Auftragsverarbeitungsvertrag (AVV)

Data Processing Agreement (DPA)

Stand: 06. Jun 2026

DEUTSCH

1. Präambel, Parteien, Rangfolge

• Dieser Auftragsverarbeitungsvertrag („AVV") regelt die Verarbeitung personenbezogener Daten durch EZTO TECHNOLOGIES GmbH, Mainz („Auftragsverarbeiter") im Auftrag des Kunden („Verantwortlicher") im Zusammenhang mit dem Service „Zentre".

• Dieser AVV ist Bestandteil des Hauptvertrags (AGB/Order Form). Bei Widersprüchen gehen die Regelungen dieses AVV für datenschutzrechtliche Fragen vor. Im Übrigen gilt der Hauptvertrag.

• Begriffe der DSGVO gelten entsprechend.

2. Rollen und Abgrenzung (Processor vs. Controller)

• Processor-Scope: Dieser AVV gilt für Verarbeitungen, bei denen EZTO Kundendaten als Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet, insbesondere: Bereitstellung und Betrieb von Zentre (Workspace/Chat, Nutzerverwaltung, Zugriffskontrolle); Inference/Orchestrierung/Routing an KI-Provider nach Konfiguration; Support und Fehleranalyse, soweit hierfür Kundendaten verarbeitet werden; Security/Missbrauchsprävention/Incident-Handling.

• Controller-Scope: Soweit EZTO personenbezogene Daten als eigener Verantwortlicher verarbeitet (z. B. Marketing/Website, Vertragsanbahnung/-abschluss, Abrechnung/Zahlungsabwicklung, unternehmensbezogene Compliance), gilt dieser AVV nicht; hierfür gelten die Datenschutzhinweise und ggf. separate Vereinbarungen.

• Kein BYOK: Zentre unterstützt derzeit kein „Bring Your Own Key" (BYOK). Die Auswahl/Aktivierung von KI-Providern erfolgt über Zentre-Konfigurationen.

3. Definitionen

• „Kundendaten": alle personenbezogenen Daten, die der Verantwortliche oder dessen Nutzer in Zentre eingibt, hochlädt, erzeugt oder anderweitig bereitstellt (einschließlich Inhaltsdaten und Metadaten).

• „Inhaltsdaten": Workspace-/Chat-Inhalte, Prompts, Uploads, Dokumente sowie Outputs (soweit in Zentre gespeichert/angezeigt).

• „Metadaten": Nutzungs-, Abrechnungs-, Sicherheits- und technische Telemetriedaten (z. B. Zeitstempel, Request-IDs, Konfigurationsparameter, Token-/Volumenmetriken, Fehlermeldungen), soweit personenbezogen.

• „KI-Provider": Drittanbieter, an den Zentre Workloads zur Inference/Generierung weiterleitet.

• „Subprozessor": Unterauftragsverarbeiter i. S. d. Art. 28 Abs. 2 DSGVO.

ENGLISH (US)

1. Preamble, parties, order of precedence

• This Data Processing Agreement ("DPA") governs the processing of personal data by EZTO TECHNOLOGIES GmbH, Mainz ("Processor") on behalf of the Customer ("Controller") in connection with the "Zentre" service.

• This DPA forms part of the main agreement (Terms/order form). In case of conflict, the provisions of this DPA prevail for data protection matters. Otherwise, the main agreement applies.

• GDPR terms apply accordingly.

2. Roles and delineation (Processor vs. Controller)

• Processor scope: This DPA applies to processing in which EZTO processes Customer data as a processor on behalf of the Controller, in particular: provision and operation of Zentre (workspace/chat, user management, access control); inference/orchestration/routing to AI providers per configuration; support and error analysis where Customer data is processed for this purpose; security/abuse prevention/incident handling.

• Controller scope: Where EZTO processes personal data as its own controller (e.g., marketing/website, contract initiation/conclusion, billing/payment processing, company-related compliance), this DPA does not apply; the privacy notices and any separate agreements apply instead.

• No BYOK: Zentre does not currently support "Bring Your Own Key" (BYOK). The selection/activation of AI providers takes place via Zentre configurations.

3. Definitions

• "Customer data": all personal data that the Controller or its users input, upload, generate, or otherwise provide in Zentre (including content data and metadata).

• "Content data": workspace/chat content, prompts, uploads, documents, and outputs (where stored/displayed in Zentre).

• "Metadata": usage, billing, security, and technical telemetry data (e.g., timestamps, request IDs, configuration parameters, token/volume metrics, error messages), where personal.

• "AI provider": a third-party provider to which Zentre forwards workloads for inference/generation.

• "Subprocessor": a sub-processor within the meaning of Art. 28 (2) GDPR.

