

Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung - DSGVO)

ENTWURF - noch nicht abschließend; einzelne Stellen sind zu ergänzen. Diese Fassung ist fachlich vorbereitet und gegen Art. 28 DSGVO, die AGB der Gosign GmbH und die Datenschutzerklärung abgeglichen. Sie ist **nicht rechtsverbindlich**, solange sie nicht als verbindliche Fassung veröffentlicht ist. Wir legen sie Ihnen bewusst schon jetzt vor, damit Sie den Inhalt kennen und Ihre Anmerkungen einbringen können, bevor die Endfassung gezeichnet wird. Stellen, die mit dem Vermerk ERGÄNZEN gekennzeichnet sind, enthalten bewusst **keine** erfundenen Angaben. Dieser Entwurf hat **26 offene Stellen**; jede steht am Ende unter „Offene Punkte“ mit nächstem Schritt und zuständiger Seite. Die kundenspezifischen Angaben - Firma, Anschrift, Vertretung, Ansprechpartner und beauftragte Leistungsvariante - werden bei Vertragsschluss aus den Stammdaten des Kunden eingesetzt. Solange sie fehlen, steht an ihrer Stelle sichtbar die benannte Lücke.

Stand: **v1-2026-08**

Was produktiv ist und was vereinbart, aber nicht aktiviert. Der Vertrag beschreibt die Verarbeitung vollständig — auch die Teile, die noch nicht laufen. Was davon heute in Betrieb ist, steht hier:

Verarbeitung	Betriebsstatus
Hosting, Auslieferung und Formular-Zustellung des Webauftritts	produktiv
Mail-Betrieb über Google Workspace in EU-Konfiguration	produktiv
Ablage und Weitergabe von Meldungen über Sicherheitslücken	produktiv
BV-Konto und KI-gestützter Entwurfsassistent	produktiv
Erzeugung des Vertrags aus Kundenstammdaten	vereinbart, noch nicht produktiv aktiviert
Selbstbedienung mit Domain-Nachweis	vereinbart, noch nicht produktiv aktiviert

Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „**AVV**“ oder „**Vertrag**“) konkretisiert die datenschutzrechtlichen Pflichten der Parteien für die Leistungen, die die Gosign GmbH für den Verantwortlichen erbringt.

Der Vertrag deckt **zwei Leistungsvarianten** ab. Welche gilt, richtet sich nach den tatsächlich beauftragten Leistungen; werden beide bezogen, gelten beide nebeneinander:

Variante	Leistungen	Anlage 1
Variante A - KI-Leistungen	„BV-Konto“ (Funktion „Für später speichern“) und der KI-gestützte Entwurfsassistent „BV-KI-Drafter“	Abschnitt A
Variante B - Website-Betrieb	Erstellung, Hosting, Pflege und Betrieb von Webauftritten einschließlich Formularen, Mailzustellung und Betriebsprotokollen	Abschnitt B

Beauftragt ist: [ANGABE FEHLT: Beauftragte Leistungsvariante].

Alle Paragraphen dieses Vertrags gelten für **beide** Varianten. Nur dort, wo die Verarbeitung sich tatsächlich unterscheidet - Art, Zweck und Umfang (§ 3), betroffene Personen (§ 4), Datenkategorien (§ 5) sowie die Anlagen 1, 2 und 4 - ist nach Varianten getrennt geregelt. § 10 gilt ausschließlich für Variante A.

Der AVV ergänzt die zwischen den Parteien geltenden Allgemeinen Geschäftsbedingungen der Gosign GmbH (nachfolgend „**AGB**“, aktuelle Fassung abrufbar unter gosign.de/de/agb/). § 13 der AGB sieht den Abschluss dieses AVV ausdrücklich vor.

Soweit der Verantwortliche eine eigene, DSGVO-konforme AVV-Vorlage bereitstellt, kann diese nach Maßgabe von § 13 der AGB an die Stelle dieses Vertrags treten.

