

# Verschwiegenheitsvereinbarung — Variante für Wirtschaftsprüfer und vereidigte Buchprüfer (WPO)

**Dokument:** Variante der Verschwiegenheitsvereinbarung · **Stand:** 4. Sep 2026 · Nur die deutsche Fassung ist rechtsverbindlich.

zwischen **dem Auftraggeber** — Wirtschaftsprüfer/in, vereidigte/r Buchprüfer/in bzw.

Wirtschaftsprüfungsgesellschaft i. S. d. Wirtschaftsprüferordnung (WPO) (nachfolgend "Berufsträger") — und **EZTO TECHNOLOGIES GmbH**, Am Brand 41, 55116 Mainz, Deutschland (nachfolgend "EZTO").

## § 1 Präambel und Geltungsbereich

Der Berufsträger nutzt die SaaS-Plattform "Zentre" von EZTO. Dabei können fremde Geheimnisse verarbeitet werden, die dem strafbewehrten Schutz des § 203 Abs. 1 Nr. 3 StGB unterliegen. Diese Vereinbarung ergänzt den Hauptvertrag und den AVV/DPA; bei Widersprüchen gehen ihre Regelungen für Sachverhalte des § 203 StGB vor (vgl. Ziff. 20 AVV).

## § 2 Rechtlicher Rahmen

- **§ 203 Abs. 1 Nr. 3 StGB:** Wirtschaftsprüfer und vereidigte Buchprüfer sind gesetzlich zur strengen Verschwiegenheit verpflichtet; die unbefugte Offenbarung fremder Geheimnisse ist strafbar.
- **§ 43 Abs. 1 WPO:** Berufspflicht zur Verschwiegenheit als tragende Berufspflicht.
- **§ 50 WPO:** Pflicht, alle beschäftigten und mitwirkenden Personen in Textform zur Verschwiegenheit zu verpflichten und über die strafrechtlichen Folgen zu belehren.
- **§ 50a WPO:** Inanspruchnahme von Dienstleistern: Verpflichtung in Textform, Belehrung, sorgfältige Auswahl. Die Auswahl- und Beendigungspflichten des Berufsträgers sowie das Einwilligungserfordernis nach § 50a Abs. 5 WPO bei Dienstleistungen, die unmittelbar einem einzelnen Auftrag dienen, bleiben unberührt (Muster „Mandanteninformation und Einwilligungsbaustein“ im Trust Center).
- **§ 50a WPO (Inanspruchnahme von Dienstleistungen):** Der Berufsträger darf Dienstleistern den Zugang zu geschützten Tatsachen eröffnen, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist (Abs. 1). Er hat den Dienstleister sorgfältig auszuwählen und die Zusammenarbeit unverzüglich zu beenden, wenn die Einhaltung der Vorgaben nicht gewährleistet ist (Abs. 2). Der Vertrag bedarf der Textform und muss die Verpflichtung unter Belehrung, die Beschränkung der Kenntnisnahme auf das Erforderliche sowie eine ausdrückliche Regelung zur Heranziehung weiterer Personen enthalten (Abs. 3) — diese Anforderungen erfüllt die vorliegende Vereinbarung (§§ 4 bis 6). Bei im Ausland erbrachten Dienstleistungen ist ein dem inländischen vergleichbarer Schutz erforderlich (Abs. 4); im § 203-Modus erfolgen Hosting, Routing und Inferenz ausschließlich in der EU/dem EWR. **Dient die Nutzung unmittelbar einem einzelnen Mandat, setzt die Eröffnung des Zugangs die Einwilligung des Mandanten voraus (Abs. 5); die Einholung dieser Einwilligung obliegt dem Berufsträger.**
- **§ 323 Abs. 1 HGB:** Bei gesetzlichen Abschlussprüfungen gilt die Verschwiegenheitspflicht des Abschlussprüfers zusätzlich; Geschäfts- und Betriebsgeheimnisse dürfen nicht unbefugt verwertet werden. EZTO verwertet solche Geheimnisse nicht und nutzt sie insbesondere nicht zum Training oder Fine-Tuning. Die Verantwortlichkeit und Haftung des Abschlussprüfers nach § 323 HGB bleibt unberührt und wird durch diese Vereinbarung weder ausgeschlossen noch beschränkt (§ 323 Abs. 4 HGB).
- **§ 203 Abs. 3 Satz 2, Abs. 4 StGB:** Zulässigkeit der Einschaltung mitwirkender Personen; deren eigene Strafbarkeit; Verpflichtungs- und Belehrungspflicht des Berufsträgers.
- **Berufssatzung WP/vBP:** ergänzende berufsrechtliche Anforderungen beim Einsatz externer Dienstleister.

