

ZENTRE – Auftragsverarbeitungsvertrag (AVV / DPA)

Letzte Aktualisierung: 15. Jul 2026

Das Wichtigste in Kürze (*unverbindliche Orientierung — maßgeblich ist der Vertragstext*): Ihre Daten werden ausschließlich in der EU verarbeitet (Hosting: Scaleway, Paris) · KI-Anfragen laufen über das EU-Gateway Cortecs, mit Zero Data Retention soweit verfügbar · Ihre Inhalte werden nicht zum Training von KI-Modellen genutzt · Chats werden nach 90 Tagen gelöscht (vorher exportierbar) · Neue Subprozessoren kündigen wir 14 Tage vorher an; Sie können widersprechen · Datenschutzverletzungen melden wir binnen 48 Stunden · Für Berufsgeheimnisträger gilt zusätzlich Ziff. 20 (§ 203-Modus).

Wer ist wer: „Verantwortlicher“ in diesem AVV sind Sie — der Kunde im Sinne der AGB. „Auftragsverarbeiter“ ist EZTO.

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.
- **„Plan“:** die im Order Form/Hauptvertrag benannte Seat-basierte Lizenz (ein Plan, pro Nutzer); daneben bestehen Enterprise- und Private-Cloud-Optionen nach gesonderter Vereinbarung.

4. Gegenstand, Art, Zweck, Dauer

- Gegenstand ist die Verarbeitung von Kundendaten zur Bereitstellung, zum sicheren Betrieb, zur Wartung, Support-Leistung sowie zur Weiterentwicklung von Zentre.
- Dauer: Laufzeit des Hauptvertrags; anschließend Löschung/Rückgabe gemäß Ziff. 15.
- Details zu Art/Zweck/Datenkategorien/Betroffenen: Anlage 1.

5. Weisungen und Weisungsmanagement

- Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO).
- Dokumentierte Weisungen umfassen: (i) Hauptvertrag/AVV, (ii) Produkt- und Account-Konfigurationen (Provider-Auswahl, Allow/Deny, Routing, Regionen, Retention, Logging), (iii) Einzelweisungen eines Administrators des Verantwortlichen in Textform an legal@zentre.ai; Weisungen einzelner Nutzer kann EZTO an die Administratoren verweisen.
- Offensichtlich rechtswidrige Weisungen werden nicht ausgeführt; der Verantwortliche wird informiert.
- Zusätzlicher, nicht vereinbarter Aufwand kann nach Maßgabe des Hauptvertrags vergütet werden, soweit zulässig.

6. Pflichten des Verantwortlichen

- Verantwortlich für Rechtsgrundlagen/Transparenzpflichten, Inhalte der Kundendaten, Konfiguration (Provider/Region/Retention/Logging) sowie die Bewertung der Eignung/Zulässigkeit von Outputs für eigene Zwecke.
- 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.
- 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.

7. Vertraulichkeit

- EZTO stellt sicher, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind (Art. 28 Abs. 3 lit. b DSGVO).
- Need-to-know, rollenbasierte Zugriffe, angemessene Protokollierung.
- Für Berufsgeheimnisträger gilt ergänzend Ziff. 20.

8. Sicherheit der Verarbeitung (Art. 32 DSGVO)

- Angemessene TOMs gemäß Anlage 2 (u. a. Transportverschlüsselung TLS 1.2 oder höher, Verschlüsselung ruhender Daten/Artefakte mit AES-256 (mindestens), RBAC/Least Privilege, Mandantentrennung, Secure SDLC, Monitoring/Incident Response). EZTO betreibt ein an ISO/IEC 27001 ausgerichtetes ISMS; die Zertifizierung läuft; den aktuellen Status veröffentlicht EZTO im Trust Center.
- TOMs dürfen weiterentwickelt werden, sofern das Sicherheitsniveau insgesamt nicht unterschritten wird.

9. Hosting und Datenstandort (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.
- Abweichende Enterprise-Optionen können per Order Form vereinbart werden.

10. Unterstützung bei Betroffenenrechten

- 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.
- Direkte Betroffenenanfragen an EZTO werden – soweit zulässig – an den Verantwortlichen weitergeleitet; keine eigenständige Beantwortung ohne Weisung.