§ 1 Parteien des Vertrags

(1) **Auftragsverarbeiter** im Sinne von Art. 4 Nr. 8 DSGVO:

Gosign GmbH, Hallerstraße 8, 20146 Hamburg, Deutschland (nachfolgend „**Gosign**“ oder „**Auftragsverarbeiter**“). Kontakt in Datenschutzangelegenheiten: datenschutz@gosign.de Hinweis: Bei der Gosign GmbH ist gemäß § 38 Abs. 1 BDSG derzeit kein Datenschutzbeauftragter zu bestellen, da nicht ständig mindestens 20 Personen mit der automatisierten Verarbeitung personenbezogener Daten befasst sind. Amtsgericht Hamburg, HRB 112197; Umsatzsteuer-Identifikationsnummer DE215891388; vertreten durch die Geschäftsführer Bert Gogolin und Dieter Gogolin

(2) **Verantwortlicher** im Sinne von Art. 4 Nr. 7 DSGVO ist das die Leistungen beziehende Unternehmen:

[ANGABE FEHLT: Firma des Verantwortlichen], [ANGABE FEHLT: Anschrift des Verantwortlichen], vertreten durch [ANGABE FEHLT: Vertretungsberechtigte Person] ([ANGABE FEHLT: Funktion der vertretungsberechtigten Person]) - nachfolgend „**Verantwortlicher**“. Kontakt in Datenschutzangelegenheiten: [ANGABE FEHLT: Datenschutz-Kontakt des Verantwortlichen]

(3) **Klarstellung für berufsprivilegierte Berater.** Kanzleien, Steuerberatungen, WP- und sonstige Beratungsgesellschaften tragen als Vertragspartner ihre **eigene** Firma ein - nicht die der betreuten Mandanten. Für die in ihrer beruflichen Tätigkeit verarbeiteten Daten sind diese Berater **selbst Verantwortlicher** (vgl. § 11 StBerG, Art. 28 DSGVO). Dieser eine Vertrag deckt die gesamte berufliche Tätigkeit gegenüber Gosign ab; ein gesonderter AVV je Mandant ist gegenüber Gosign nicht erforderlich.

(4) Auftragsverarbeiter und Verantwortlicher: einzeln „**Partei**“, gemeinsam „**Parteien**“.

§ 2 Gegenstand, Rollenverteilung und Rangfolge

(1) **Gegenstand.** Verarbeitung personenbezogener Daten durch Gosign **ausschließlich im Auftrag und nach Weisung** des Verantwortlichen im Rahmen der beauftragten Leistungsvariante. Der Verantwortliche bleibt „Herr der Daten“ und allein verantwortlich für die Rechtmäßigkeit (Art. 5, 6 DSGVO).

(2) **Keine gemeinsame Verantwortlichkeit** nach Art. 26 DSGVO. Gosign verarbeitet nicht zu eigenen Zwecken.

(2a) **Zuständigkeit für die Bewertung.** Gosign stellt die Tatsachen und Nachweise bereit — eingesetzte Anbieter, Verarbeitungsorte, Aufbewahrung, technische Maßnahmen und deren Status nach Anlage 2. Die datenschutzrechtliche und, soweit einschlägig, berufsrechtliche Bewertung und Freigabe trifft der Verantwortliche. **Gosign behauptet eine solche Freigabe ausdrücklich nicht selbst**; eine technische Schutzmaßnahme ersetzt die Bewertung nicht.

(3) **Inhaltsklassifizierung.** Die Verantwortung dafür, welche Inhalte in die Leistungen eingebracht werden und welche Sensibilität sie haben, liegt **allein beim Verantwortlichen**. Gosign nimmt keine inhaltliche Vorabprüfung vor, gewährleistet aber die Maßnahmen nach Anlage 2 unabhängig von der Sensibilität.

(3a) **Eigene Anbieterverträge des Verantwortlichen.** Unterhält der Verantwortliche eigene Verträge — etwa mit seinem Hoster, seinem Mail-Anbieter oder einem Modell-Provider in seinem eigenen Konto —, bleiben diese Beziehungen außerhalb der Unterauftragnehmerkette von Gosign. Gosign erhält dort ausschließlich den weisungsgebundenen Zugriff, der für Administration und Wartung erforderlich ist, und ist für diese Anbieter nicht Vertragspartner. Eine Vereinbarung von Gosign mit einem solchen Anbieter erstreckt sich nicht auf die direkte Vertragsbeziehung des Verantwortlichen.