## § 3 Stellung von EZTO als mitwirkende Person

EZTO wird für den Berufsträger als sonstige mitwirkende Person i. S. d. § 203 Abs. 3 Satz 2 StGB tätig. Die Offenbarung geschützter Geheimnisse gegenüber EZTO ist auf das für die Leistungserbringung Erforderliche

beschränkt. EZTO nimmt Kenntnis von geschützten Geheimnissen nur, soweit und solange dies zur Bereitstellung, Wartung, Störungsbeseitigung und Sicherheit des Dienstes erforderlich ist.

#### **§ 4 Verpflichtung zur Verschwiegenheit und Belehrung**

EZTO verpflichtet sich zur Verschwiegenheit über alle fremden Geheimnisse i. S. d. § 203 StGB, die EZTO im Rahmen der Leistungserbringung bekannt werden. Diese Verpflichtung erfolgt in Textform i. S. d. § 50 WPO. EZTO ist über die strafrechtlichen Folgen einer unbefugten Offenbarung nach § 203 Abs. 4 StGB belehrt worden; der Wortlaut der maßgeblichen Vorschriften ist als Anlage beigelegt. Die Verschwiegenheitspflicht besteht nach Beendigung des Vertragsverhältnisses fort.

#### **§ 5 Verpflichtung der bei EZTO mitwirkenden Personen**

EZTO stellt sicher, dass sämtliche Personen, die bei der Leistungserbringung mitwirken und Zugang zu geschützten Geheimnissen erhalten können, vor Aufnahme ihrer Tätigkeit in Textform zur Verschwiegenheit verpflichtet und über die strafrechtlichen Folgen einer unbefugten Offenbarung belehrt werden. Der Zugang erfolgt nach dem Need-to-know-Prinzip, rollenbasiert und protokolliert. Auf Anforderung weist EZTO die erfolgten Verpflichtungen durch eine zusammenfassende Bestätigung nach; das Muster der Verpflichtungserklärung wird auf Wunsch bereitgestellt. Personenbezogene Einzelnachweise erfolgen nur nach gesonderter Vereinbarung oder soweit berufsrechtlich zwingend erforderlich.

#### **§ 6 Einschaltung weiterer mitwirkender Personen (Subunternehmer)**

Zieht EZTO weitere Personen zur Leistungserbringung hinzu, die Zugang zu geschützten Geheimnissen erhalten können (insbesondere Subprozessoren und KI-Anbieter), wählt EZTO diese sorgfältig aus und verpflichtet sie vor ihrem Einsatz in Textform zu einer mindestens gleichwertigen Verschwiegenheit (Flow-down gemäß Ziff. 20 AVV). Kann eine weitere mitwirkende Person nicht gleichwertig verpflichtet werden, wird sie für die Verarbeitung geschützter Geheimnisse nicht eingesetzt. Die aktuelle Subprozessorenliste ist im Trust Center abrufbar; Änderungen werden entsprechend der im AVV vereinbarten Frist angekündigt. Die von EZTO unmittelbar eingesetzten Dienstleister (Hosting, Content Delivery, KI-Gateway) haben ihren Sitz in der EU/dem EWR; für die Betreiber der Modell-Endpunkte gilt die Zuordnung nach den Modellklassen (§ 7). EZTO weist die Verpflichtungen dem Berufsträger auf Anfrage nach und teilt die Namen der verpflichteten Stellen dabei unter Vertraulichkeit mit.

