

Leitfaden für Rechtsanwältinnen und Rechtsanwälte: Einsatz von Zentre im Einklang mit BRAO/BORA und § 203 StGB

Herausgeber: EZTO TECHNOLOGIES GmbH (Zentre) · **Stand:** 13. Jul 2026

Auch für andere Berufsgeheimnisträger: Die Ausführungen gelten für Steuerberater, Wirtschaftsprüfer, Notare, Patentanwälte und Heilberufe entsprechend; maßgeblich ist die jeweilige Variante der Verschwiegenheitsvereinbarung im Trust Center.

Kein Rechtsrat. Dieser Leitfaden erläutert, wie Zentre den Einsatz durch Berufsgeheimnisträger unterstützt und welche berufsrechtlichen Pflichten bei der Kanzlei verbleiben. Die abschließende Beurteilung obliegt der jeweiligen Kanzlei; im Zweifel ist berufsrechtlicher Rat einzuholen.

1. Zweck

Rechtsanwältinnen und Rechtsanwälte unterliegen einer strengen Verschwiegenheitspflicht. Dieser Leitfaden zeigt, (a) welcher berufsrechtliche Rahmen beim Einsatz von KI-/Cloud-Diensten gilt, (b) wie Zentre diesen Rahmen technisch und vertraglich unterstützt und (c) welche Pflichten bei der Kanzlei verbleiben.

2. Berufsrechtlicher Rahmen

- **§ 43a Abs. 2 BRAO** — Verschwiegenheitspflicht als Kernpflicht.
- **§ 2 BORA** — Konkretisierung: Pflicht zu risikoadäquaten technischen und organisatorischen Maßnahmen nach dem Stand der Technik; Fortgeltung über das Mandatsende hinaus.
- **§ 43e BRAO** — ausdrückliche Erlaubnis zur Inanspruchnahme von Dienstleistern (u. a. IT/Cloud) unter Bedingungen: Erforderlichkeit, Verpflichtung des Dienstleisters in Textform, Belehrung über Verschwiegenheit, sorgfältige Auswahl, Beendigungsmöglichkeit bei Pflichtverletzung.
- **§ 203 StGB** — strafrechtliche Absicherung; seit der Reform 2017 (Abs. 3/4) ist die Einbindung „mitwirkender Personen“ zulässig, wobei diese strafrechtlich verantwortlich werden und die Kanzlei diese zu verpflichten hat.
- **CCBE-Berufsregeln** — grenzüberschreitende Verschwiegenheit; Sensibilität gegenüber ausländischen Offenlegungspflichten (z. B. US CLOUD Act).

3. Wie Zentre unterstützt

- **§ 203-Modus (Berufsgeheimnis-Modus):** dedizierte Konfiguration für die Verarbeitung geschützter Geheimnisse — EU-Hosting (Scaleway, Paris), EU-basiertes Routing über Cortecs, **Zero Data Retention**, Beschränkung der Modellauswahl auf zugelassene EU-Endpunkte.
- **Ausschließlich EU-kontrollierte Modelle:** Im § 203-Modus stehen ausschließlich EU-Anbieter (z. B. Mistral) bzw. von Cortecs in der EU selbst betriebene Modelle zur Verfügung; der Modellhersteller erhält keinen Zugriff. Endpunkte von Modellanbietern mit Nicht-EU-Mutterkonzern sind im § 203-Modus technisch deaktiviert — das Risiko ausländischer Offenlegungspflichten (z. B. US CLOUD Act) ist strukturell minimiert, da sämtliche Modellanbieter, das KI-Gateway (Cortecs, Österreich) und das Hosting (Scaleway, Frankreich) keiner Nicht-EU-Konzernobergesellschaft unterliegen.
- **Gesonderte Verschwiegenheitsvereinbarung nach § 203 StGB** (DE: § 203 StGB / AT: § 80 WTBG 2017, § 9 RAO, §§ 121 f. öStGB / CH: Art. 321 StGB) mit Belehrung nach § 203 Abs. 4 StGB, Verpflichtung der EZTO-Mitarbeitenden in Textform und **Flow-down** auf Subprozessoren/Modellanbieter.
- **Kein Training** mit Mandantendaten (vertraglich ausgeschlossen; der Ausschluss wird per Flow-down an die Modellanbieter durchgereicht; bei Cortecs-selbst-betriebenen Modellen zusätzlich technisch ohne Herstellerzugriff).

