AVV Legal-Center Kanzlei-Side — Template-Stack + Kanzlei-Addendum

⚠️ Eigenbau-Risk-Flag (zwingend dokumentieren)

User-Entscheidung 2026-04-20: Alles Eigenbau, keine Anwalt-Beauftragung. Dieser AVV entsteht ohne anwaltliche Prüfung. CFO flaggt folgende Risiken:

- Haftungsklauseln nicht AGB-Kontrolle-geprüft (§305-310 BGB)
- §203 StGB-Compliance bei Kanzlei-Mandatsgeheimnis ist **strafrechtlich relevant** bei Fehlern — nicht nur zivilrechtlich
- Kanzlei-Kunden werden in eigener Prüfung Widersprüche einlegen → Anpassungs-Aufwand iterativ
- Bei erstem Datenschutz-Vorfall oder Audit ist Eigenbau-AVV Angriffsfläche

Mitigation: Template-Stack aus amtlichen + Branchenverbands-Mustern (maximale Risiko-Reduktion ohne Anwalt). Spätere Anwalts-Review ausdrücklich empfohlen sobald Budget freigegeben.

Template-Stack (Eigenbau-Bauplan)

Grundgerüst: BayLDA Muster AV-Vertrag (Bayerisches Landesamt für Datenschutzaufsicht) **Drittland-Modul:** EU SCCs 2021/914, Modul 2 (Controller→Processor) **Kanzlei-Addendum:** §§6-7 (siehe Struktur unten), §203 StGB + §43e BRAO + §50 BRAO **TOM-Anlage:** Starter aus Sipgate/Mittwald-Struktur abstrahiert + Lakeware-Spezifika

Quellen (alle kostenlos, Public Domain oder kompatible Lizenz)

Quelle	URL	Lizenz
BayLDA Muster	https://www.lda.bayern.de/media/muster/muster_adv.pdf	Public Domain (Behörde)
EU SCCs 2021/914	https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj	EU Public Domain
DSK Kurzpapier Nr. 13	https://www.datenschutzkonferenz-online.de/kurzpapiere.html	Public Domain
LfDI BW Orientierungshilfe	https://www.baden-wuerttemberg.datenschutz.de/auftragsverarbeitung/	Public Domain

Quelle	URL	Lizenz
BRAK §43e Hinweise	https://www.brak.de/fuer-anwaelte/berufsrecht/	Public Domain
EDPB Guidelines 07/2020	https://edpb.europa.eu — Controller/Processor	Public Domain

AVV-Struktur (zusammengesetzt für Kanzlei-Kontext)

```
§1  Präambel / Vertragsgegenstand
§2  Begriffsbestimmungen
§3  Gegenstand, Art, Zweck, Dauer (→ Anlage 1)
§4  Weisungsrecht Verantwortlicher
§5  Pflichten Auftragsverarbeiter (Art. 28 Abs. 3 DSGVO)
§6  Mandatsgeheimnis & §203 StGB                    ← KANZLEI-
ADDENDUM
§7  Verpflichtung der Beschäftigten (über DSGVO hinaus) ← KANZLEI-
ADDENDUM
§8  Technisch-organisatorische Maßnahmen (→ Anlage 2)
§9  Sub-Auftragsverarbeiter (→ Anlage 3)
§10 Drittlandstransfer / SCCs 2021 Modul 2 (→ Anlage 4)
§11 Betroffenenrechte / Mitwirkung
§12 Meldung von Datenschutzverletzungen (24h an Kanzlei, nicht
72h!)
§13 Prüf- und Audit-Rechte
§14 Löschung und Rückgabe (BRAO-Aufbewahrungsfristen beachten!)
§15 Haftung
§16 Schlussbestimmungen (Schriftform, Gerichtsstand München)

Anlagen:
1 – Beschreibung der Verarbeitung (Datenarten, Betroffene, Zweck,
Dauer)
2 – Technisch-organisatorische Maßnahmen (Kanzlei-Level)
3 – Genehmigte Sub-Auftragsverarbeiter
4 – SCCs 2021 Modul 2 (ausgefüllt)
5 – Formular: Einzelverpflichtung Beschäftigte auf
Verschwiegenheit
```