**Unternehmensgruppe.** EZTO gehört zu einer Unternehmensgruppe; die Obergesellschaft hat ihren Sitz außerhalb der EU. Die Beteiligung besteht ausschließlich auf Gesellschafterebene; Einzelheiten und Konzernübersicht: Datenflussdokument im Trust Center, Abschnitt 4. Keine Gesellschaft dieser Unternehmensgruppe wirkt an der Erbringung der Leistung für den Berufsträger mit; oberhalb der EZTO TECHNOLOGIES GmbH findet keine Verarbeitung geschützter Geheimnisse statt. Keiner Gesellschaft der Unternehmensgruppe außerhalb der EU/des EWR wird der Zugriff auf geschützte Geheimnisse, auf die Systeme, in denen sie verarbeitet werden, oder auf Schlüsselmaterial eingeräumt oder die Kenntnisnahme ermöglicht; Gesellschaften der Gruppe sind aus diesem Grund keine Subunternehmer und nicht in der Subprozessorenliste geführt. Technisch abgesichert ist dies durch eine ausschließlich von EZTO betriebene Verwaltungsebene, das Fehlen eines konzernweiten administrativen Zugangs und eines gemeinsam genutzten Notfallzugangs sowie durch Erzeugung und Haltung des Schlüsselmaterials ausschließlich in der EU/dem EWR. Wird künftig eine Service-Region außerhalb der EU betrieben, werden die Regionen getrennt geführt; ein wechselseitiger Zugriff besteht nicht, und die Verarbeitung geschützter Geheimnisse findet ausschließlich in der EU-Region statt.

#### **§ 7 § 203-Modus: technische und organisatorische Konfiguration**

Die Verarbeitung geschützter Geheimnisse ist nur in einer geeigneten Konfiguration zulässig ("§ 203-Modus"):

- EU-Hosting (Scaleway, Region Paris fr-par) und EU-Routing über das AI-Gateway Cortecs;
- Zero Data Retention (ZDR) bei den angebundenen Modellanbietern;
- Websuche ist in diesem Modus deaktiviert;

- **Modellklassen:** Alle zugelassenen Endpunkte sind einer von zwei Klassen zugeordnet. Beide Klassen setzen kumulativ voraus: Inferenz ausschließlich über Endpunkte in der EU/dem EWR, Zero Data Retention, kein Training und kein Fine-Tuning mit Inhalten sowie die vorherige Verpflichtung jedes Kettenglieds zur Verschwiegenheit in Textform. Sie unterscheiden sich darin, wessen Recht der Betreiber des Endpunkts unterliegt:
- **"EU-souverän":** Der Betreiber unterliegt ausschließlich dem Recht eines EU-/EWR-Staates und hat keine Konzernobergesellschaft in einem Drittland; hierzu zählen auch offene Modelle, die dieser Betreiber selbst in der EU betreibt. Kein Glied der Verarbeitungskette — Hosting, Content Delivery, KI-Gateway und Betreiber der Endpunkte — unterliegt dem Recht eines Drittlands; EZTO selbst unterliegt deutschem Recht (§ 6).
- **"EU-gehostet":** Der Endpunkt wird in der EU/dem EWR betrieben; der Betreiber oder dessen Konzernobergesellschaft kann daneben dem Recht eines Drittlands unterliegen (einschließlich Frontier-Modellen über EU-Endpunkte). Ein Herausgabeverlangen einer Drittlandsbehörde gegenüber dem Betreiber ist insoweit rechtlich nicht vollständig ausgeschlossen.
- **Wahl der Modellklasse:** Der Berufsträger wählt die Modellklasse. Die Wahl ist bei der Aktivierung des § 203-Modus ausdrücklich zu treffen; ohne Wahl wird der Modus nicht aktiviert. Wahl und jede Umstellung werden mit Zeitpunkt, wählender Person und gewählter Klasse protokolliert und sind für den Berufsträger abrufbar; eine Umstellung ist jederzeit möglich und wirkt für Anfragen ab dem Zeitpunkt der Umstellung. Die berufsrechtliche Bewertung, welche Klasse für die konkrete Tätigkeit erforderlich ist, obliegt dem Berufsträger; für Vereinbarungen, die vor dem Wirksamwerden dieser Fassung geschlossen wurden, bleibt es bei der Klasse "EU-souverän", bis der Berufsträger aktiv eine andere Klasse wählt;
- **Bildgenerierung:** Die Bildgenerierung ist im Service verfügbar; es gelten dieselben Modellklassen, derselbe Trainingsausschluss und dieselbe Kennzeichnung wie für die übrigen Ausgabearten. Die Kennzeichnung erzeugter Bilddateien ist aktiv (IPTC Digital Source Type; zusätzlich C2PA-Content-Credentials, soweit das Format dies unterstützt); Bildformate ohne verfügbare Kennzeichnung stehen für die Erzeugung nicht zur Verfügung;
- **dedizierter, logisch isolierter Tenant mit eigener, isolierter Wissensbasis;** keine tenantübergreifende Suche und kein tenantübergreifender Datentransfer (eine physisch getrennte Umgebung — Private Cloud/On-Premises — kann als Enterprise-Option gesondert vereinbart werden).

