

AVV-Baustein (Art. 28 DSGVO) - Gosign-Selbstverpflichtung und Gateway-Regeln

v0.11 (2026-08-19) - Muster zur anwaltlichen Einzelfall-Anpassung, ohne Gewähr, ersetzt keine Rechtsberatung.

Dieser Baustein ergänzt den Auftragsverarbeitungsvertrag zwischen Kanzlei/ Praxis (Verantwortlicher) und Gosign GmbH (Auftragsverarbeiter) um die für Berufsgeheimnisträger wesentlichen Zusagen. Er benennt Gosign ausdrücklich als **eigenes verpflichtetes Glied der 203er-Kette** - nicht nur die nachgelagerten Modell-Anbieter. Dieser Baustein ergänzt den Haupt-AVV; die lit.-a-Weisungsausnahme und die Remonstrationspflicht (Art. 28 Abs. 3 UAbs. 2 DSGVO) deckt der Haupt-AVV ab.

1. Gegenstand. Verarbeitung von Eingaben/Ausgaben KI-gestützter Dienste über den Gosign-Gateway (Pseudonymisierung vor Modell-Aufruf, Wieder- Einsetzung danach, Schlüssel-/Budget-Verwaltung, Audit-Protokollierung). Stammbblatt nach Art. 28 Abs. 3 UAbs. 1 DSGVO (je Vertrag auszufüllen):

Gegenstand	Dauer	Art und Zweck der Verarbeitung	Datenarten	Kategorien betroffener Personen
[AUSFÜLLEN]	[AUSFÜLLEN]	[AUSFÜLLEN]	[AUSFÜLLEN]	[AUSFÜLLEN]

2. Personal-Verpflichtung. Alle mit der Verarbeitung befassten Personen sind auf Vertraulichkeit nach Art. 28 Abs. 3 lit. b, Art. 32 DSGVO **und** zur Verschwiegenheit nach § 203 StGB in Textform verpflichtet und über die Strafbarkeit belehrt (siehe Zusatzvereinbarung, § 3-4).

3. Gateway-Regeln (technisch-organisatorische Kernzusagen). a) **Zero-Retention im Gateway:** Klartext-Inhalte werden nicht persistent gespeichert; Verarbeitung erfolgt transient. b) **Pseudonym-Mappings** sind ephemere bzw. mandantenindividuell verschlüsselt mit definierter TTL; kein menschlicher Zugriff im Regelbetrieb. c) **Break-Glass:** Ausnahme-Zugriffe nur nach Vier-Augen-Prinzip, protokolliert, mit nachträglicher Information des Verantwortlichen. d) **Audit-Protokoll klartextfrei:** append-only, hash-verkettet, ohne Inhaltsklartext (Hash-Referenzen), inkl. Modell-/Versions-Metadaten. e) **Schlüssel** der Modell-Anbieter liegen in einem Schlüsselverwaltungssystem; mandantengetrennte Verwaltung. *(Stand der Umsetzung: Anforderungs-Zusagen des Angebots; produktive Feature-Zusagen erst nach Umsetzungs-Nachweis.)*

4. Weisungen, Unterstützung, Betroffenenrechte. Verarbeitung nur auf dokumentierte Weisung; Unterstützung bei Betroffenenrechten (Art. 12-23) sowie nach Art. 28 Abs. 3 lit. f DSGVO bei den Pflichten aus den Artikeln 32 bis 36 DSGVO: Sicherheit (Art. 32), Meldungen (Art. 33/34: unverzüglich, spätestens so, dass der Verantwortliche seine 72-Stunden-Frist wahren kann), DSFA und Vorabkonsultation (Art. 35/36 - Zulieferbaustein: DSFA-Vorlage).

5. Subprozessoren. Nur gemäß Subprozessoren-Liste (inkl. § 203- Kettenverpflichtung nach Zusatzvereinbarung § 3); Änderungen mit Vorab-Information und Widerspruchsrecht.

6. Drittlandtransfers. Nur nach Maßgabe des Drittlandtransfer-Bausteins. CLOUD-Act-freie Wege sind vorgesehen; den aktuellen Status je Bezugsweg weist die Subprozessoren-Liste aus.

7. Löschung/Rückgabe. Nach Vertragsende Löschung bzw. Rückgabe gemäß dem Baustein zu Aufbewahrung, Einwilligung und Transparenz; gesetzliche Aufbewahrungspflichten bleiben unberührt.

8. Nachweis- und Prüfrechte. Gosign stellt dem Verantwortlichen alle zum Nachweis der Einhaltung dieses Bausteins erforderlichen Informationen zur Verfügung und duldet und unterstützt Überprüfungen - einschließlich Inspektionen - durch den Verantwortlichen oder einen von ihm beauftragten, seinerseits der Verschwiegenheit unterliegenden Prüfer (Art. 28 Abs. 3 lit. h DSGVO).