Kanzlei-Spezifische Pflicht-Klauseln (§6 + §7)

§6 Mandatsgeheimnis & §203 StGB

- AV erkennt an, dass verarbeitete Daten dem **anwaltlichen Berufsgeheimnis** unterliegen (§43a BRAO, §2 BORA)
- Mitarbeitende AV sind **"mitwirkende Personen"** i.S.d. §203 Abs. 3 StGB
- Zugriff durch Mitarbeitende AV nur nach **schriftlicher Verpflichtung** auf Verschwiegenheit (→ Anlage 5)

- Verstoß kann **strafrechtliche Konsequenzen** (§203 StGB) und berufsrechtliche Folgen für die Kanzlei haben

§7 Verpflichtung der Beschäftigten

- Jede Person mit potenziellem Datenzugriff **einzeln** verpflichtet (Formular Anlage 5)
- Dokumentation vor Zugangs-Gewährung, nicht erst danach
- Pflicht auch nach Ende der Tätigkeit (Nachwirkung)
- Kanzlei hat Einsichtnahme-Recht in Verpflichtungs-Dokumentation

TOMs (Anlage 2) — Kanzlei-Level

Vertraulichkeit - Zutritt: Cloud-RZ (Provider-Zertifikat ISO 27001 oder gleichwertig) - Zugang: MFA (TOTP/WebAuthn) verpflichtend, Passwort-Policy NIST SP 800-63B - Zugriff: RBAC mit Least-Privilege, Separation-of-Duties Dev/Ops - **Tenant-Isolation:** Kanzlei-Daten per Tenant-ID separiert, logische Trennung auf DB-Ebene (Row-Level-Security) - Pseudonymisierung: Dev-/Test-Umgebung nur mit anonymisierten Daten

Integrität - Verschlüsselung at-rest: **AES-256** (Pflicht bei Kanzlei-Daten) - Verschlüsselung at-transit: **TLS 1.3** (Mindeststandard) - Audit-Log aller CRUD-Operationen, append-only, **Retention min. 6 Monate** (BRAK-IT-Sicherheitshinweise)

Verfügbarkeit + Belastbarkeit - Backup: verschlüsselt (`age` oder gleichwertig), Off-Site - RTO 4h, RPO 1h - DR-Runbook dokumentiert

Wiederherstellung - Restore-Test quartalsweise, Protokoll

Incident-Response - **Meldepflicht an Kanzlei binnen 24h** (strenger als Art. 33 DSGVO 72h), damit Kanzlei eigene Meldepflichten einhalten kann - Runbook + Kontaktkette, Post-Mortem binnen 14 Tagen

Privacy-by-Design (Art. 25) - Default-Retention minimiert - Pen-Test jährlich extern (z.B. Cure53 / SySS) — wenn Budget vorhanden

Sub-AV-Liste (Anlage 3) — Draft für Legal-Center

Kategorie	Anbieter	Sitz	Drittland-Status	Kanzlei-OK?
Hosting/Infra	`<TBD – CIO-Entscheidung, EU bevorzugt>`	EU bevorzugt	direkt DSGVO	✅ wenn EU
CDN	Cloudflare Inc.	US	EU-US DPF (aktiv seit 07/2023)	🟡 — TIA nötig
E-Mail	Postmark / SendGrid	US	DPF + SCC-Fallback	🟡 — kein Mandanten-Content

Kategorie	Anbieter	Sitz	Drittland-Status	Kanzlei-OK?
Monitoring	Grafana Cloud (EU)	EU	direkt	✅
AI-Proxy LLM	Anthropic (Claude), Google (Gemini), Mistral (FR)	US/FR	DPF + SCC / EU	🟡 — **kein Mandanten-Content** durch AI-Proxy
Lokale LLM	Qwen self-hosted	intern (Voss Mobil Infra)	kein Drittland	✅
Explizit ausgeschlossen	DeepSeek, andere CN	CN	kein AdEq, PIPL-Risiko	❌ kein Mandanten-Content
Billing	Mollie (Kanzlei-Enterprise)	NL (EU)	direkt	✅ best fit

Ablehnungsrecht Kanzlei: binnen 14 Tagen nach Notifikation, begründet.