Die Zuordnung von Daten zum geschützten Tenant obliegt dem Berufsträger; im Zweifel ist der geschützte Tenant zu verwenden. Geheimnisfreie interne Angelegenheiten können im normalen Tenant verarbeitet werden.

Für Änderungen der zugelassenen Modellkonfiguration gilt: Die Aufnahme zusätzlicher Endpunkte oder Modellversionen bereits nach dieser Vereinbarung verpflichteter Betreiber, die die vorstehenden Anforderungen erfüllen und der vom Berufsträger gewählten Modellklasse zugeordnet sind, ist ohne gesonderte Ankündigung zulässig; die Aufnahme von Endpunkten neuer Betreiber wird mindestens 14 Tage vor ihrer Freischaltung in Textform angekündigt; ein Endpunkt wird nicht ohne Wahl des Berufsträgers der jeweils anderen Klasse zugeordnet. Die Entfernung oder der Ersatz zugelassener Modellanbieter sowie sonstige Änderungen dieser Konfiguration werden dem Berufsträger mindestens 30 Tage vor Wirksamwerden in Textform angekündigt; ein Ersatz erfolgt nur durch mindestens gleichwertige Anbieter. Widerspricht der Berufsträger innerhalb der Ankündigungsfrist, steht ihm ein Sonderkündigungsrecht zum Wirksamwerden der Änderung zu.

## **§ 8 Weisungen, Kontrolle, Nachweise**

Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Berufsträgers gemäß AVV. EZTO unterstützt den Berufsträger bei der Erfüllung seiner berufsrechtlichen Nachweispflichten durch geeignete Informationen und Nachweise (vgl. Ziff. 18, 19 AVV).

## **§ 9 Schlussbestimmungen**

Es gilt deutsches Recht; Gerichtsstand ist Mainz, soweit zulässig. Änderungen und Ergänzungen bedürfen mindestens der Textform. Diese Vereinbarung kann elektronisch geschlossen werden; EZTO stellt dem Berufsträger nach Abschluss eine vollständige Ausfertigung einschließlich der bei Abschluss geltenden

Modellkonfiguration (Stand-Datum) und der Gesetzesanlage als Dokument bereit. Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Ort, Datum: \_\_ Berufsträger: \_\_ EZTO TECHNOLOGIES GmbH: \_\_

**Anlage:** Wortlaut der maßgeblichen Vorschriften (§ 203 StGB (Auszug), § 43 Abs. 1, § 50 WPO) — siehe "Anlage Gesetzeswortlaut" im Trust Center.

# Confidentiality Agreement — Variant for German public auditors and sworn auditors (WPO)

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

**Document:** confidentiality agreement variant · **Last updated:** 4 Sep 2026

between **the Customer** — a public auditor, sworn auditor, or audit firm within the meaning of the German Public Accountants Act (WPO) (the "Professional") — and **EZTO TECHNOLOGIES GmbH**, Am Brand 41, 55116 Mainz, Germany ("EZTO").

## Section 1 Preamble and scope

The Professional uses EZTO's SaaS platform "Zentre". In doing so, third-party secrets protected under criminal law by Section 203(1) no. 3 StGB may be processed. This agreement supplements the main agreement and the DPA; in case of conflict, its provisions prevail for Section 203 matters (cf. Section 20 DPA).

