BORA-Leitfaden

BORA Guide

Stand: 06. Jun 2026

DEUTSCH

> Kein Rechtsrat. Dieser Leitfaden erläutert, wie Zentre den Einsatz durch Berufsgeheimnisträger unterstützt und welche berufsrechtlichen Pflichten beim Kunden 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 (Fassung 01.12.2025) — 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 (Fassung 2026) — grenzüberschreitende Verschwiegenheit; Sensibilität gegenüber ausländischen Offenlegungspflichten (z. B. US CLOUD Act).

3. Wie Zentre unterstützt

• § 203-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.

• Zwei wählbare Stufen (Sie entscheiden):

• Stufe A — strikt (EU-kontrolliert): ausschließlich EU-Anbieter (z. B. Mistral) bzw. von Cortecs in der EU selbst betriebene Modelle; der Modellhersteller erhält keinen Zugriff. Höchste Rechtssicherheit (kein US-Mutterkonzern/CLOUD-Act-Bezug).

ENGLISH (US)

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 (version of 1 December 2025) — 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 (2026 version) — 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.

• Two selectable tiers (you decide):

• Tier A — strict (EU-controlled): exclusively EU providers (e.g., Mistral) or models self-hosted in the EU by Cortecs; the model maker has no access. Highest legal certainty (no US parent/CLOUD Act exposure).

DEUTSCH	ENGLISH (US)
• Stufe B — EU-gehostet: zusätzlich EU-Endpunkte von US-Anbietern (mit ZDR/SCC). Breitere Modellauswahl; mögliche Restexposition gegenüber ausländischen Offenlegungspflichten — bewusst zu wählen.	• Tier B — EU-hosted: additionally EU endpoints of US providers (with ZDR/SCC). Broader model selection; possible residual exposure to foreign disclosure obligations — to be chosen deliberately.
• Gesonderte Verschwiegenheitsvereinbarung nach § 203 StGB (DACH: § 203 StGB / § 121 öStGB / Art. 321 CH-StGB) mit Belehrung nach § 203 Abs. 4 StGB, Verpflichtung der EZTO-Mitarbeitenden in Textform und Flow-down auf Subprozessoren/Modellanbieter.	• Separate confidentiality agreement under Section 203 StGB (DACH: Section 203 StGB / Section 121 öStGB / Article 321 CH-StGB) with instruction under Section 203 (4) StGB, binding of EZTO employees in text form, and flow-down to subprocessors/model providers.
• Kein Training mit Mandantendaten (vertraglich und technisch ausgeschlossen, an Provider durchgereicht).	• No training with client data (excluded contractually and technically, passed on to providers).
• TOM nach Stand der Technik (Verschlüsselung in Übertragung (TLS 1.3) und ruhender Daten/Artefakte (AES-256-GCM), RBAC, Mandantentrennung, Protokollierung); ISMS nach ISO/IEC 27001 im Aufbau (Zertifizierung in Vorbereitung; Ersatznachweise auf Anfrage).	• TOM at the state of the art (encryption in transit TLS 1.3 / data and artifacts at rest AES-256-GCM, RBAC, tenant separation, logging); ISMS pursuant to ISO/IEC 27001 in progress (certification in preparation; alternative evidence on request).
• Need-to-know-Zugriff seitens EZTO, möglichst begrenzt, freigegeben und protokolliert.	• Need-to-know access by EZTO, as limited as possible, approved, and logged.
• Websuche im § 203-Modus: Die Websuche ist in beiden § 203-Modi (EU-kontrolliert und EU-gehostet) deaktiviert. Geschützte Geheimnisse (Mandantendaten) gehören nicht in Suchanfragen.	
• Mandatstrennung durch separaten Tenant: Mandantsdaten werden in einer vom Normalbetrieb physisch getrennten Umgebung (eigener Tenant) mit eigener, isolierter Wissensbasis verarbeitet. 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	**4. Obligations remaining with the law firm**
1. Erforderlichkeit prüfen und nur die für das Mandat erforderlichen Daten eingeben (Datenminimierung).	1. Check necessity and enter only the data necessary for the mandate (data minimization).
2. Sorgfältige Auswahl/Überwachung des Dienstleisters (dieser Leitfaden, AVV, Verschwiegenheitsvereinbarung und Nachweise dienen der Dokumentation).	2. Careful selection/monitoring of the service provider (this guide, the DPA, the confidentiality agreement, and the evidence serve as documentation).
3. Verschwiegenheitsvereinbarung abschließen (Phase 1: per Kontakt unterzeichnen; Phase 2: in-App) — erforderlich für beide Stufen.	3. Conclude the confidentiality agreement (Phase 1: sign via contact; Phase 2: in-app) — required for both tiers.
4. Mandatsdaten ausschließlich im § 203-Tenant verarbeiten (Stufe A „EU-kontrolliert" oder B „EU-gehostet"); interne/mandatsfreie Vorgänge im Normal-Tenant; im Zweifel § 203-Tenant. Außerhalb des § 203-Tenants keine geschützten Geheimnisse eingeben.	4. Process client data exclusively in the Section 203 tenant (Tier A "EU-controlled" or B "EU-hosted"); 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. Eigene Mitarbeitende/Nutzer zur Verschwiegenheit verpflichten.	5. Bind your own employees/users to confidentiality.
6. Mandantenbezug/Einwilligung im Einzelfall prüfen, soweit berufsrechtlich erforderlich.	6. Check the mandate reference/consent on a case-by-case basis where required under professional law.
7. KI-Ausgaben fachlich prüfen (keine Gewähr für Richtigkeit; Verantwortung verbleibt bei der Kanzlei).	7. Review AI outputs professionally (no warranty as to accuracy; responsibility remains with the firm).

