service (need-to-know), as time-limited as possible, approved, and logged.
2. EZTO implements appropriate technical and organizational measures at the state of the art (Art. 32 GDPR; details per the DPA and its TOM annex), in particular transport encryption (TLS 1.2 or higher), encryption of data/artifacts at rest (AES-256 (at minimum)), role-based access control, tenant separation, and access logging. EZTO operates an ISO/IEC 27001-aligned ISMS and is currently undergoing ISO/IEC 27001 certification; evidence is provided through the standard evidence package pursuant to Annex 2 of the DPA (Trust Center); EZTO makes the ISO/IEC 27001 certificate available in the Trust Center once issued. The level of security shall not be set lower than for EZTO's own confidential information.

Section 7 Data location and Section 203 mode

1. Hosting and productive processing take place in Section 203 mode exclusively within the EU/EEA (hosting: Scaleway, region Paris/fr-par). Zero data retention is activated. Use of content for model training is excluded contractually; for models operated by Cortecs itself in the EU, the model manufacturer has no technical access to inference data, and for external EU providers their contractual zero-data-retention commitments apply.
2. In Section 203 mode, only EU-controlled endpoints or endpoints operated by Cortecs in the EU itself are used (Annex 2). Model providers subject to a non-EU jurisdiction are technically deactivated.
3. Activation of Section 203 mode constitutes a documented instruction.
4. The addition to Annex 2 of further model providers or model versions that meet the requirements of paragraphs 1 and 2 is permitted without separate announcement. The removal or replacement of authorized model providers and other changes to the configuration of Section 203 mode are announced to the Customer in text form at least 30 days before they take effect; a replacement is made only by at least equivalent providers meeting the requirements of paragraphs 1 and 2. If the Customer objects within the notice period, the Customer has a special right of termination effective as of the date the change takes effect. Annex 2 is maintained with a "last updated" date; the version in effect at the

conclusion of this Agreement is attached to the executed copy. The current version of Annex 2 is available in the Trust Center; previous versions are available in the Trust Center with their date.

5. Web search: In Section 203 mode, the web search function is deactivated. Protected secrets must not be entered as search queries.
6. Mandate separation through a separate tenant: For the processing of protected secrets, a dedicated, logically isolated environment separated from normal operation (separate tenant) is provided. A physically separated environment (private cloud/on-premises) may be agreed separately as an Enterprise option. The Section 203 tenant has its own, isolated knowledge base (RAG index/vector store), its own data storage, and a dedicated model and routing configuration; encryption is applied on a tenant-related basis within the framework of the TOM. There is no shared knowledge base with the normal tenant; data transfer and cross-tenant search between the Section 203 tenant and the normal tenant are prevented by technical access controls. Any switch between tenants is a pure identity/navigation switch (e.g., via single sign-on) without transfer of content. The active tenant is clearly indicated to the user.

Section 8 Notification obligations

1. EZTO informs the Customer without undue delay of any actual or threatened unauthorized access to protected secrets.
2. Regarding legally binding disclosure requests from third parties or authorities concerning protected secrets, EZTO informs the Customer – to the extent legally permissible – without undue delay and before any disclosure; disclosures are limited to the legally mandatory minimum.

Section 9 Obligations and responsibility of the Customer

1. The Customer remains solely responsible for the permissibility of disclosing protected secrets to EZTO, for the careful selection and – within reason – monitoring of EZTO, and for limiting the data entered to what is necessary (data minimization, need-to-know).
2. The Customer ensures that protected secrets are processed exclusively in the Section 203 tenant (in Section 203 mode); the assessment of whether data constitutes a protected secret rests with the Customer; in case of doubt, the Section 203 tenant is to be used. Mandate-free/internal matters without protected secrets may be processed in the normal tenant.
3. The Customer binds its own employees and users to confidentiality on its own responsibility.

Section 10 Term and termination

1. This Agreement applies for the term of the main agreement. The confidentiality obligations continue without time limit.
2. The Customer may terminate this Agreement and the main agreement for good cause with immediate effect if compliance with the statutory requirements (in particular Section 203 StGB, Section 43e BRAO/ Section 2 BORA or Section 62a StBerG; in Austria the relevant professional and criminal law requirements, e.g., Section 80 WTBG 2017, Sections 121, 122 öStGB; in Switzerland Article 321 of the Swiss Criminal Code) is no longer ensured; any corresponding professional-law right of termination remains unaffected.

Section 11 Relationship to other agreements

This Agreement supplements the DPA and the terms of service. In case of conflict, the provisions of this Agreement prevail for matters of secret protection; otherwise, the DPA and the terms of service apply.

Section 12 Final provisions

1. Amendments and supplements require at least text form; this also applies to the waiver of this form requirement. This Agreement may be concluded electronically (text form/electronic signature); after conclusion, EZTO provides the Customer with a complete executed copy including the annexes in effect at the time of conclusion (in particular Annex 2 and the statutory texts) as a document. In the event of a transfer of the main agreement pursuant to Section 16 of the Terms, the legal successor accedes to this Agreement; the transfer is permitted only if the legal successor assumes the obligations under Sections 4 and 5 and it is ensured that the persons contributing at the successor are bound and instructed before their first access to protected secrets.
2. German law applies. The place of jurisdiction is – to the extent permissible – Mainz. Mandatory professional and criminal law provisions of the Customer's home state (in particular in Austria and Switzerland) remain unaffected.
3. Should any provision be or become invalid, the validity of the remaining provisions remains unaffected. The Parties shall replace the invalid provision with a valid one that comes closest to the economic purpose.

Customer — Place, date: _____ Signature: _____

EZTO TECHNOLOGIES GmbH — Place, date: _____ Signature: _____

Annex 1 — Confidentiality undertaking of employees (template)

I, [name], am hereby bound to confidentiality as a contributing person. I am aware that

- I must maintain secrecy regarding all third-party secrets that become accessible to me in the course of my activity for EZTO TECHNOLOGIES GmbH, and may neither disclose nor exploit them;
- the unauthorized disclosure of such secrets is punishable under Section 203 (4) StGB (Germany) – and correspondingly under Austrian law (depending on the profession Sections 121, 122 öStGB, Section 80 WTBG 2017) or Article 321 of the Swiss Criminal Code (Switzerland) – and already includes enabling unauthorized persons to take note of the information;
- this obligation continues beyond the end of my activity.

Place, date: _____ Signature: _____

Annex 2 — Section 203 mode: authorized model providers

Configuration principle: In § 203 mode, only the authorized EU-operated endpoints listed below are enabled in Cortecs (Cortecs GmbH, Vienna); all other providers are technically blocked. Activation of Section 203 mode constitutes a documented instruction. What matters is who can access the data during inference: for open models that Cortecs operates in the EU itself, the model maker has no access.

Authorized model providers — EU-controlled

Exclusively EU-controlled models or models operated by Cortecs in the EU; no provider with a non-EU parent company.

Model / provider	Origin	Hosting	ZDR
Mistral (Large, Medium, Codestral, Devstral, Nemo)	France (EU)	EU	Yes

Model / provider	Origin	Hosting	ZDR
Open models operated by Cortecs in the EU (Llama, Qwen, DeepSeek, Gemma, Phi, gpt-oss)	Operated by Cortecs (EU)	EU	Yes
EU inference providers (STACKIT, IONOS, OVH, Scaleway, AKI.IO)	Germany / EU	EU	Yes

Excluded: all endpoints of providers with a non-EU ultimate parent (including EU-hosted endpoints), as well as providers without an EU endpoint, without zero data retention, or without a confidentiality flow-down.