11. Unterstützung bei Compliance (Art. 28 Abs. 3 lit. f DSGVO)

EZTO unterstützt den Verantwortlichen angemessen bei Art. 32–34, 35, 36 DSGVO — vorrangig durch die im Trust Center bereitgestellte Dokumentation (TOM, Datenfluss-Dokument, Subprozessorenliste). Darüber hinausgehende individuelle Mitwirkung (z. B. Ausfüllen kundenspezifischer DSFA-Vorlagen, Workshops) wird nach Maßgabe des Hauptvertrags angemessen vergütet, soweit zulässig.

12. Subprozessoren

- Allgemeine Genehmigung (Art. 28 Abs. 2 DSGVO).
- Aktuelle Liste: Anlage 3 sowie die im Trust Center (zentre.ai/trust-center) veröffentlichte Subprozessorenliste.
- Änderungen (Neubeauftragung oder Ersetzung von Subprozessoren) werden mindestens vierzehn (14) Tage vor Wirksamwerden in Textform an die im Account hinterlegte Administrator-E-Mail-Adresse angekündigt und ergänzend über die im Trust Center veröffentlichte Subprozessorenliste bekannt gemacht; die Ankündigungsfrist beginnt mit Absendung der E-Mail. Der Verantwortliche hält die Adresse aktuell. Zwingende Sicherheitsgründe können eine kurzfristigere Änderung erfordern; in diesem Fall wird der Verantwortliche unverzüglich informiert. Der Verantwortliche kann der Änderung innerhalb der Ankündigungsfrist in Textform an legal@zentre.ai widersprechen (Art. 28 Abs. 2 DSGVO).
- Bei berechtigten Einwänden: zumutbare Alternative oder Sonderkündigungsrecht für den betroffenen Service-Teil.
- Flow-down: EZTO verpflichtet Subprozessoren mindestens gleichwertig (Art. 28 Abs. 4 DSGVO).
- EZTO bleibt verantwortlich für die Einhaltung der Subprozessor-Pflichten im Rahmen der DSGVO, soweit gesetzlich zwingend.

13. KI-Provider / KI-Routing

- Zentre fungiert als Infrastruktur-, Orchestrierungs- und Governance-Schicht. Je nach Konfiguration werden Inhaltsdaten an KI-Provider zur Inference/Generierung weitergeleitet.
- 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 / Trust Center).
- 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 deaktiviert.

- **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.
- **Klarstellung:** Eine zusätzliche dauerhafte Inhalts-„Log“-Speicherung erfolgt standardmäßig nicht, außer in den nachfolgenden Ausnahmefällen.
- **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.
- **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.
- **Provider-abhängige Verarbeitung:** Die Verarbeitung durch KI-Provider ist providerabhängig; Auswahl/Aktivierung eines KI-Providers gilt als dokumentierte Weisung.
- **Berufsgeheimnis:** Für die Verarbeitung geschützter Geheimnisse i. S. d. § 203 StGB ist die Modellauswahl im § 203-Modus ausschließlich auf zugelassene EU-kontrollierte bzw. EU-selbstgehostete Endpunkte beschränkt (Ziff. 20).
- **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.
- **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.

14. Drittlandübermittlungen

- 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).
- EZTO stellt dem Verantwortlichen auf Anfrage angemessene Informationen zu Transfer-Mechanismen und – soweit verfügbar – ergänzenden Maßnahmen bereit.

15. Löschung und Rückgabe

- Während der Vertragslaufzeit erfolgt Löschung nach konfigurierter Retention (vgl. Ziff. 13 und Anlage 4).
- Nach Vertragsende: Auf Wahl des Verantwortlichen (i) Rückgabe (Export in gängigen maschinenlesbaren Formaten, soweit verfügbar) oder (ii) Löschung.
- **Produktionssysteme:** Die Bereitstellung des Exports erfolgt grundsätzlich innerhalb von 30 Tagen nach Eingang der Anforderung. Die Löschung erfolgt nach Ablauf der 30-tägigen Abruffrist (Anlage 4), frühestens jedoch nach vollständiger Bereitstellung eines fristgerecht angeforderten Exports; bei Inanspruchnahme einer vereinbarten Exit-Unterstützung (z. B. Ziff. 8 Abs. 4 DORA-Addendum) frühestens nach deren Abschluss.
- **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. Werden Daten aus Backups wiederhergestellt, werden zuvor gelöschte Daten unverzüglich erneut gelöscht.