DEUTSCH	ENGLISH (US)
• „Plan": die im Order Form/Hauptvertrag benannte Seat-basierte Lizenz (ein Plan, pro Nutzer); daneben bestehen Enterprise- und Private-Cloud-Optionen nach gesonderter Vereinbarung.	• "Plan": the seat-based license named in the order form/main agreement (one plan, per user); in addition, Enterprise and Private Cloud options exist by separate agreement.
4. Gegenstand, Art, Zweck, Dauer	**4. Subject matter, nature, purpose, duration**
• Gegenstand ist die Verarbeitung von Kundendaten zur Bereitstellung, zum sicheren Betrieb, zur Wartung, Support-Leistung sowie zur Weiterentwicklung von Zentre.	• The subject matter is the processing of Customer data to provide, securely operate, maintain, support, and further develop Zentre.
• Dauer: Laufzeit des Hauptvertrags; anschließend Löschung/Rückgabe gemäß Ziff. 15.	• Duration: the term of the main agreement; thereafter deletion/return in accordance with Section 15.
• Details zu Art/Zweck/Datenkategorien/Betroffenen: Anlage 1.	• Details on nature/purpose/data categories/data subjects: Annex 1.
5. Weisungen und Weisungsmanagement	**5. Instructions and instruction management**
• Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO).	• Processing takes place exclusively on the documented instruction of the Controller (Art. 28 (3) (a) GDPR).
• Dokumentierte Weisungen umfassen: (i) Hauptvertrag/AVV, (ii) Produkt- und Account-Konfigurationen (Provider-Auswahl, Allow/Deny, Routing, Regionen, Retention, Logging), (iii) Einzelweisungen in Textform (Ticket/E-Mail).	• Documented instructions include: (i) the main agreement/DPA, (ii) product and account configurations (provider selection, allow/deny, routing, regions, retention, logging), (iii) individual instructions in text form (ticket/email).
• Offensichtlich rechtswidrige Weisungen werden nicht ausgeführt; der Verantwortliche wird informiert.	• Manifestly unlawful instructions are not carried out; the Controller is informed.
• Zusätzlicher, nicht vereinbarter Aufwand kann nach Maßgabe des Hauptvertrags vergütet werden, soweit zulässig.	• Additional, non-agreed effort may be remunerated in accordance with the main agreement, to the extent permissible.
6. Pflichten des Verantwortlichen	**6. Obligations of the Controller**
• Verantwortlich für Rechtsgrundlagen/Transparenzpflichten, Inhalte der Kundendaten, Konfiguration (Provider/Region/Retention/Logging) sowie die Bewertung der Eignung/Zulässigkeit von Outputs für eigene Zwecke.	• Responsible for legal bases/transparency obligations, the content of the Customer data, the configuration (provider/region/retention/logging), and the assessment of the suitability/permissibility of outputs for its own purposes.
• Datenminimierung: Der Verantwortliche stellt sicher, dass nur erforderliche personenbezogene Daten verarbeitet werden. Besondere Kategorien (Art. 9 DSGVO) nur, wenn rechtlich abgesichert und für den Use-Case erforderlich.	• Data minimization: The Controller ensures that only necessary personal data is processed. Special categories (Art. 9 GDPR) only where legally safeguarded and necessary for the use case.
• Kirchliche Einrichtungen (optional): Unterliegt der Verantwortliche dem kirchlichen Datenschutzrecht (Gesetz über den Kirchlichen Datenschutz – KDG (katholisch) bzw. Datenschutzgesetz der EKD – DSG-EKD (evangelisch)), so gelten dessen Bestimmungen ergänzend bzw. vorrangig. Die Parteien stellen die Verarbeitung entsprechend sicher, insbesondere hinsichtlich Meldewegen und der Zuständigkeit der jeweiligen kirchlichen Datenschutzaufsicht; Verweise auf die DSGVO gelten insoweit entsprechend für KDG/DSG-EKD.	• Religious (church) institutions (optional): Where the Controller is subject to ecclesiastical data protection law (the Catholic KDG or the Protestant DSG-EKD), its provisions apply additionally or with priority. The Parties shall ensure processing accordingly, in particular as regards reporting channels and the competence of the respective ecclesiastical data protection supervisory authority; references to the GDPR apply mutatis mutandis to the KDG/DSG-EKD.
7. Vertraulichkeit	**7. Confidentiality**
• EZTO stellt sicher, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind (Art. 28 Abs. 3 lit. b DSGVO).	• EZTO ensures that persons authorized to process are bound to confidentiality (Art. 28 (3) (b) GDPR).