(4) **Rangfolge:** (i) zwingendes Datenschutzrecht, (ii) dieser AVV einschließlich seiner Anlagen, (iii) die AGB, (iv) sonstige Vereinbarungen. Bei Widersprüchen in datenschutzrechtlichen Fragen geht dieser AVV den AGB vor; im Übrigen gelten die AGB.

§ 3 Art, Zweck und Umfang der Verarbeitung

Der Umfang richtet sich in beiden Varianten nach dem beauftragten Leistungsumfang, den Eingaben des Verantwortlichen und den dokumentierten Weisungen (§ 6).

Variante A - KI-Leistungen

(1) **Art:** Erheben, Erfassen, Organisieren, Speichern, Auslesen, Verwenden, Übermitteln an den KI-Dienstleister zur Entwurfserzeugung, Einschränken, Löschen/Vernichten - im erforderlichen Umfang.

(2) **Zweck:** a) **BV-Konto** (Speicherung des Arbeitsstands sowie der Konto- und AVV-Akzeptanzdaten); b) **BV-KI-Drafter** (Erzeugung und Zustellung eines unverbindlichen Textentwurfs); c) **Missbrauchsbegrenzung** (verschlüsselte E-Mail-Adresse und anonyme Auswahl-Zusammenfassung).

(3) **Datensparsamkeit.** Die Leistungen sind auf **Beispiel- und Testangaben** ausgelegt, nicht auf echte Beschäftigtendaten; der Verantwortliche wird vorab darauf hingewiesen. Bei abweichender Nutzung gelten die Regelungen dennoch vollumfänglich.

Variante B - Website-Betrieb

(1) **Art:** Erheben, Speichern, Auslesen, Verwenden, Weiterleiten zur Zustellung, Einschränken, Löschen/Vernichten - im erforderlichen Umfang für Bereitstellung und Betrieb des Webauftritts.

(2) **Zweck:** a) **Hosting und Auslieferung** des Webauftritts einschließlich der dabei technisch anfallenden Verbindungsdaten; b) **Formular-Zustellung** (Kontakt-, Bewerbungs-, Anfrage- und Meldeformulare) an die vom Verantwortlichen benannten Postfächer; c) **Mail-Betrieb**, soweit Gosign den Versand oder Empfang für den Webauftritt übernimmt; d) **Betriebsprotokolle** (Logfiles) zur Fehlersuche, Erkennung von Missbrauch und Nachweis der Verfügbarkeit; e) **Pflege und Wartung** des redaktionellen Systems, soweit Gosign dabei auf Bestände mit Personenbezug zugreifen kann.

(3) **Kein Tracking als Auftragsleistung.** Reichweiten- oder Werbemessung ist nicht Bestandteil dieser Variante. Setzt der Verantwortliche solche Dienste ein, verantwortet er sie selbst; Gosign erbringt insoweit keine Auftragsverarbeitung. [VON LEGAL/OPS ZU ERGÄNZEN: bestätigen, ob im Einzelfall eine Messlösung mitbetreut wird - dann als eigene Zweckposition aufnehmen]

§ 4 Kategorien betroffener Personen

Die abschließende Festlegung trifft der Verantwortliche (Anlage 1).

Variante A - KI-Leistungen

a) Beschäftigte und Bewerber des Verantwortlichen; b) Mitglieder von Arbeitnehmervertretungen; c) Mandanten, Auftraggeber und Dritte (insbesondere bei berufsprivilegierten Beratern); d) Ansprechpartner und Nutzer des Verantwortlichen; e) weitere nach den konkreten Eingaben.

Variante B - Website-Betrieb

a) Besucher des Webauftritts; b) Personen, die ein Formular absenden (Interessenten, Kunden, Bewerber, Hinweisgeber); c) Empfänger und Absender der über den Webauftritt geführten Korrespondenz; d) Redakteure und Administratoren des Verantwortlichen; e) Personen, deren Daten der Verantwortliche in redaktionelle Inhalte einstellt.

§ 5 Kategorien personenbezogener Daten

(1) **Für beide Varianten gilt:** Stamm- und Kontaktdaten (Firma, Zustelladresse, Handlungsbefugnis) sowie Vertrags- und Nutzungsmetadaten nach § 12.