16. Datenschutzverletzungen

- EZTO informiert den Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnisnahme über Verletzungen des Schutzes personenbezogener Daten.
- 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.

17. Behördenanfragen / Offenlegung

- Soweit rechtlich zulässig, informiert EZTO den Verantwortlichen unverzüglich über rechtlich bindende Anfragen von Behörden zur Offenlegung von Kundendaten.
- Offenlegungen werden – soweit möglich – auf das erforderliche Minimum beschränkt; EZTO wirkt an angemessenen Schutzmaßnahmen mit.

18. Nachweise und 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.
- Audits sind nach vorheriger Ankündigung (mind. 60 Tage) und unter angemessenen Bedingungen zulässig; „remote-first“ auf Grundlage des Standard-Nachweispakets (Anlage 2). Vor-Ort-Inspektionen finden nur statt, soweit Remote-Audit und Nachweise im Einzelfall nachweislich nicht ausreichen oder eine zuständige Aufsichtsbehörde dies verbindlich anordnet; weitergehende Vor-Ort-Rechte können im Enterprise-Order-Form vereinbart werden.
- Häufigkeit: max. 1 Audit pro Vertragsjahr, sofern kein Sicherheitsvorfall oder berechtigter Anlass vorliegt.
- Keine (automatisierten) Schwachstellen-/Penetrationstests gegen EZTO-Systeme ohne vorherige Zustimmung in Textform.
- Audits unterliegen strenger Vertraulichkeit; keine Offenlegung von Betriebs-/Geschäftsgeheimnissen über das erforderliche Maß hinaus.
- Kosten: Der Verantwortliche trägt seine Auditkosten; angemessener Aufwand von EZTO kann nach Maßgabe des Hauptvertrags berechnet werden, soweit zulässig.

19. Dokumentation

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.

20. Mitwirkung an Berufsgeheimnissen (§ 203 StGB; berufsrechtliche Vorgaben)

- Anwendungsbereich: Soweit der Verantwortliche einer strafbewehrten Verschwiegenheitspflicht nach § 203 StGB (Österreich: berufsrechtliche Verschwiegenheitspflichten wie § 80 WTBG 2017 oder § 9 RAO sowie – insbesondere für Gesundheitsberufe – § 121 öStGB; Schweiz: Art. 321 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), § 62a StBerG (Steuerberater), § 43 Abs. 1 und § 50 WPO (Wirtschaftsprüfer und vereidigte Buchprüfer), § 18 und § 26 BNotO (Notare), § 39a i. V. m. § 39c PAO (Patentanwälte) sowie § 80 WTBG 2017 (österreichische Wirtschaftstreuhänder).
- 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.

- Flow-down: EZTO verpflichtet Subprozessoren und KI-Provider, die auf geschützte Geheimnisse zugreifen können, vor ihrem Einsatz in Textform gleichwertig zur Verschwiegenheit. Kann eine weitere mitwirkende Person nicht gleichwertig verpflichtet werden, wird sie für die Verarbeitung geschützter Geheimnisse nicht eingesetzt.
- § 203-Modus: Die Verarbeitung geschützter Geheimnisse ist nur in einer hierfür geeigneten Konfiguration zulässig: EU-Hosting, EU-Routing, Zero Data Retention, deaktivierte Websuche sowie ausschließlich autorisierte EU-kontrollierte bzw. EU-selbst-gehostete Modellanbieter. Endpunkte von Anbietern mit Nicht-EU-Konzernobergesellschaft stehen im § 203-Modus nicht zur Verfügung.
- Web-Suche im § 203-Modus: Die Websuche ist im § 203-Modus deaktiviert.
- Mandatstrennung (separater Tenant): Geschützte Geheimnisse werden in einem vom Normalbetrieb getrennten, dedizierten und logisch isolierten Tenant mit eigener, isolierter Wissensbasis/Index verarbeitet. Eine physisch getrennte Umgebung (Private Cloud/On-Premises) kann als Enterprise-Option gesondert vereinbart werden. 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.
- Ergänzende Vereinbarung: Die Verarbeitung geschützter Geheimnisse setzt den Abschluss einer gesonderten, auch elektronisch abschließbaren Verschwiegenheitsvereinbarung nach § 203 StGB voraus; EZTO stellt diese bereit. Im Konfliktfall gehen deren Regelungen für § 203-Sachverhalte vor.
- Modelländerungen im § 203-Modus: Für die Entfernung oder den Ersatz der im § 203-Modus zugelassenen Modellanbieter gilt abweichend von Ziff. 12 die 30-Tage-Frist nach § 7 Abs. 4 der Verschwiegenheitsvereinbarung.