DEUTSCH	ENGLISH (US)
• Need-to-know, rollenbasierte Zugriffe, angemessene Protokollierung.	• Need-to-know, role-based access, appropriate logging.
• Für Berufsgeheimnisträger gilt ergänzend Ziff. 20.	• For professional secrecy holders, Section 20 applies in addition.
8. Sicherheit der Verarbeitung (Art. 32 DSGVO)	**8. Security of processing (Art. 32 GDPR)**
• Angemessene TOMs gemäß Anlage 2 (u. a. Transportverschlüsselung TLS 1.3, Verschlüsselung ruhender Daten/Artefakte mit AES-256-GCM, RBAC/Least Privilege, Mandantentrennung, Secure SDLC, Monitoring/Incident Response). EZTO betreibt ein an ISO/IEC 27001 ausgerichtetes ISMS und befindet sich derzeit im Zertifizierungsprozess.	• Appropriate TOMs pursuant to Annex 2 (including TLS, encryption of data at rest at the infrastructure level, RBAC/least privilege, tenant separation, secure SDLC, monitoring/incident response). EZTO operates an ISO/IEC 27001-aligned ISMS and is currently undergoing certification.
• TOMs dürfen weiterentwickelt werden, sofern das Sicherheitsniveau insgesamt nicht unterschritten wird.	• TOMs may be further developed, provided the overall level of security is not reduced.
9. Hosting und Datenstandort (Default)	**9. Hosting and data location (default)**
• Standard-Hostingpfad: EU-Hosting bei Scaleway (Scaleway SAS, Frankreich), Region Paris (fr-par), soweit im jeweiligen Service/Plan technisch vorgesehen. Die produktive Verarbeitung von Kundendaten erfolgt innerhalb der EU/des EWR.	• Standard hosting path: EU hosting with Scaleway (Scaleway SAS, France), region Paris (fr-par), to the extent technically provided for in the respective service/plan. Productive processing of Customer data takes place within the EU/EEA.
• Abweichende Enterprise-Optionen können per Order Form vereinbart werden.	• Differing Enterprise options may be agreed via order form.
10. Unterstützung bei Betroffenenrechten	**10. Assistance with data subject rights**
• EZTO unterstützt den Verantwortlichen – soweit möglich und unter Berücksichtigung der Art der Verarbeitung – bei Betroffenenrechten (Art. 28 Abs. 3 lit. e DSGVO), insbesondere durch bereitgestellte Funktionen (Export/Löschung) und angemessene Mitwirkung.	• EZTO assists the Controller – to the extent possible and taking into account the nature of the processing – with data subject rights (Art. 28 (3) (e) GDPR), in particular through provided functions (export/deletion) and appropriate cooperation.
• Direkte Betroffenenanfragen an EZTO werden – soweit zulässig – an den Verantwortlichen weitergeleitet; keine eigenständige Beantwortung ohne Weisung.	• Direct data subject requests to EZTO are – where permissible – forwarded to the Controller; no independent response without instruction.
11. Unterstützung bei Compliance (Art. 28 Abs. 3 lit. f DSGVO)	**11. Assistance with compliance (Art. 28 (3) (f) GDPR)**
EZTO unterstützt den Verantwortlichen angemessen bei Art. 32–34, 35, 36 DSGVO. Zusätzlicher Aufwand kann nach Maßgabe des Hauptvertrags vergütet werden, soweit zulässig.	EZTO appropriately assists the Controller with Art. 32–34, 35, 36 GDPR. Additional effort may be remunerated in accordance with the main agreement, to the extent permissible.
12. Subprozessoren	**12. Subprocessors**
• Allgemeine Genehmigung (Art. 28 Abs. 2 DSGVO).	• General authorization (Art. 28 (2) GDPR).
• Aktuelle Liste: Anlage 3 sowie /legal/subprocessors.	• Current list: Annex 3 and /legal/subprocessors.
• Änderungen werden mindestens 30 Tage vor Wirksamwerden angekündigt, sofern nicht zwingende Sicherheitsgründe eine schnellere Änderung erfordern.	• Changes are announced at least 30 days before they take effect, unless compelling security reasons require a faster change.
• Einwände in Textform an legal@ezto.io.	• Objections in text form to legal@ezto.io.
• Bei berechtigten Einwänden: zumutbare Alternative oder Sonderkündigungsrecht für den betroffenen Service-Teil.	• In the event of legitimate objections: a reasonable alternative or a right of termination for the affected part of the service.
• Flow-down: EZTO verpflichtet Subprozessoren mindestens gleichwertig (Art. 28 Abs. 4 DSGVO).	• Flow-down: EZTO binds subprocessors at least equivalently (Art. 28 (4) GDPR).

DEUTSCH	ENGLISH (US)
• EZTO bleibt verantwortlich für die Einhaltung der Subprozessor-Pflichten im Rahmen der DSGVO, soweit gesetzlich zwingend.	• EZTO remains responsible for compliance with subprocessor obligations within the framework of the GDPR, to the extent legally mandatory.
13. KI-Provider / KI-Routing	**13. AI providers / AI routing**
• Zentre fungiert als Infrastruktur-, Orchestrierungs- und Governance-Schicht. Je nach Konfiguration werden Inhaltsdaten an KI-Provider zur Inference/Generierung weitergeleitet.	• Zentre acts as an infrastructure, orchestration, and governance layer. Depending on the configuration, content data is forwarded to AI providers for inference/generation.
• KI-Gateway Cortecs: Das Routing zu KI-Providern erfolgt standardmäßig über das EU-basierte KI-Gateway Cortecs (Cortecs GmbH, Wien), das Daten innerhalb der EU verarbeitet (Zero Data Retention, soweit verfügbar) und die KI-Provider als eigene Unterauftragsverarbeiter einbindet; maßgeblich ist insoweit die Unterauftragsverarbeiterliste von Cortecs (Anlage 3 / /legal/subprocessors).	• AI gateway Cortecs: Routing to AI providers takes place by default via the EU-based AI gateway Cortecs (Cortecs GmbH, Vienna), which processes data within the EU (zero data retention, where available) and integrates the AI providers as its own subprocessors; the current subprocessor list of Cortecs is decisive in this respect (Annex 3 / /legal/subprocessors).
• Web-Suche (Linkup): Sofern die Websuche-Funktion aktiviert ist, werden Suchanfragen an den Such-Provider Linkup (Linkup Technologies SAS, Frankreich) übermittelt; die Aktivierung gilt als dokumentierte Weisung; eine dauerhafte Speicherung der Anfragen durch EZTO erfolgt nicht. Für die Verarbeitung geschützter Geheimnisse (§ 203 StGB) gilt Ziff. 20: Im § 203-Modus ist die Websuche standardmäßig deaktiviert.	• Web search (Linkup): Where the web search function is activated, search queries are transmitted to the search provider Linkup (Linkup Technologies SAS, France); activation constitutes a documented instruction; no permanent storage of the queries by EZTO takes place. For the processing of protected secrets (Section 203 StGB), Section 20 applies: in Section 203 mode, web search is deactivated by default.
• Speicherung/Retention in Zentre (Chat/Workspace): Chat-/Workspace-Inhaltsdaten werden standardmäßig 90 Tage aufbewahrt; abweichende Konfigurationen (z. B. Enterprise/Private Cloud) gelten als dokumentierte Weisung. Nach Ablauf der Retention werden die Inhaltsdaten gelöscht oder – soweit technisch vorgesehen – irreversibel entfernt.	• Storage/retention in Zentre (chat/workspace): chat/workspace content data is retained for 90 days by default; differing configurations (e.g., Enterprise/Private Cloud) constitute a documented instruction. After expiry of the retention, the content data is deleted or – where technically provided for – irreversibly removed.
• Klarstellung: Eine zusätzliche dauerhafte Inhalts-„Log"-Speicherung erfolgt standardmäßig nicht, außer in den nachfolgenden Ausnahmefällen.	• Clarification: additional permanent content "logging" does not take place by default, except in the following exceptional cases.
• Ausnahmen (Logging/Support/Security): Inhaltsdaten können vorübergehend verarbeitet/gespeichert werden, soweit erforderlich für aktivierte Debug-/Logging-Optionen, Supportfälle auf dokumentierte Weisung oder sicherheitsrelevante Ereignisse – jeweils nach Maßgabe der Retention-Konfiguration und des Erforderlichkeitsgrundsatzes.	• Exceptions (logging/support/security): content data may be temporarily processed/stored to the extent necessary for activated debug/logging options, support cases on documented instruction, or security-relevant events – in each case in accordance with the retention configuration and the principle of necessity.
• Kein Training: EZTO nutzt Inhaltsdaten nicht zum Training eigener oder generischer Modelle. Eine Nutzung zu Trainingszwecken ist – soweit vertraglich vereinbart und technisch verfügbar (z. B. Zero Data Retention) – auch gegenüber den eingebundenen KI-Providern ausgeschlossen.	• No training: EZTO does not use content data to train its own or generic models. Use for training purposes is also excluded vis-à-vis the integrated AI providers – where contractually agreed and technically available (e.g., zero data retention).
• Provider-abhängige Verarbeitung: Die Verarbeitung durch KI-Provider ist providerabhängig; Auswahl/Aktivierung eines KI-Providers gilt als dokumentierte Weisung.	• Provider-dependent processing: processing by AI providers is provider-dependent; the selection/activation of an AI provider constitutes a documented instruction.