DEUTSCH	ENGLISH (US)
5. Kurz-Checkliste • [ ] Verschwiegenheitsvereinbarung (§ 203) unterzeichnet • [ ] Stufe gewählt (A strikt / B EU-gehostet) und dokumentiert • [ ] § 203-Modus aktiviert • [ ] eigene Mitarbeitende verpflichtet • [ ] Datenminimierung/Need-to-know beachtet • [ ] Nachweise/AVV/TOM zur Akte genommen • [ ] Websuche im § 203-Modus beachtet (standardmäßig deaktiviert; keine Mandantengeheimnisse in Suchanfragen)	**5. Short checklist** • [ ] Confidentiality agreement (Section 203) signed • [ ] Tier selected (A strict / B EU-hosted) and documented • [ ] 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 by default; no client secrets in search queries)
6. Verantwortungsabgrenzung Die Kanzlei bleibt datenschutz- und berufsrechtlich Verantwortliche; EZTO wird als mitwirkende Person/Auftragsverarbeiter tätig. Die Auswahl der Stufe und die Aktivierung des § 203-Modus liegen bei der Kanzlei. EZTO stellt die hierfür geeignete Konfiguration und die vertraglichen Instrumente bereit.	**6. Allocation of responsibility** The law firm remains the controller under data protection and professional law; EZTO acts as a contributing person/processor. The selection of the tier and the activation of the Section 203 mode rest with the law firm. EZTO provides the suitable configuration and the contractual instruments.
7. Quellen BRAO (§ 43a, § 43e) · BORA (§ 2, Fassung 01.12.2025) · § 203 StGB · CCBE-Berufsregeln (2026) · DSGVO/BDSG · KI-VO (VO (EU) 2024/1689). Aktuelle Fassungen u. a. über die Bundesrechtsanwaltskammer (brak.de) und gesetze-im-internet.de.	**7. Sources** BRAO (Section 43a, Section 43e) · BORA (Section 2, version of 1 December 2025) · Section 203 StGB · CCBE Code of Conduct (2026) · 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.