21. Schlussbestimmungen

- Recht und Gerichtsstand richten sich nach dem Hauptvertrag (deutsches Recht; Gerichtsstand Mainz, soweit zulässig).
- 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.
- Änderungen und Ergänzungen bedürfen mindestens der Textform.

Anlagen zum AVV

Anlage 1 — Beschreibung der Verarbeitung (Art. 28 Abs. 3 DSGVO)

Gegenstand der Verarbeitung: Bereitstellung und Betrieb der KI-Orchestrierungs- und Governance-Plattform „Zentre“ (Chat-Assistent, Agenten, RAG/Wissenstool) als 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.

Zweck: Erbringung der vertraglich vereinbarten Leistungen, Nutzer-/Zugriffsverwaltung, Support/Fehleranalyse, Sicherheit/Missbrauchsprävention/Incident-Handling.

Kategorien personenbezogener Daten: - Account-/Organisationsdaten (Name, dienstliche E-Mail, Organisation, Rollen/Berechtigungen); - Nutzungs-, Abrechnungs-, Sicherheits- und technische Metadaten (Zeitstempel, Request-IDs, Konfiguration, Token-/Volumenmetriken, Fehlermeldungen, IP soweit erforderlich); - Inhaltsdaten (Prompts, Uploads, Dokumente, Outputs); - Web-Suchanfragen (nur sofern die Websuche aktiviert ist).

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.

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).

Dauer: für die Laufzeit des Hauptvertrags; Chat-/Workspace-Inhaltsdaten 90 Tage; anschließend Löschung/Rückgabe gemäß Ziff. 15 und Anlage 4.

Ort der Verarbeitung: EU/EWR – Hosting Scaleway (Frankreich, Paris fr-par); Content Delivery über Bunny CDN (BunnyWay d.o.o., Slowenien, EU – Auslieferung beschränkt auf EU/EWR-Standorte); KI-Routing über Cortecs (EU); Websuche über Linkup (EU). Drittlandübermittlung nur nach Ziff. 14.

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

EZTO betreibt ein an ISO/IEC 27001 ausgerichtetes Informationssicherheits-Managementsystem (ISMS) und befindet sich derzeit im Zertifizierungsprozess nach ISO/IEC 27001. Das Standard-Nachweispaket (TOM-Dokumentation, Sicherheits-Whitepaper, Management-Zusammenfassung aktueller Penetrationstests, von EZTO ausgefüllter Standard-Sicherheitsfragebogen) steht im Trust Center zum Abruf bereit. Vollständige Penetrationstest-Berichte sowie die Beantwortung kundenindividueller Fragebögen und Vorlagen erfolgen nur nach gesonderter Vereinbarung (Enterprise/Order Form), unter Vertraulichkeit und gegen angemessene Vergütung.

1. Vertraulichkeit - Zutrittskontrolle: Hosting in zertifizierten EU-Rechenzentren (Scaleway); physische Sicherung durch den Infrastruktur-Anbieter. - Zugangskontrolle: Authentifizierung mit Multi-Faktor-Authentisierung (MFA) für administrative Zugänge; rollenbasierte Rechtevergabe (RBAC) nach dem Least-Privilege-Prinzip. - Zugriffskontrolle: Need-to-know, rollenbasierte Zugriffe, Zugriffsprotokollierung; Beschränkung administrativer Zugriffe. - Trennungskontrolle: mandantengetrennte Verarbeitung (logische Mandantentrennung). - Pseudonymisierung/Minimierung: soweit für den Zweck möglich.