Drittlandstransfer-Klausel (§10)

```
§10 Drittlandstransfer
(1) Transfers in Drittländer erfolgen nur auf Basis:
    a) Angemessenheitsbeschluss (Art. 45 DSGVO), insbesondere
       EU-US Data Privacy Framework für zertifizierte US-
Empfänger;
    b) Standardvertragsklauseln 2021/914 (Modul 2) inkl. TIA
       (Transfer Impact Assessment);
    c) Ausnahmen nach Art. 49 DSGVO nur im Einzelfall.
(2) Für Mandatsdaten gilt: Transfers in die VR China werden
ausgeschlossen.
(3) AI-Proxy-Routing für Mandatsdaten erfolgt ausschließlich über
    EU-Endpunkte oder lokale Inference (Qwen self-hosted).
```

Löschung/Rückgabe (§14) — Kanzlei-spezifisch

- Nach Vertragsende: **kryptografische Vernichtung** + schriftliche Bestätigung
- **BRAO-Aufbewahrungsfristen beachten:** §50 BRAO = Handakten 6 Jahre
- Wahlrecht Kanzlei: Rückgabe (verschlüsselt, via SCP/SFTP) **oder** Löschung
- Fristen: 30/90 Tage nach Auswahl

Operative CFO-Todos (nach User-Approval)

1. **Templates herunterladen:** BayLDA-Muster + DSK + SCCs als Basis in `cfo/decisions/legal-center-avv-draft.docx` zusammenführen (manuelle Arbeit, ca. 3-4h)
2. **Kanzlei-Addendum** aus diesem File in den Vertrag einbauen

3. **TOMs** mit CIO abstimmen (was wir technisch wirklich bieten)
4. **Sub-AV-Liste** mit CIO + COO final besetzen (welche Services nutzt Lakeware Legal Center tatsächlich)
5. **Anlage 5** (Verpflichtungs-Formular) separat erstellen
6. **PDF-Export + digital signierbare Version** (DocuSign-light oder ähnlich) — User-Entscheidung ob Signing-Tool
7. **Kanzlei-Customer-Kommunikation:** AVV im Onboarding-Flow integrieren (COO-Scope)

Offene Punkte / Escalations

#	Punkt	Owner
1	Final-Sub-AV-Liste (was nutzen wir wirklich?)	CFO + CIO + COO
2	Signing-Tool-Wahl (DocuSign, OpenSignature, manuelles PDF)	CFO + COO
3	Erste Kanzlei-Kunden: bestehender AVV wird von Kanzlei geprüft werden → iterativer Review-Prozess	CFO
4	Anwalts-Review nachziehen sobald Budget freigegeben	P1 bei erstem Incident

Quellen + Lizenzen

Siehe Tabelle oben. Template-Lizenzen geprüft: - BayLDA = amtliches Werk, §5 UrhG gemeinfrei - DSK = Public Domain - SCCs = EU Public Domain - BRAK = Public Domain

Kein Copy-Paste ohne Anpassung. Alle Anlagen + individuelle Passagen sind Platzhalter zu füllen.

Frist

- User-Approval dieses Drafts: bis morgen Abend 2026-04-21
- AVV-PDF-Erstellung: Do 2026-04-23 (laut CEO-Task)
- Go-Live Legal-Center mit AVV: Fr 2026-04-24

Änderungs-History

Datum	Änderung
2026-04-21	Initial nach Subagent-Recherche + CFO-Analyse