DEUTSCH	ENGLISH (US)
• Berufsgeheimnis: Für die Verarbeitung geschützter Geheimnisse i. S. d. § 203 StGB ist die Modellauswahl im § 203-Modus auf zugelassene EU-Endpunkte beschränkt (Ziff. 20; Stufe A „EU-kontrolliert" / Stufe B „EU-gehostet").	• Professional secrecy: For the processing of protected secrets within the meaning of Section 203 StGB, the model selection in Section 203 mode is restricted to authorized EU endpoints (Section 20; Tier A "EU-controlled" / Tier B "EU-hosted").
• Keine darüberhinausgehenden Garantien über Provider: EZTO schuldet hinsichtlich KI-Providern keine darüberhinausgehenden Garantien als (i) deren vertragliche Einbindung als Subprozessor, soweit vom jeweiligen Provider angeboten/ermöglicht, sowie (ii) die Weitergabe der vom Provider zugesagten Bedingungen/Erklärungen. Eine Verantwortung für Abweichungen des KI-Providers von dessen eigenen Zusagen besteht nur im Rahmen zwingender gesetzlicher Regelungen und im Übrigen nach Maßgabe der Haftungsregelungen des Hauptvertrags.	• No guarantees beyond this regarding providers: With respect to AI providers, EZTO owes no guarantees beyond (i) their contractual integration as a subprocessor, to the extent offered/enabled by the respective provider, and (ii) the passing-on of the terms/declarations promised by the provider. Responsibility for an AI provider's deviations from its own commitments exists only within the framework of mandatory statutory provisions and otherwise in accordance with the liability provisions of the main agreement.
• Kenntnis von Provider-Abweichungen: Erlangt EZTO Kenntnis von einer wesentlichen Abweichung eines KI-Providers von dessen Zusagen, ergreift EZTO angemessene Maßnahmen (z. B. Information des Verantwortlichen, Empfehlung/Umsetzung von Deaktivierung oder Routing-Blockierung), soweit technisch möglich und wirtschaftlich zumutbar.	• Knowledge of provider deviations: If EZTO becomes aware of a material deviation by an AI provider from its commitments, EZTO takes appropriate measures (e.g., informing the Controller, recommending/implementing deactivation or routing blocking), to the extent technically possible and economically reasonable.
14. Drittlandübermittlungen	**14. Third-country transfers**
• Im Standard-Setup (Scaleway/Paris, Cortecs/EU, ggf. Linkup/EU) finden regelmäßig keine Drittlandübermittlungen statt. Soweit Übermittlungen außerhalb EU/EWR erforderlich sind (z. B. bei Auswahl von Nicht-EU-Modellen), erfolgen sie unter Einhaltung Art. 44 ff. DSGVO (z. B. Angemessenheitsbeschluss, SCC).	• In the standard setup (Scaleway/Paris, Cortecs/EU, and Linkup/EU where applicable), no third-country transfers regularly take place. Where transfers outside the EU/EEA are necessary (e.g., upon selection of non-EU models), they take place in compliance with Art. 44 et seq. GDPR (e.g., adequacy decision, SCC).
• EZTO stellt dem Verantwortlichen auf Anfrage angemessene Informationen zu Transfer-Mechanismen und – soweit verfügbar – ergänzenden Maßnahmen bereit.	• Upon request, EZTO provides the Controller with appropriate information on transfer mechanisms and – where available – supplementary measures.
15. Löschung und Rückgabe	**15. Deletion and return**
• Während der Vertragslaufzeit erfolgt Löschung nach konfigurierter Retention (vgl. Ziff. 13 und Anlage 4).	• During the contract term, deletion takes place according to the configured retention (cf. Section 13 and Annex 4).
• Nach Vertragsende: Auf Wahl des Verantwortlichen (i) Rückgabe (Export in gängigen maschinenlesbaren Formaten, soweit verfügbar) oder (ii) Löschung.	• After contract termination: at the Controller's choice, (i) return (export in commonly used machine-readable formats, where available) or (ii) deletion.
• Produktionssysteme: Löschung bzw. Bereitstellung des Exports erfolgt grundsätzlich innerhalb von 30 Tagen nach Vertragsende bzw. nach Eingang einer entsprechenden Anforderung, soweit kein berechtigter Grund entgegensteht.	• Production systems: deletion or provision of the export generally takes place within 30 days of contract termination or upon receipt of a corresponding request, unless a legitimate reason prevents this.
• Backups: Daten können bis zum Ablauf technischer Lösch-/Überschreibzyklen in Backups enthalten sein; Backups werden nicht produktiv genutzt. Backup-Zyklen betragen typischerweise bis zu 90 Tage.	• Backups: data may be contained in backups until the expiry of technical deletion/overwrite cycles; backups are not used productively. Backup cycles are typically up to 90 days.
16. Datenschutzverletzungen	**16. Personal data breaches**