2. Integrität - Weitergabekontrolle: Transportverschlüsselung (TLS 1.2 oder höher) für Daten in Übertragung. - Verschlüsselung ruhender Daten/Artefakte mit AES-256 (mindestens). - Eingabekontrolle: Protokollierung relevanter Aktionen.

3. Verfügbarkeit und Belastbarkeit - Datensicherung (Backups) mit definierten Lösch-/Überschreibzyklen (bis 90 Tage); - Monitoring, Incident-Response-Prozess; Business-Continuity-/Notfallkonzept.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung - ISMS nach ISO/IEC 27001 (in Zertifizierung); regelmäßige Penetrationstests; Schwachstellenmanagement; Secure Software Development Lifecycle (Secure SDLC). - Auftrags-/Subprozessor-Kontrolle: sorgfältige Auswahl, vertragliche Bindung mind. gleichwertig (Art. 28 Abs. 4 DSGVO), Flow-down.

5. Schlüsselverwaltung: anbieterverwaltete Schlüssel; ein „Bring Your Own Key“ (BYOK) wird derzeit nicht angeboten.

Anlage 3 — Unterauftragsverarbeiter

Diese Anlage gibt den Stand bei Vertragsschluss wieder (Stand-Datum dieses AVV); Änderungen erfolgen ausschließlich nach dem Verfahren der Ziff. 12. Die jeweils aktuelle Fassung ist im Trust Center (zentre.ai/trust-center) veröffentlicht; frühere Fassungen sind mit Stand-Datum im Trust Center abrufbar. Eingesetzt werden insbesondere:

Anbieter	Zweck	Standort/Land	Transfers
Scaleway (Scaleway SAS)	Hosting/Infrastruktur	EU (Frankreich, Paris fr-par)	n/a (EU)
Bunny (BunnyWay d.o.o.)	CDN/Content Delivery (EU-Auslieferung)	EU (Slowenien)	n/a (EU, EU-Delivery-Regionen)
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., Irland)	Abrechnung/Zahlung (teilw. Verantwortlichen-Kontext, vgl. Ziff. 2)	EU (Irland); Übermittlung an Stripe, Inc. (USA) als deren Unterauftragsverarbeiter möglich	EU-US DPF / SCC
Friendly Captcha (Friendly Captcha GmbH)	Bot-/Missbrauchsschutz (Registrierungs- und Login-Seite; cookieless, gehashte IP)	EU (Deutschland)	n/a (EU)
Usercentrics (Usercentrics GmbH)	Consent-Management (Website; Verantwortlichen-Kontext, nur informatorisch)	EU (Deutschland)	n/a (EU)
Plausible (Plausible Insights OÜ)	Reichweitenmessung (Website; Verantwortlichen-Kontext, nur informatorisch)	EU	n/a (EU)

Die KI-Modellanbieter werden über das Gateway Cortecs als dessen Unterauftragsverarbeiter eingebunden (maßgeblich: Cortecs-Unterauftragsverarbeiterliste). Änderungen werden mind. 14 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; Anforderung mindestens 30 Tage lang möglich. Löschung nach Ablauf der Abruffrist — frühestens ab Tag 31 und nicht vor vollständiger Bereitstellung eines fristgerecht angeforderten Exports — gemäß Ziff. 15.

ZENTRE – Data Processing Agreement (DPA)

English convenience translation. Only the German version ("AVV/DPA") is legally binding; the English translation is provided for information purposes only. In case of discrepancies, the German version prevails.

Last updated: 15 Jul 2026

Key points at a glance (*non-binding orientation — the contract text prevails*): Your data is processed exclusively in the EU (hosting: Scaleway, Paris) · AI requests are routed via the EU gateway Cortecs, with zero data retention where available · Your content is not used to train AI models · Chats are deleted after 90 days (exportable beforehand) · New subprocessors are announced 14 days in advance and you may object · We notify you of personal data breaches within 48 hours · For professional secrecy holders, Section 20 (Section 203 mode) additionally applies.

Who is who: the "Controller" under this DPA is you — the Customer within the meaning of the GTC. The "Processor" is EZTO.