(2) **Besondere Kategorien (Art. 9 DSGVO).** Nicht Zweck der Leistungen und nicht vorgesehen. Da Freitexteingaben möglich sind, kann der Verantwortliche solche Daten einbringen; dann trägt er die Verantwortung für die Rechtsgrundlage (Art. 9 Abs. 2 DSGVO). Gosign sichert für alle Inhalte einheitlich die Maßnahmen nach Anlage 2 zu; sensible Inhalte werden nicht abgesenkt behandelt.

(3) **Beschäftigtenkontext (Art. 88 DSGVO).** Soweit Beschäftigtendaten im Kontext des Beschäftigungsverhältnisses verarbeitet werden, sind Art. 88 DSGVO in Verbindung mit den nationalen Beschäftigtendatenschutzregelungen sowie etwaige Betriebs- oder Dienstvereinbarungen vom Verantwortlichen zu beachten.

Variante A - KI-Leistungen

a) **Prompt- und Eingabeinhalte** (Freitext, potenziell beliebige personenbezogene Daten); b) **Modellantworten und Entwurfsinhalte**; c) **hochgeladene oder eingefügte Dokumentinhalte** [VON LEGAL/OPS ZU ERGÄNZEN: bestätigen, ob Datei-Uploads im Funktionsumfang]; d) **Embeddings und Vektordaten** (als potenziell personenbezogen behandelt) [VON LEGAL/OPS ZU ERGÄNZEN: bestätigen, ob eine Pipeline mit Personenbezug aktiv ist; sonst „nicht einschlägig“]; e) Konto- und Vertragsmetadaten (Akzeptanzzeitpunkt, akzeptierte Version, Status des Arbeitsstands).

Variante B - Website-Betrieb

a) **Formularinhalte** - die vom Absender ausgefüllten Felder einschließlich Freitext, Name, Kontaktdaten und Anhängen, soweit vorgesehen; b) **Kommunikationsinhalte** der über den Webauftritt ausgelösten Mail-Zustellung (Betreff, Nachrichtentext, Zustellstatus); c) **Verbindungs- und Protokolldaten** aus dem Hosting (IP-Adresse, Zeitpunkt, aufgerufene Adresse, Referrer, Browser- und Systemkennung) mit den Aufbewahrungsfristen nach § 13; d) **Zugangsdaten und Rollen** der Redakteure des Verantwortlichen im redaktionellen System; e) **Inhaltsdaten**, die der Verantwortliche selbst redaktionell einstellt und die Personenbezug aufweisen können.

§ 5a Beschriebene Verarbeitung, spätere Aktivierung

(1) Vereinbart heisst aktivierbar. Die in diesem Vertrag und seinen Anlagen vollständig beschriebene Verarbeitung ist bereits Vertragsgegenstand — auch soweit sie noch nicht produktiv aktiviert ist. Ihre spätere Aktivierung ändert allein den Betriebsstatus und **erfordert keinen Nachtrag** zu diesem Vertrag, sofern die Umsetzung der Beschreibung entspricht und die Abnahmenachweise dokumentiert sind.

(2) Zwei Stufen. Eine Aktivierung erfolgt zunächst **überwacht**: Der jeweilige Schritt wird von einer autorisierten Person ausgelöst und geprüft. Der Übergang in den **automatischen** Betrieb setzt voraus, dass die Testergebnisse der Abnahme vorliegen und vom Verantwortlichen angenommen sind — nicht, dass ein Datum erreicht ist.

(3) Wann ein Nachtrag doch nötig ist. Abschliessend in diesen Fällen: ein neuer **Zweck** der Verarbeitung; zusätzliche **Datenkategorien**; ein erweiterter **Empfängerkreis**; ein veränderter **Drittlandbezug**; eine geänderte **Aufbewahrung**; ein abgesenktes **Schutzniveau**; sowie jede Abweichung der Umsetzung von dem in den Anlagen beschriebenen Rahmen.

(4) Nachweis. Vor der Produktivaktivierung erstellen die Parteien ein gemeinsames Abnahmeprotokoll über die aktivierten Funktionen, die freigegebenen Verarbeitungspfade und den Stand der Kontrollen. Es ist ein Betriebs- und Nachweisdokument, keine Vertragsänderung.