## Section 2 Legal framework

- **Section 203(1) no. 3 StGB:** Public auditors and sworn auditors are bound by strict statutory confidentiality; unauthorized disclosure of third-party secrets is a criminal offence.
- **Section 43(1) WPO:** professional duty of confidentiality as a core professional duty.
- **Section 50 WPO:** duty to bind all employed and contributing persons to confidentiality in text form and to instruct them about the criminal consequences.
- **Section 50a WPO (use of services):** The Professional may grant service providers access to protected facts to the extent necessary for the use of the service (para. 1). The Professional must select the service provider carefully and terminate the cooperation without undue delay if compliance with the requirements is not ensured (para. 2). The contract requires text form and must contain the undertaking together with instruction, the limitation of access to what is necessary, and an express provision on the involvement of further persons (para. 3) — the present agreement meets these requirements (Sections 4 to 6). For services performed abroad, protection comparable to that available domestically is required (para. 4); in Section 203 mode, hosting, routing, and inference take place exclusively in the EU/EEA. **Where the use directly serves an individual mandate, granting access requires the client's consent (para. 5); obtaining this consent is incumbent on the Professional.** The professional's selection and termination duties and the consent requirement under Section 50a (5) WPO for services directly serving an individual engagement remain unaffected (template "Client information and consent module" in the Trust Center).
- **Section 323(1) HGB:** In statutory audits, the auditor's confidentiality obligation applies in addition; trade and business secrets must not be exploited without authorization. EZTO does not exploit such secrets and in particular does not use them for training or fine-tuning. The responsibility and liability of the auditor under Section 323 HGB remains unaffected and is neither excluded nor limited by this agreement (Section 323(4) HGB).
- **Section 203(3) sentence 2, (4) StGB:** permissibility of engaging contributing persons; their own criminal liability; the duty to bind and instruct them.
- **WP/vBP professional charter:** supplementary professional-law requirements for the use of external service providers.

## Section 3 EZTO's role as contributing person

EZTO acts for the Professional as an "other contributing person" within the meaning of Section 203(3) sentence 2 StGB. Disclosure of protected secrets to EZTO is limited to what is necessary for the provision of the service. EZTO takes note of protected secrets only to the extent and for as long as necessary for the provision, maintenance, troubleshooting, and security of the service.

## Section 4 Confidentiality undertaking and instruction

EZTO undertakes to maintain confidentiality regarding all third-party secrets within the meaning of Section 203 StGB of which EZTO becomes aware in providing the service. This undertaking is given in text form within the meaning of Section 50 WPO. EZTO has been instructed about the criminal consequences of unauthorized disclosure pursuant to Section 203(4) StGB; the wording of the relevant provisions is annexed. The duty of confidentiality continues after termination of the contractual relationship.

## Section 5 Binding of persons contributing at EZTO

EZTO ensures that all persons who contribute to the provision of the service and may gain access to protected secrets are bound to confidentiality in text form before commencing their activity and are instructed about the criminal consequences of unauthorized disclosure. Access follows the need-to-know principle, is role-based, and is logged. Upon request, EZTO evidences the undertakings by way of a summary confirmation; the template undertaking is provided on request. Person-specific individual evidence is provided only by separate agreement or to the extent mandatorily required under professional law.

## Section 6 Engagement of further contributing persons (subcontractors)

Where EZTO engages further persons who may gain access to protected secrets (in particular subprocessors and AI providers), EZTO selects them carefully and binds them, before their deployment, in text form to at least equivalent confidentiality (flow-down pursuant to Section 20 DPA). If a further contributing person cannot be bound equivalently, it is not used for the processing of protected secrets. The current subprocessor list is available in the Trust Center; changes are announced per the notice period agreed in the DPA. The service providers engaged directly by EZTO (hosting, content delivery, AI gateway) are established in the EU/EEA; for the operators of the model endpoints, the model-class classification under Section 7 applies. Upon request, EZTO demonstrates these undertakings to the professional and discloses the names of the bound entities subject to confidentiality.

**Group of companies.** EZTO belongs to a group of companies; the ultimate parent is established outside the EU. The shareholding exists solely at shareholder level; details and group chart: data flow document in the Trust Center, section 4. No company of this group participates in the provision of the service for the professional; no processing of protected secrets takes place above EZTO TECHNOLOGIES GmbH. No company of the group outside the EU/EEA is granted access to protected secrets, to the systems in which they are processed, or to key material, nor is it enabled to take note of them; for this reason companies of the group are not subcontractors and are not listed in the subprocessor list. This is safeguarded technically by a control plane operated exclusively by EZTO, the absence of any group-wide administrative access and of any shared emergency access, and by generating and holding key material exclusively in the EU/EEA. Should a service region outside the EU be operated in future, the regions will be kept separate; there is no mutual access, and the processing of protected secrets takes place exclusively in the EU region.