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.
- "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. Subject matter, nature, purpose, duration

- The subject matter is the processing of Customer data to provide, securely operate, maintain, support, and further develop Zentre.
- Duration: the term of the main agreement; thereafter deletion/return in accordance with Section 15.
- Details on nature/purpose/data categories/data subjects: Annex 1.

5. Instructions and instruction management

- Processing takes place exclusively on the documented instruction of the Controller (Art. 28 (3) (a) GDPR).
- Documented instructions include: (i) the main agreement/DPA, (ii) product and account configurations (provider selection, allow/deny, routing, regions, retention, logging), (iii) individual instructions by an administrator of the Controller in text form to legal@zentre.ai; EZTO may refer instructions from individual users to the administrators.
- Manifestly unlawful instructions are not carried out; the Controller is informed.
- Additional, non-agreed effort may be remunerated in accordance with the main agreement, to the extent permissible.

6. Obligations of the Controller

- 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.
- 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.
- 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. Confidentiality

- EZTO ensures that persons authorized to process are bound to confidentiality (Art. 28 (3) (b) GDPR).
- Need-to-know, role-based access, appropriate logging.
- For professional secrecy holders, Section 20 applies in addition.

8. Security of processing (Art. 32 GDPR)

- Appropriate TOMs pursuant to Annex 2 (including transport encryption TLS 1.2 or higher, encryption of data/artifacts at rest with AES-256 (at minimum), RBAC/least privilege, tenant separation, secure SDLC, monitoring/incident response). EZTO operates an ISO/IEC 27001-aligned ISMS; certification is underway; EZTO publishes the current status in the Trust Center.
- TOMs may be further developed, provided the overall level of security is not reduced.

9. Hosting and data location (default)

- 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.
- Differing Enterprise options may be agreed via order form.

10. Assistance with data subject rights

- 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.
- Direct data subject requests to EZTO are – where permissible – forwarded to the Controller; no independent response without instruction.

11. Assistance with compliance (Art. 28 (3) (f) GDPR)

EZTO appropriately assists the Controller with Art. 32–34, 35, 36 GDPR — primarily through the documentation provided in the Trust Center (TOM, data flow document, subprocessor list). Individual assistance beyond this (e.g., completing customer-specific DPIA templates, workshops) is reasonably remunerated in accordance with the main agreement, to the extent permissible.

12. Subprocessors

- General authorization (Art. 28 (2) GDPR).
- Current list: Annex 3 and the subprocessor list published in the Trust Center (zentre.ai/trust-center).
- Changes (engagement or replacement of subprocessors) are announced at least fourteen (14) days before they take effect in text form to the administrator e-mail address stored in the account and are additionally published via the subprocessor list in the Trust Center; the notice period begins upon dispatch of the e-mail. The Controller keeps the address up to date. Compelling security reasons may require a faster change, in which case the Controller is informed without undue delay. The Controller may object to the change in text form to legal@zentre.ai within the notice period (Art. 28(2) GDPR).
- In the event of legitimate objections: a reasonable alternative or a right of termination for the affected part of the service.
- Flow-down: EZTO binds subprocessors at least equivalently (Art. 28 (4) GDPR).
- EZTO remains responsible for compliance with subprocessor obligations within the framework of the GDPR, to the extent legally mandatory.

13. AI providers / AI routing

- Zentre acts as an infrastructure, orchestration, and governance layer. Depending on the configuration, content data is forwarded to AI providers for inference/generation.
- 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 / Trust Center).
- 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.
- 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.
- Clarification: additional permanent content “logging” does not take place by default, except in the following exceptional cases.
- 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.

- 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-dependent processing: processing by AI providers is provider-dependent; the selection/activation of an AI provider constitutes a documented instruction.
- Professional secrecy: For the processing of protected secrets within the meaning of Section 203 StGB, the model selection in Section 203 mode is restricted exclusively to authorized EU-controlled/EU-self-hosted endpoints (Section 20).
- 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.
- 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. Third-country transfers

- 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).
- Upon request, EZTO provides the Controller with appropriate information on transfer mechanisms and – where available – supplementary measures.