§ 6 Weisungsrecht (Art. 28 Abs. 3 lit. a DSGVO)

(1) Verarbeitung ausschließlich auf **dokumentierte Weisung**, auch hinsichtlich einer Drittlandübermittlung, außer bei gesetzlicher Verpflichtung (dann Mitteilung vor der Verarbeitung, soweit nicht verboten). **(2)** Vertrag, Anlagen und bestimmungsgemäße Eingaben sind die anfängliche dokumentierte Weisung; mündliche Weisungen werden unverzüglich in Textform bestätigt. **(3)** Über die Leistungen hinausgehende Einzelweisungen bedürfen der Textform und eines Nachtrags; sie werden gegebenenfalls nach den AGB vergütet. **(4)** Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung des Verantwortlichen gegen die DSGVO oder gegen sonstige Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, so informiert er den Verantwortlichen unverzüglich. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung durch den Verantwortlichen auszusetzen; die Durchführung offensichtlich rechtswidriger Weisungen darf er ablehnen. Diese Hinweis- und Aussetzungsrechte lassen die alleinige Verantwortung des Verantwortlichen für die Rechtmäßigkeit seiner Weisungen unberührt (Art. 28 Abs. 3 UAbs. 2 DSGVO). **(5)** Weisungs- und Empfangsberechtigte sind in Anlage 3 benannt. [VON LEGAL/OPS ZU ERGÄNZEN: Namen und Erreichbarkeiten]

§ 7 Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO)

(1) Verpflichtung der befugten Personen zur Vertraulichkeit (oder gesetzliche Verschwiegenheit), fortwirkend über die Tätigkeit hinaus. **(2)** Zugriff nach dem Need-to-know-Grundsatz. **(3) Berufsgeheimnisträger (§ 203 StGB):** Soweit der Verantwortliche beruflicher Verschwiegenheit unterliegt (Anwalt, Steuerberater, Wirtschaftsprüfer, Arzt und berufsmäßige Gehilfen), verpflichtet Gosign alle mitwirkenden Personen einschließlich der Subunternehmer **schriftlich** zur Verschwiegenheit und belehrt sie über § 203 StGB, insbesondere Absatz 4 für mitwirkende Personen; Verpflichtungs- und Belehrungserklärungen werden dokumentiert und auf Anfrage nachgewiesen. Gosign gilt als „mitwirkende Person“ nach § 203 Abs. 3 StGB. **(4) Zugriffsort.** Produktive Inhaltsdaten, Backups, Supportinhalte und produktive Zugangsdaten werden ausschließlich durch ausdrücklich autorisierte Personen mit physischem Zugriffsort in Deutschland oder im EWR verarbeitet. Personal von Gosign außerhalb des EWR erhält keinen Zugriff auf Produktivdaten, Supportinhalte, Backups oder produktive Zugangsdaten. Entwicklungs-, Administrations- und Architekturtätigkeiten außerhalb des EWR erfolgen ausschließlich ohne Produktivdaten oder mit synthetischen beziehungsweise anonymisierten Daten. **(5)** Nachweis auf Verlangen.

§ 8 Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO)

(1) Die Maßnahmen nach Art. 32 DSGVO sind in **Anlage 2** beschrieben. (2) Eine Fortentwicklung ist zulässig, sofern das Schutzniveau nicht unterschritten wird; wesentliche Änderungen werden dokumentiert und auf Anfrage mitgeteilt. (3) Umfasst sind Pseudonymisierung und Verschlüsselung, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, Wiederherstellbarkeit sowie die regelmäßige Überprüfung. (4) **Mandantentrennung**: logische Trennung der Daten verschiedener Verantwortlicher (Datenbestände, Protokolle, Historien, Speicher, Schlüssel); kein Datenfluss zwischen Mandanten.