DEUTSCH	ENGLISH (US)
• EZTO informiert den Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnisnahme über Verletzungen des Schutzes personenbezogener Daten.	• EZTO informs the Controller without undue delay, at the latest within 48 hours of becoming aware, of breaches of the protection of personal data.
• Die Meldung enthält – soweit verfügbar – Art des Vorfalls, betroffene Datenkategorien, ungefähre Anzahl, wahrscheinliche Folgen, ergriffene/geplante Abhilfemaßnahmen und Kontaktstelle; Updates erfolgen, sobald neue Informationen vorliegen.	• The notification contains – where available – the nature of the incident, the categories of data affected, the approximate number, the likely consequences, the remedial measures taken/planned, and a point of contact; updates follow as soon as new information is available.
17. Behördenanfragen / Offenlegung	**17. Authority requests / disclosure**
• Soweit rechtlich zulässig, informiert EZTO den Verantwortlichen unverzüglich über rechtlich bindende Anfragen von Behörden zur Offenlegung von Kundendaten.	• To the extent legally permissible, EZTO informs the Controller without undue delay of legally binding requests from authorities to disclose Customer data.
• Offenlegungen werden – soweit möglich – auf das erforderliche Minimum beschränkt; EZTO wirkt an angemessenen Schutzmaßnahmen mit.	• Disclosures are – where possible – limited to the necessary minimum; EZTO cooperates in appropriate protective measures.
18. Nachweise und Audits	**18. Evidence and audits**
• EZTO stellt auf Anfrage angemessene Informationen zur Nachweisführung bereit (Art. 28 Abs. 3 lit. h DSGVO), z. B. TOM-Übersichten/Policies/Reports soweit vorhanden.	• Upon request, EZTO provides appropriate information for the provision of evidence (Art. 28 (3) (h) GDPR), e.g., TOM overviews/policies/reports where available.
• Audits sind nach vorheriger Ankündigung (mind. 60 Tage) und unter angemessenen Bedingungen zulässig; „remote-first". Vor-Ort-Audits nur bei begründetem Bedarf.	• Audits are permitted after prior notice (at least 60 days) and under appropriate conditions; "remote-first". On-site audits only where there is a justified need.
• Häufigkeit: max. 1 Audit pro Vertragsjahr, sofern kein Sicherheitsvorfall oder berechtigter Anlass vorliegt.	• Frequency: a maximum of 1 audit per contract year, unless there is a security incident or legitimate cause.
• Keine (automatisierten) Schwachstellen-/Penetrationstests gegen EZTO-Systeme ohne vorherige schriftliche Zustimmung.	• No (automated) vulnerability/penetration tests against EZTO systems without prior written consent.
• Audits unterliegen strenger Vertraulichkeit; keine Offenlegung von Betriebs-/Geschäftsgeheimnissen über das erforderliche Maß hinaus.	• Audits are subject to strict confidentiality; no disclosure of operating/trade secrets beyond the necessary extent.
• Kosten: Der Verantwortliche trägt seine Auditkosten; angemessener Aufwand von EZTO kann nach Maßgabe des Hauptvertrags berechnet werden, soweit zulässig.	• Costs: the Controller bears its audit costs; reasonable effort by EZTO may be charged in accordance with the main agreement, to the extent permissible.
19. Dokumentation	**19. Documentation**
EZTO führt – soweit erforderlich – ein Verzeichnis von Verarbeitungstätigkeiten als Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO) und stellt dem Verantwortlichen auf Anfrage angemessene Informationen/Auszüge daraus zur Verfügung, soweit zur Erfüllung der Rechenschaftspflicht erforderlich und keine berechtigten Geheimhaltungsinteressen oder Geschäftsgeheimnisse Dritter entgegenstehen.	EZTO maintains – to the extent required – a record of processing activities as a processor (Art. 30 (2) GDPR) and provides the Controller upon request with appropriate information/extracts therefrom, to the extent necessary to fulfil the accountability obligation and provided no legitimate confidentiality interests or third-party trade secrets conflict.
20. Mitwirkung an Berufsgeheimnissen (§ 203 StGB; berufsrechtliche Vorgaben)	**20. Involvement in professional secrecy (Section 203 StGB; professional law requirements)**