15. Deletion and return

- During the contract term, deletion takes place according to the configured retention (cf. Section 13 and Annex 4).
- After contract termination: at the Controller's choice, (i) return (export in commonly used machine-readable formats, where available) or (ii) deletion.
- Production systems: the export is generally provided within 30 days of receipt of the request. Deletion takes place after expiry of the 30-day retrieval period (Annex 4), but no earlier than after complete provision of an export requested within that period; where agreed exit assistance is used (e.g., Section 8(4) of the DORA Addendum), no earlier than after its completion.
- 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. Where data is restored from backups, previously deleted data is deleted again without undue delay.

16. Personal data breaches

- EZTO informs the Controller without undue delay, at the latest within 48 hours of becoming aware, of breaches of the protection of personal data.
- 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. Authority requests / disclosure

- To the extent legally permissible, EZTO informs the Controller without undue delay of legally binding requests from authorities to disclose Customer data.
- Disclosures are – where possible – limited to the necessary minimum; EZTO cooperates in appropriate protective measures.

18. Evidence and audits

- 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 are permitted after prior notice (at least 60 days) and under appropriate conditions; “remote-first” on the basis of the standard evidence package (Annex 2). On-site inspections take place only where remote audit and evidence are demonstrably insufficient in the individual case or a competent supervisory authority bindingly orders them; more extensive on-site rights may be agreed in the Enterprise order form.
- Frequency: a maximum of 1 audit per contract year, unless there is a security incident or legitimate cause.
- No (automated) vulnerability/penetration tests against EZTO systems without prior consent in text form.
- Audits are subject to strict confidentiality; no disclosure of operating/trade secrets beyond the necessary extent.
- 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. Documentation

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. Involvement in professional secrecy (Section 203 StGB; professional law requirements)

- Scope: To the extent the Controller is subject to a criminally sanctioned confidentiality obligation under Section 203 StGB (Austria: professional confidentiality duties such as Section 80 WTBG 2017 or Section 9 RAO and – in particular for health professions – Section 121 öStGB; Switzerland: 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), Section 62a of the German Tax Advisory Act (StBerG), Sections 43(1) and 50 of the German Public Accountants Act (WPO), Sections 18 and 26 of the German Federal Notaries Act (BNotO), Section 39a in conjunction with Section 39c of the German Patent Attorneys Act (PAO), and Section 80 of the Austrian WTBG 2017 (Austrian tax advisors and auditors).
- 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 binds subprocessors and AI providers that may access protected secrets, before their deployment, to equivalent confidentiality in text form. If a further contributing person cannot be bound equivalently, it is not used for the processing of protected secrets.
- Section 203 mode: The processing of protected secrets is permitted only in a suitable configuration: EU hosting, EU routing, zero data retention, deactivated web search, and exclusively authorized EU-

controlled/EU-self-hosted model providers. Endpoints of providers with a non-EU ultimate parent are not available in Section 203 mode.

- Web search in Section 203 mode: Web search is deactivated in Section 203 mode.
- Tenant separation (separate tenant): Protected secrets are processed in a dedicated, logically isolated tenant separated from normal operation, with its own, isolated knowledge base/index. A physically separated environment (private cloud/on-premises) may be agreed separately as an Enterprise option. 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.
- Supplementary agreement: The processing of protected secrets requires the conclusion of a separate confidentiality agreement under Section 203 StGB, which may also be concluded electronically; EZTO provides this agreement. In case of conflict, its provisions prevail for Section 203 matters.
- Model changes in Section 203 mode: For the removal or replacement of model providers authorized in Section 203 mode, the 30-day period pursuant to Section 7(4) of the confidentiality agreement applies, notwithstanding Section 12.

21. Final provisions

- Governing law and place of jurisdiction are governed by the main agreement (German law; place of jurisdiction Mainz, to the extent permissible).
- 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.
- Amendments and supplements require at least text form.

Annexes to the DPA

Annex 1 — Description of the processing (Art. 28 (3) GDPR)

Subject matter of the processing: provision and operation of the AI orchestration and governance platform “Zentre” (chat assistant, agents, RAG/knowledge tool) as SaaS.

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.