- **TOM nach Stand der Technik** (Verschlüsselung in Übertragung (TLS 1.2 oder höher) und ruhender Daten/Artefakte (AES-256 (mindestens)), RBAC, Mandantentrennung, Protokollierung); an ISO/IEC 27001 ausgerichtetes ISMS; Zertifizierung läuft (aktueller Status und Standard-Nachweispaket im Trust Center).
- **Need-to-know-Zugriff** seitens EZTO, möglichst begrenzt, freigegeben und protokolliert.
- **Websuche im § 203-Modus:** Die Websuche ist im § 203-Modus deaktiviert. Geschützte Geheimnisse (Mandantendaten) gehören nicht in Suchanfragen.
- **Mandattrennung durch separaten Tenant:** Mandantendaten werden in einer vom Normalbetrieb getrennten, dedizierten und logisch isolierten Umgebung (eigener Tenant) mit eigener, isolierter Wissensbasis verarbeitet; eine physisch getrennte Umgebung (Private Cloud/On-Premises) kann als Enterprise-Option gesondert vereinbart werden. Es gibt keine gemeinsame Wissensbasis und keinen tenantübergreifenden Datentransfer; ein Wechsel in den internen Tenant ist ein reiner Ansichts-/ Navigationswechsel und überträgt keine Inhalte.

4. Pflichten, die bei der Kanzlei verbleiben

1. **Erforderlichkeit prüfen** und nur die für das Mandat erforderlichen Daten eingeben (**Datenminimierung**).
2. **Sorgfältige Auswahl/Überwachung** des Dienstleisters (dieser Leitfaden, AVV, Verschwiegenheitsvereinbarung und Nachweise dienen der Dokumentation).
3. **Verschwiegenheitsvereinbarung abschließen** (Phase 1: per Kontakt unterzeichnen; Phase 2: in-App) — Voraussetzung für den § 203-Modus.
4. **Mandatsdaten ausschließlich im § 203-Tenant** verarbeiten; interne/mandatsfreie Vorgänge im Normal-Tenant; **im Zweifel § 203-Tenant**. Außerhalb des § 203-Tenants keine geschützten Geheimnisse eingeben.
5. **Eigene Mitarbeitende/Nutzer** zur Verschwiegenheit verpflichten.
6. **Mandantenbezug/Einwilligung** im Einzelfall prüfen, soweit berufsrechtlich erforderlich.
7. **KI-Ausgaben fachlich prüfen** (keine Gewähr für Richtigkeit; Verantwortung verbleibt bei der Kanzlei).

5. Kurz-Checkliste

- ☐ Verschwiegenheitsvereinbarung (§ 203) unterzeichnet
- ☐ § 203-Modus aktiviert
- ☐ eigene Mitarbeitende verpflichtet
- ☐ Datenminimierung/Need-to-know beachtet
- ☐ Nachweise/AVV/TOM zur Akte genommen
- ☐ Websuche im § 203-Modus beachtet (deaktiviert; keine Mandantengeheimnisse in Suchanfragen)

6. Verantwortungsabgrenzung

Die Kanzlei bleibt datenschutz- und berufsrechtlich Verantwortliche; EZTO wird als mitwirkende Person/ Auftragsverarbeiter tätig. Die Aktivierung des § 203-Modus liegt bei der Kanzlei. EZTO stellt die hierfür geeignete Konfiguration und die vertraglichen Instrumente bereit.

7. Quellen

BRAO (§ 43a, § 43e) · BORA (§ 2) · § 203 StGB · CCBE-Berufsregeln · DSGVO/BDSG · KI-VO (VO (EU) 2024/1689). Aktuelle Fassungen u. a. über die Bundesrechtsanwaltskammer ([brak.de](https://www.brak.de)) und [gesetze-im-internet.de](https://www.gesetze-im-internet.de).

Guide for Lawyers: Using Zentre in Compliance with BRAO/BORA and Section 203 StGB

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

Publisher: EZTO TECHNOLOGIES GmbH (Zentre) · **Last updated:** 13 Jul 2026

Also for other professional secrecy holders: These explanations apply accordingly to tax advisors, auditors, notaries, patent attorneys, and healthcare professions; the respective variant of the confidentiality agreement in the Trust Center is decisive.

This is not legal advice. This guide explains how Zentre supports use by professional secrecy holders and which professional-law obligations remain with the customer. The final assessment rests with the respective law firm; in case of doubt, professional-law advice should be obtained.

1. Purpose

Lawyers are subject to a strict duty of confidentiality. This guide shows (a) the professional-law framework applicable when using AI/cloud services, (b) how Zentre supports this framework technically and contractually, and (c) which obligations remain with the law firm.