DEUTSCH	ENGLISH (US)
• Anwendungsbereich: Soweit der Verantwortliche einer strafbewehrten Verschwiegenheitspflicht nach § 203 StGB (bzw. § 121 öStGB, Art. 321 CH-StGB) unterliegt und Zentre zur Verarbeitung geschützter Geheimnisse einsetzt, wird EZTO als „sonstige mitwirkende Person" i. S. d. § 203 Abs. 3 StGB tätig. Ergänzend gelten die einschlägigen berufsrechtlichen Vorgaben, insbesondere § 43e BRAO i. V. m. § 2 BORA (Rechtsanwälte) und § 62a StBerG (Steuerberater).	• Scope: To the extent the Controller is subject to a criminally sanctioned confidentiality obligation under Section 203 StGB (or Section 121 of the Austrian Criminal Code, Article 321 of the Swiss Criminal Code) and uses Zentre to process protected secrets, EZTO acts as an "other contributing person" within the meaning of Section 203 (3) StGB. In addition, the relevant professional-law requirements apply, in particular Section 43e of the German Federal Lawyers' Act (BRAO) in conjunction with Section 2 of the Professional Code for Lawyers (BORA) and Section 62a of the German Tax Advisory Act (StBerG).
• Verschwiegenheit & Belehrung: EZTO und die zur Verarbeitung befugten Personen werden in Textform zur Geheimhaltung verpflichtet und über die strafrechtlichen Folgen (§ 203 Abs. 4 StGB) belehrt; die Verpflichtung gilt nach Vertragsende fort.	• Confidentiality & instruction: EZTO and the persons authorized to process are bound to confidentiality in text form and instructed about the criminal consequences (Section 203 (4) StGB); the obligation continues after contract termination.
• Flow-down: EZTO verpflichtet Subprozessoren und KI-Provider, die auf geschützte Geheimnisse zugreifen können, in Textform gleichwertig zur Verschwiegenheit, soweit für die Leistung erforderlich und vom jeweiligen Dienstleister angeboten/ermöglicht.	• Flow-down: EZTO binds subprocessors and AI providers that may access protected secrets to equivalent confidentiality in text form, to the extent necessary for the service and offered/enabled by the respective provider.
• § 203-Modus (Stufen A/B): Die Verarbeitung geschützter Geheimnisse ist nur in einer hierfür geeigneten Konfiguration zulässig (EU-Hosting, EU-Routing, Zero Data Retention, deaktivierte Websuche, ausschließlich zugelassene Modellanbieter). Der Verantwortliche wählt die Stufe: A „EU-kontrolliert" (nur EU-kontrollierte/EU-selbstgehostete Modelle) oder B „EU-gehostet" (zusätzlich EU-gehostete Endpunkte); in beiden Stufen gelten Zero Data Retention und deaktivierte Websuche.	• Section 203 mode (Tiers A/B): The processing of protected secrets is permitted only in a suitable configuration (EU hosting, EU routing, zero data retention, deactivated web search, exclusively authorized model providers). The Controller selects the tier: A "EU-controlled" (only EU-controlled/EU-self-hosted models) or B "EU-hosted" (additionally EU-hosted endpoints); in both tiers, zero data retention applies and web search is deactivated.
• Web-Suche im § 203-Modus: Die Websuche ist im § 203-Modus in beiden Stufen (EU-kontrolliert und EU-gehostet) deaktiviert.	• Web search in Section 203 mode: Web search is deactivated in Section 203 mode in both tiers (EU-controlled and EU-hosted).
• Mandatstrennung (separater Tenant): Geschützte Geheimnisse werden in einem vom Normalbetrieb physisch getrennten Tenant mit eigener, isolierter Wissensbasis/Index verarbeitet. Es besteht keine gemeinsame Wissensbasis und kein tenantübergreifender Datentransfer/keine tenantübergreifende Suche; ein Tenant-Wechsel ist ein reiner Identitäts-/Navigationswechsel (z. B. via SSO) ohne Inhaltsübertragung. Die Zuordnung von Daten zum § 203-Tenant obliegt dem Verantwortlichen (im Zweifel § 203-Tenant); mandatsfreie/interne Vorgänge können im Normal-Tenant verarbeitet werden.	• Tenant separation (separate tenant): Protected secrets are processed in a tenant physically separated from normal operation, with its own, isolated knowledge base/index. There is no shared knowledge base and no cross-tenant data transfer/cross-tenant search; a tenant switch is a pure identity/navigation switch (e.g., via SSO) without content transfer. The assignment of data to the Section 203 tenant is the responsibility of the Controller (in case of doubt, the Section 203 tenant); secrecy-free/internal matters may be processed in the normal tenant.
• Ergänzende Vereinbarung: Auf Wunsch schließt EZTO eine gesonderte, auch elektronisch abschließbare Verschwiegenheitsvereinbarung nach § 203 StGB; im Konfliktfall gehen deren Regelungen für § 203-Sachverhalte vor.	• Supplementary agreement: Upon request, EZTO concludes a separate confidentiality agreement under Section 203 StGB, which may also be concluded electronically; in case of conflict, its provisions prevail for Section 203 matters.
21. Schlussbestimmungen	**21. Final provisions**
• Recht und Gerichtsstand richten sich nach dem Hauptvertrag (deutsches Recht; Gerichtsstand Mainz, soweit zulässig).	• Governing law and place of jurisdiction are governed by the main agreement (German law; place of jurisdiction Mainz, to the extent permissible).

DEUTSCH	ENGLISH (US)
• Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt; an die Stelle der unwirksamen Regelung tritt eine wirksame, die dem Zweck am nächsten kommt und den Anforderungen der DSGVO genügt.	• Should any provision of this DPA be or become invalid, the validity of the remaining provisions remains unaffected; the invalid provision is replaced by a valid one that comes closest to its purpose and meets the requirements of the GDPR.
• Änderungen und Ergänzungen bedürfen mindestens der Textform.	• Amendments and supplements require at least text form.
3. Anlagen zum AVV (generiert)	**Annexes to the DPA**