§ 9 Sub-Auftragsverarbeiter (Art. 28 Abs. 2 und 4 DSGVO)

(1) **Allgemeine Genehmigung** zur Inanspruchnahme weiterer Auftragsverarbeiter; die bei Vertragsschluss eingesetzten sind in **Anlage 4** je Leistungsvariante abschließend aufgeführt und damit genehmigt. Anlage 4 wird aus dem **Anbieter-Register** (Anlage 5) erzeugt, das Gosign fortlaufend pflegt; eine von Hand gepflegte Kopie im Vertragstext gäbe es damit nicht. Ein Wechsel wird im Register mit Datum, altem und neuem Stand dokumentiert und nach Absatz 2 vorab mitgeteilt. (2) **Vorab-Information und Widerspruchsrecht** bei Hinzuziehung oder Ersetzung: Textform, Frist mindestens **14 Kalendertage**. Die Information benennt mindestens Anbieter, Zweck, Standort, Datenkategorien, Aufbewahrungsdauer, Transfermechanismus und die wesentlichen Schutzmaßnahmen. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem **oder berufsrechtlichem** Grund widersprechen. (3) **Folgen**: einvernehmliche Lösung, sonst Kündigungsrecht des betroffenen Leistungsteils. (4) **Flow-Down (Art. 28 Abs. 4)**: dieselben Datenschutzpflichten werden jedem Sub-Auftragsverarbeiter auferlegt; **Gosign haftet** für deren Pflichteinhaltung. (5) **Modellprovider**. Ein Provider, der personenbezogene oder pseudonymisierte Daten, Mandats- oder Patientendaten, Originalanhänge oder sonstige fremde Geheimnisse erhalten kann, darf erst nach **dokumentierter Provider- und Pfadprüfung** und **schriftlicher Freigabe durch den Verantwortlichen** eingesetzt werden. Erforderlich sind mindestens: ein Auftragsverarbeitungsvertrag, belastbare Vertraulichkeitsregelungen, der Ausschluss der Nutzung zu allgemeinem Training oder zur Modellverbesserung, eine projekt- und modellbezogen bestätigte Zero- oder No-Retention-Konfiguration, die Festlegung zulässiger Regionen und Unterauftragnehmer sowie eine Bewertung möglicher Providerzugriffe und Drittlandbezüge. Eine gesonderte Verschwiegenheitsvereinbarung nach § 203 Abs. 4 StGB ist ein möglicher Nachweis; fehlt sie, ist vor Aktivierung eine dokumentierte berufsrechtliche Bewertung und ausdrückliche Freigabe des Verantwortlichen erforderlich. **Zero Retention ersetzt diese Bewertung nicht.** (6) **Modellregister statt Vertragsanhang**. Die Plattform bleibt provider- und modellneutral. Konkrete Modellnamen werden nicht dauerhaft in diesem Vertrag festgeschrieben, sondern in einem aktuellen Provider- und Modellregister geführt (Anlage 5). Ein Wechsel zwischen Modellen eines bereits freigegebenen Providers erfordert keine Vertragsänderung, solange Vertragsrolle, Datenklasse, Region, Aufbewahrung, Zugriffsmöglichkeiten, Transfermechanismus und Schutzniveau unverändert bleiben; der Wechsel wird im Register dokumentiert. (7) **Abgrenzung Plattform- und Modell-Provider**: im Standardbetrieb werden alle als Sub-Auftragsverarbeiter von Gosign geführt; eine abweichende „Bring-your-own-Tenant“-Konstellation ist gesondert zu vereinbaren. (8) Reine Telekommunikations- und Postdienste ohne Verarbeitung personenbezogener Daten sind keine Sub-Auftragsverarbeiter; die Sorgfaltspflicht bleibt unberührt.

(9) **Sperre bei Änderung der Grundlage**. Ändert ein Anbieter seine **Aufbewahrung**, seine **Protokollierung**, die **Region** der Verarbeitung, die **Trainingsnutzung** der Inhalte oder seine **Zugriffsmöglichkeiten**, wird der betroffene Verarbeitungspfad **bis zur erneuten Bewertung gesperrt** — er wird nicht lediglich weiter beobachtet. Gosign informiert den Verantwortlichen unverzüglich. Entfällt eine Vertraulichkeits- oder Sicherheitszusage, gilt dasselbe. Das Register wird mindestens jährlich sowie anlassbezogen überprüft.