2. Professional-law framework

- **Section 43a (2) BRAO** — confidentiality as a core duty.
- **Section 2 BORA** — concretization: obligation to implement risk-adequate technical and organizational measures at the state of the art; continuation beyond the end of the mandate.
- **Section 43e BRAO** — express permission to engage service providers (including IT/cloud) subject to conditions: necessity, binding the service provider in text form, instruction about confidentiality, careful selection, and the ability to terminate in the event of a breach of duty.
- **Section 203 StGB** — criminal-law backstop; since the 2017 reform (subsections 3/4), the involvement of “contributing persons” is permissible, whereby they become criminally liable and the firm must bind them.
- **CCBE Code of Conduct** — cross-border confidentiality; sensitivity to foreign disclosure obligations (e.g., the US CLOUD Act).

3. How Zentre supports

- **Section 203 mode:** a dedicated configuration for the processing of protected secrets — EU hosting (Scaleway, Paris), EU-based routing via Cortecs, **zero data retention**, restriction of model selection to authorized EU endpoints.
- **Exclusively EU-controlled models:** In Section 203 mode, only EU providers (e.g., Mistral) or models self-hosted in the EU by Cortecs are available; the model maker has no access. Endpoints of model providers with a non-EU parent are technically deactivated in Section 203 mode — the risk of foreign disclosure obligations (e.g., the US CLOUD Act) is structurally minimized, as all model providers, the AI gateway (Cortecs, Austria), and the hosting (Scaleway, France) are not subject to a non-EU parent company.
- **Separate confidentiality agreement under Section 203 StGB** (DE: Section 203 StGB / AT: Section 80 WTBG 2017, Section 9 RAO, Sections 121 et seq. öStGB / CH: Article 321 StGB) with instruction under Section 203 (4) StGB, binding of EZTO employees in text form, and **flow-down** to subprocessors/model providers.
- **No training** with client data (excluded contractually; the exclusion is passed on to the model providers via flow-down; for models operated by Cortecs itself, additionally without technical manufacturer access).

- **Web search in Section 203 mode:** web search is deactivated in Section 203 mode. Protected secrets (client data) do not belong in search queries.
- **Mandate separation through a separate tenant:** client data is processed in a dedicated, logically isolated environment separated from normal operation (own tenant) with its own, isolated knowledge base; 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; switching to the internal tenant is a pure view/navigation switch and transfers no content.
- **TOM at the state of the art** (encryption in transit TLS 1.2 or higher / data and artifacts at rest AES-256 (at minimum), RBAC, tenant separation, logging); ISO/IEC 27001-aligned ISMS; certification underway (current status and standard evidence package in the Trust Center).
- **Need-to-know access** by EZTO, as limited as possible, approved, and logged.

4. Obligations remaining with the law firm

1. **Check necessity** and enter only the data necessary for the mandate (**data minimization**).
2. **Careful selection/monitoring** of the service provider (this guide, the DPA, the confidentiality agreement, and the evidence serve as documentation).
3. **Conclude the confidentiality agreement** (Phase 1: sign via contact; Phase 2: in-app) — a prerequisite for Section 203 mode.
4. **Process client data exclusively in the Section 203 tenant**; process internal/mandate-free matters in the normal tenant; **in case of doubt, the Section 203 tenant**. Do not enter protected secrets outside the Section 203 tenant.
5. **Bind your own employees/users** to confidentiality.
6. **Check the mandate reference/consent** on a case-by-case basis where required under professional law.
7. **Review AI outputs professionally** (no warranty as to accuracy; responsibility remains with the firm).

5. Short checklist

- ☐ Confidentiality agreement (Section 203) signed
- ☐ Section 203 mode activated
- ☐ Own employees bound
- ☐ Data minimization/need-to-know observed
- ☐ Evidence/DPA/TOM placed on file
- ☐ Web search in Section 203 mode observed (deactivated; no client secrets in search queries)

6. Allocation of responsibility

The law firm remains the controller under data protection and professional law; EZTO acts as a contributing person/processor. The activation of the Section 203 mode rests with the law firm. EZTO provides the suitable configuration and the contractual instruments.

7. Sources

BRAO (Section 43a, Section 43e) · BORA (Section 2) · Section 203 StGB · CCBE Code of Conduct · GDPR/ BDSG · AI Act (Regulation (EU) 2024/1689). Current versions are available, among others, via the German Federal Bar (brak.de) and gesetze-im-internet.de.