DEUTSCH	ENGLISH (US)
Anlage 1 — Beschreibung der Verarbeitung (Art. 28 Abs. 3 DSGVO)	**Annex 1 — Description of the processing (Art. 28 (3) GDPR)**
Gegenstand der Verarbeitung: Bereitstellung und Betrieb der KI-Orchestrierungs- und Governance-Plattform „Zentre" (Chat-Assistent, Agenten, RAG/Wissenstool) als SaaS.	Subject matter of the processing: provision and operation of the AI orchestration and governance platform "Zentre" (chat assistant, agents, RAG/knowledge tool) as SaaS.
Art der Verarbeitung: automatisiertes Erheben, Erfassen, Speichern, Anzeigen, Strukturieren, Übermitteln (an KI-Gateway/KI-Provider sowie – sofern aktiviert – an den Such-Provider), Einschränken und Löschen.	Nature of the processing: automated collection, recording, storage, display, structuring, transmission (to the AI gateway/AI providers and – where activated – to the search provider), restriction, and deletion.
Zweck: Erbringung der vertraglich vereinbarten Leistungen, Nutzer-/Zugriffsverwaltung, Support/Fehleranalyse, Sicherheit/Missbrauchsprävention/Incident-Handling.	Purpose: provision of the contractually agreed services, user/access management, support/error analysis, security/abuse prevention/incident handling.
Kategorien personenbezogener Daten:	Categories of personal data:
• Account-/Organisationsdaten (Name, dienstliche E-Mail, Organisation, Rollen/Berechtigungen);	• account/organization data (name, business email, organization, roles/permissions);
• Nutzungs-, Abrechnungs-, Sicherheits- und technische Metadaten (Zeitstempel, Request-IDs, Konfiguration, Token-/Volumenmetriken, Fehlermeldungen, IP soweit erforderlich);	• usage, billing, security, and technical metadata (timestamps, request IDs, configuration, token/volume metrics, error messages, IP where necessary);
• Inhaltsdaten (Prompts, Uploads, Dokumente, Outputs);	• content data (prompts, uploads, documents, outputs);
• Web-Suchanfragen (nur sofern die Websuche aktiviert ist).	• web search queries (only where web search is activated).
Kategorien betroffener Personen: Nutzer des Verantwortlichen (Beschäftigte); ggf. in Inhalts-/Suchdaten genannte Dritte (z. B. Mandanten, Patienten, Kunden, Geschäftspartner des Verantwortlichen) – abhängig von den Eingaben des Verantwortlichen.	Categories of data subjects: users of the Controller (employees); where applicable, third parties named in content/search data (e.g., clients, patients, customers, business partners of the Controller) – depending on the Controller's inputs.
Besondere Kategorien (Art. 9 DSGVO): nur, soweit der Verantwortliche solche Daten eingibt; dies liegt in der Verantwortung und auf Weisung des Verantwortlichen (vgl. Ziff. 6).	Special categories (Art. 9 GDPR): only where the Controller inputs such data; this is the responsibility of and on the instruction of the Controller (cf. Section 6).
Dauer: für die Laufzeit des Hauptvertrags; Chat-/Workspace-Inhaltsdaten 90 Tage; anschließend Löschung/Rückgabe gemäß Ziff. 15 und Anlage 4.	Duration: for the term of the main agreement; chat/workspace content data 90 days; thereafter deletion/return pursuant to Section 15 and Annex 4.
Ort der Verarbeitung: EU/EWR – Hosting Scaleway (Frankreich, Paris fr-par); KI-Routing über Cortecs (EU); Websuche über Linkup (EU). Drittlandübermittlung nur nach Ziff. 14.	Place of processing: EU/EEA – hosting Scaleway (France, Paris fr-par); AI routing via Cortecs (EU); web search via Linkup (EU). Third-country transfers only pursuant to Section 14.
Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)	**Annex 2 — Technical and organizational measures (Art. 32 GDPR)**
EZTO betreibt ein an ISO/IEC 27001 ausgerichtetes Informationssicherheits-Managementsystem (ISMS) und befindet sich derzeit im Zertifizierungsprozess nach ISO/IEC 27001. Bis zur Erteilung werden Nachweise (TOM-Dokumentation, Pentest-Berichte, Sicherheitsfragebögen) auf Anfrage bereitgestellt.	EZTO operates an ISO/IEC 27001-aligned information security management system (ISMS) and is currently undergoing ISO/IEC 27001 certification. Pending issuance, evidence (TOM documentation, pen-test reports, security questionnaires) is provided upon request.
1. Vertraulichkeit	1. Confidentiality
• Zutrittskontrolle: Hosting in zertifizierten EU-Rechenzentren (Scaleway); physische Sicherung durch den Infrastruktur-Anbieter.	• Physical access control: hosting in certified EU data centers (Scaleway); physical security by the infrastructure provider.