## Section 7 Section 203 mode: technical and organizational configuration

The processing of protected secrets is permitted only in a suitable configuration ("Section 203 mode"):

- EU hosting (Scaleway, region Paris fr-par) and EU routing via the Cortecs AI gateway;
- zero data retention (ZDR) at the integrated model providers;
- web search is deactivated in this mode;
- Model classes: all authorized endpoints are assigned to one of two classes. Both classes cumulatively require: inference exclusively via endpoints in the EU/EEA, zero data retention, no training and no fine-tuning on content, and a prior undertaking of confidentiality in text form from every link in the chain. They differ in whose law the operator of the endpoint is subject to:
- "EU-sovereign": the operator is subject exclusively to the law of an EU/EEA state and has no ultimate parent in a third country; this also includes open models that this operator runs itself in the EU. No link in the

processing chain — hosting, content delivery, AI gateway and the operators of the endpoints — is subject to the law of a third country; EZTO itself is subject to German law (Section 6).

- "EU-hosted": the endpoint is operated in the EU/EEA; the operator or its ultimate parent may additionally be subject to the law of a third country (including frontier models via EU endpoints). To that extent, a disclosure request by a third-country authority addressed to the operator is not entirely excluded in law.
- Selection of the model class: the Professional selects the model class. The selection must be made expressly upon activation of Section 203 mode; without such selection, the mode is not activated. The selection and every switch are logged with timestamp, selecting person and selected class and are retrievable by the Professional; a switch is possible at any time and takes effect for requests from the time of the switch. The professional-law assessment of which class is required for the specific activity is incumbent on the Professional; for agreements concluded before this version took effect, the class "EU-sovereign" continues to apply until the Professional actively selects a different class;
- Image generation: image generation is available in the Service; the same model classes, the same exclusion of training and the same marking apply as for the other types of output. The marking of generated image files is active (IPTC Digital Source Type; additionally C2PA Content Credentials where the format supports this); image formats for which no marking is available are not available for generation;
- dedicated, logically isolated tenant with its own, isolated knowledge base; no cross-tenant search and no cross-tenant data transfer (a physically separated environment — private cloud/on-premises — may be agreed separately as an Enterprise option).

The assignment of data to the protected tenant is the responsibility of the Professional; in case of doubt, the protected tenant is to be used. Secrecy-free internal matters may be processed in the normal tenant.

For changes to the authorized model configuration: the addition of further endpoints or model versions of operators already bound under this Agreement that meet the above requirements and are assigned to the model class selected by the Professional is permitted without separate announcement; endpoints of new operators are announced in text form at least 14 days before their activation; an endpoint is not assigned to the respective other class without a selection by the Professional. The removal or replacement of authorized model providers and other changes to this configuration are announced to the Professional in text form at least 30 days before they take effect; a replacement is made only by at least equivalent providers. If the Professional objects within the notice period, the Professional has a special right of termination effective as of the date the change takes effect.

## **Section 8 Instructions, control, evidence**

Processing takes place exclusively on the documented instruction of the Professional pursuant to the DPA. EZTO supports the Professional in fulfilling its professional-law evidence obligations through suitable information and evidence (cf. Sections 18, 19 DPA).

## **Section 9 Final provisions**

German law applies; the place of jurisdiction is Mainz, to the extent permissible. Amendments and supplements require at least text form. This agreement may be concluded electronically; after conclusion, EZTO provides the Professional with a complete executed copy including the model configuration in effect at conclusion (dated) and the statutory annex as a document. Should individual provisions be or become invalid, the validity of the remaining provisions remains unaffected.

Place, date: \_\_ Professional: \_\_ EZTO TECHNOLOGIES GmbH: \_\_

**Annex:** wording of the relevant provisions (Section 203 StGB (excerpt), Sections 43(1) and 50 WPO) — see "Legal texts annex" in the Trust Center (statutory texts available in German only).