Purpose: provision of the contractually agreed services, user/access management, support/error analysis, security/abuse prevention/incident handling.

Categories of personal data: - account/organization data (name, business email, organization, roles/permissions); - usage, billing, security, and technical metadata (timestamps, request IDs, configuration, token/volume metrics, error messages, IP where necessary); - content data (prompts, uploads, documents, outputs); - web search queries (only where web search is activated).

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.

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).

Duration: for the term of the main agreement; chat/workspace content data 90 days; thereafter deletion/return pursuant to Section 15 and Annex 4.

Place of processing: EU/EEA – hosting Scaleway (France, Paris fr-par); content delivery via Bunny CDN (BunnyWay d.o.o., Slovenia, EU – delivery restricted to EU/EEA locations); AI routing via Cortecs (EU); web search via Linkup (EU). Third-country transfers only pursuant to Section 14.

Annex 2 — Technical and organizational measures (Art. 32 GDPR)

EZTO operates an ISO/IEC 27001-aligned information security management system (ISMS) and is currently undergoing ISO/IEC 27001 certification. The standard evidence package (TOM documentation, security whitepaper, management summary of current penetration tests, standard security questionnaire completed by EZTO) is available for retrieval in the Trust Center. Full penetration-test reports and the completion of customer-specific questionnaires and templates take place only by separate agreement (Enterprise/order form), under confidentiality, and against reasonable remuneration.

1. Confidentiality - Physical access control: hosting in certified EU data centers (Scaleway); physical security by the infrastructure provider. - System access control: authentication with multi-factor authentication (MFA) for administrative access; role-based assignment of rights (RBAC) according to the least-privilege principle. - Data access control: need-to-know, role-based access, access logging; restriction of administrative access. - Separation control: tenant-separated processing (logical tenant separation). - Pseudonymization/minimization: to the extent possible for the purpose.

2. Integrity - Transfer control: transport encryption (TLS 1.2 or higher) for data in transit. - Encryption of data/artifacts at rest with AES-256 (at minimum). - Input control: logging of relevant actions.

3. Availability and resilience - Data backup (backups) with defined deletion/overwrite cycles (up to 90 days); - monitoring, incident response process; business continuity/emergency plan.

4. Procedures for regular review, assessment, and evaluation - ISMS pursuant to ISO/IEC 27001 (undergoing certification); regular penetration tests; vulnerability management; secure software development lifecycle (secure SDLC). - Order/subprocessor control: careful selection, contractual binding at least equivalently (Art. 28 (4) GDPR), flow-down.

5. Key management: provider-managed keys; “Bring Your Own Key” (BYOK) is not currently offered.

Annex 3 — Subprocessors

This Annex reflects the status at the time of contract conclusion (the “last updated” date of this DPA); changes are made exclusively in accordance with the procedure under Section 12. The current version is published in the Trust Center (zentre.ai/trust-center); previous versions are available in the Trust Center with their date. The following are engaged in particular:

Provider	Purpose	Location/Country	Transfers
Scaleway (Scaleway SAS)	Hosting/infrastructure	EU (France, Paris fr-par)	n/a (EU)
Bunny (BunnyWay d.o.o.)	CDN/content delivery (EU delivery)	EU (Slovenia)	n/a (EU, EU delivery regions)
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., Ireland)			EU-US DPF / SCC

Provider	Purpose	Location/Country	Transfers
	Billing/payment (partly controller context, cf. Section 2)	EU (Ireland); transfer to Stripe, Inc. (USA) as its sub-processor possible	
Friendly Captcha (Friendly Captcha GmbH)	Bot/abuse protection (signup and login pages; cookieless, hashed IP)	EU (Germany)	n/a (EU)
Usercentrics (Usercentrics GmbH)	Consent management (website; controller context, informational only)	EU (Germany)	n/a (EU)
Plausible (Plausible Insights OÜ)	Analytics (website; controller context, informational only)	EU	n/a (EU)

The AI model providers are integrated via the Cortecs gateway as its subprocessors (decisive: Cortecs subprocessor list). Changes are announced at least 14 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; requests are possible for at least 30 days. Deletion after expiry of the retrieval period — no earlier than day 31 and not before complete provision of an export requested in time — pursuant to Section 15.