DEUTSCH	ENGLISH (US)
• Zugangskontrolle: Authentifizierung mit Multi-Faktor-Authentisierung (MFA) für administrative Zugänge; rollenbasierte Rechtevergabe (RBAC) nach dem Least-Privilege-Prinzip.	• System access control: authentication with multi-factor authentication (MFA) for administrative access; role-based assignment of rights (RBAC) according to the least-privilege principle.
• Zugriffskontrolle: Need-to-know, rollenbasierte Zugriffe, Zugriffsprotokollierung; Beschränkung administrativer Zugriffe.	• Data access control: need-to-know, role-based access, access logging; restriction of administrative access.
• Trennungskontrolle: mandantengetrennte Verarbeitung (logische Mandantentrennung).	• Separation control: tenant-separated processing (logical tenant separation).
• Pseudonymisierung/Minimierung: soweit für den Zweck möglich.	• Pseudonymization/minimization: to the extent possible for the purpose.
2. Integrität	2. Integrity
• Weitergabekontrolle: Transportverschlüsselung (TLS 1.3) für Daten in Übertragung.	• Transfer control: transport encryption (TLS 1.3) for data in transit.
• Verschlüsselung ruhender Daten/Artefakte mit AES-256-GCM.	• Encryption of data/artifacts at rest with AES-256-GCM.
• Eingabekontrolle: Protokollierung relevanter Aktionen.	• Input control: logging of relevant actions.
3. Verfügbarkeit und Belastbarkeit	3. Availability and resilience
• Datensicherung (Backups) mit definierten Lösch-/Überschreibzyklen (bis 90 Tage);	• Data backup (backups) with defined deletion/overwrite cycles (up to 90 days);
• Monitoring, Incident-Response-Prozess; Business-Continuity-/Notfallkonzept.	• monitoring, incident response process; business continuity/emergency plan.
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	4. Procedures for regular review, assessment, and evaluation
• ISMS nach ISO/IEC 27001 (in Zertifizierung); regelmäßige Penetrationstests; Schwachstellenmanagement; Secure Software Development Lifecycle (Secure SDLC).	• ISMS pursuant to ISO/IEC 27001 (undergoing certification); regular penetration tests; vulnerability management; secure software development lifecycle (secure SDLC).
• Auftrags-/Subprozessor-Kontrolle: sorgfältige Auswahl, vertragliche Bindung mind. gleichwertig (Art. 28 Abs. 4 DSGVO), Flow-down.	• Order/subprocessor control: careful selection, contractual binding at least equivalently (Art. 28 (4) GDPR), flow-down.
5. Schlüsselverwaltung: anbieterverwaltete Schlüssel; ein „Bring Your Own Key" (BYOK) wird derzeit nicht angeboten.	5. Key management: provider-managed keys; "Bring Your Own Key" (BYOK) is not currently offered.
Anlage 3 — Unterauftragsverarbeiter	**Annex 3 — Subprocessors**
Maßgeblich ist die jeweils aktuelle Subprozessorenliste (/legal/subprocessors). Eingesetzt werden insbesondere:	The current subprocessor list (/legal/subprocessors) is decisive. The following are engaged in particular:

Anbieter	Zweck	Standort/Land	Transfers
Scaleway (Scaleway SAS)	Hosting/Infrastruktur	EU (Frankreich, Paris fr-par)	n/a (EU)
Cortecs (Cortecs GmbH)	KI-Gateway/Routing (EU-Routing, ZDR)	EU (Österreich)	i. d. R. keine; soweit erforderlich SCC
Linkup (Linkup Technologies SAS)	Web-Suche (sofern aktiviert; ZDR)	EU (Frankreich)	n/a (EU)
Infomaniak (Infomaniak Network SA)	Transaktionale E-Mails	Schweiz/EU	Angemessenheitsbeschluss (CH)
Stripe (Stripe Payments Europe Ltd.)	Abrechnung/Zahlung	EU (Irland)/USA	SCC, soweit erforderlich
Usercentrics (Usercentrics GmbH)	Consent-Management (Website)	EU (Deutschland)	n/a (EU)
Plausible (Plausible Insights OÜ)	Reichweitenmessung (Website)	EU	n/a (EU)

DEUTSCH **ENGLISH (US)**

Provider	Purpose	Location/Country	Transfers
Scaleway (Scaleway SAS)	Hosting/infrastructure	EU (France, Paris fr-par)	n/a (EU)
Cortecs (Cortecs GmbH)	AI gateway/routing (EU routing, ZDR)	EU (Austria)	generally none; SCC where necessary
Linkup (Linkup Technologies SAS)	Web search (where activated; ZDR)	EU (France)	n/a (EU)
Infomaniak (Infomaniak Network SA)	Transactional emails	Switzerland/EU	adequacy decision (CH)
Stripe (Stripe Payments Europe Ltd.)	Billing/payment	EU (Ireland)/USA	SCC where necessary
Usercentrics (Usercentrics GmbH)	Consent management (website)	EU (Germany)	n/a (EU)
Plausible (Plausible Insights OÜ)	Analytics (website)	EU	n/a (EU)

Die KI-Modellanbieter werden über das Gateway Cortecs als dessen Unterauftragsverarbeiter eingebunden (maßgeblich: Cortecs-Unterauftragsverarbeiterliste). Änderungen werden mind. 30 Tage vorher angekündigt (Ziff. 12).

Anlage 4 — Aufbewahrung und Löschung

• Chat-/Workspace-Inhaltsdaten: standardmäßig 90 Tage (einheitlich); abweichend nur bei Enterprise/Private Cloud nach gesonderter Vereinbarung. Nach Ablauf Löschung bzw. irreversible Entfernung.

• Backups: technische Lösch-/Überschreibzyklen typischerweise bis 90 Tage; keine produktive Nutzung.

• Metadaten/Sicherheitsprotokolle: nur solange erforderlich (Sicherheit, Missbrauchsprävention, Incident-Analyse); ggf. länger bei Rechtsansprüchen/gesetzlichen Pflichten.

• Web-Suchanfragen: keine dauerhafte Speicherung durch EZTO.

• Nach Vertragsende: Export in gängigem, maschinenlesbarem Format für 30 Tage; anschließend Löschung gemäß Ziff. 15.

The AI model providers are integrated via the Cortecs gateway as its subprocessors (decisive: Cortecs subprocessor list). Changes are announced at least 30 days in advance (Section 12).

Annex 4 — Retention and deletion

• Chat/workspace content data: 90 days by default (uniform); differing only for Enterprise/Private Cloud by separate agreement. After expiry, deletion or irreversible removal.

• Backups: technical deletion/overwrite cycles typically up to 90 days; no productive use.

• Metadata/security logs: only as long as necessary (security, abuse prevention, incident analysis); potentially longer in the event of legal claims/statutory obligations.

• Web search queries: no permanent storage by EZTO.

• After contract termination: export in a commonly used, machine-readable format for 30 days; thereafter deletion pursuant to Section 15.