§ 10 KI-spezifische Pflichten - gilt ausschließlich für Variante A

(1) **Kein Training mit Auftraggeberdaten**. Verwendung der im Auftrag verarbeiteten Daten ausschließlich zur Leistungserbringung; **kein** Training, Fine-Tuning, keine Entwicklung oder Evaluierung eigener oder fremder Modelle, außer bei ausdrücklicher gesonderter Freigabe in Textform (entspricht § 6.6 AGB). (2) **Flow-Down der Trainings-Beschränkung**: Modell-Provider werden vertraglich so eingesetzt, dass auch sie die Daten nicht zu Trainingszwecken nutzen und keine Content-Retention über die Anfrage hinaus vornehmen („Zero-Retention“, soweit providerseitig verfügbar). Der Status ist je Anbieter in Anlage 4 ausgewiesen. Für die Wege, die über eine gezeichnete Verschwiegenheitsvereinbarung nach § 203 Abs. 4 StGB laufen, ist der Ausschluss der Trainingsnutzung Vertragsbestandteil. Wo eine anbieterseitige Missbrauchs- oder Sicherheitsüberwachung besteht und keine genehmigte Ausnahme vorliegt, ist der Pfad **nicht als Zero Retention einzustufen**; das ist je Ressource nachzuweisen und nicht aus einer allgemeinen Produktaussage abzuleiten. (3) **In-flight statt at-rest**: Modellverarbeitung ohne persistente Speicherung beim Provider; vorübergehende Speicherung bei Gosign zur Zustellung nach § 13 und Anlage 2. (4) **Modell-Agnostik**: ein Modellwechsel ist ein Wechsel des Sub-Auftragsverarbeiters und löst die Information nach § 9 Abs. 2 aus. (5) **Pseudonymisierung (optional)**: Eingangs- und Ausgangsfilter, Pseudonymisierung vor der Übermittlung und Rückführung danach; bei reversibler Zuordnung gilt eine Zugriffs- und Schlüsselregelung. [VON LEGAL/OPS ZU ERGÄNZEN: ob aktiv] (6) **Keine automatisierte Entscheidung im Einzelfall (Art. 22**

DSGVO) - Entwürfe sind unverbindliche Vorschläge. **(7) Audit-Trail** inhaltsdatenarm: Metadaten ohne Eingabe- oder Dokumentinhalte (§ 12).

§ 11 Ort der Verarbeitung; Drittlandübermittlung (Kapitel V DSGVO)

(1) Grundsatz EU/EWR. Der Mail-Betrieb läuft über Google Workspace in EU-Konfiguration; Auslieferung und Routing der Webaufritte laufen über Cloudflare. Die persistenten Bestände liegen in Deutschland; die Region je Anbieter und Dienst weist Anlage 4 aus. [VON LEGAL/OPS ZU ERGÄNZEN: für diese Kundenumgebung Region und Rechenzentrum je Dienst bestätigen] **(2) Drittlandbezug in Variante A.** Ob eine Übermittlung in ein Drittland stattfindet, hängt am gewählten Modellpfad und ist je Pfad in Anlage 4 und im Modellregister nach Anlage 5 ausgewiesen. Pfade über Anbieter mit US-Mutterkonzern lösen die Prüfung nach Art. 44 ff. DSGVO aus, auch wenn die Vertragspartei in der EU sitzt und die Verarbeitung in einer EU-Region erfolgt. **(3) Geeignete Garantien:** je Pfad Standardvertragsklauseln (Art. 46 Abs. 2 lit. c) oder, soweit der Anbieter zertifiziert ist, der Angemessenheitsbeschluss zum EU-US Data Privacy Framework, ergänzend Standardvertragsklauseln. Das jeweils tragende Instrument ist in Anlage 4 je Anbieter benannt. **(4) Stand des Angemessenheitsbeschlusses:** Beschluss vom 10.07.2023 derzeit gültig; die Klage T-553/23 (Latombe) wurde am 03.09.2025 abgewiesen, das Rechtsmittel C-703/25 P ist anhängig. US-Übermittlungen werden deshalb **zusätzlich** auf Standardvertragsklauseln gestützt. In der Rechtssache C-703/25 P ist unter dem 04.06.2026 eine Entscheidung verzeichnet; ob sie das Rechtsmittel abschließt und mit welchem Ergebnis, ist vor Zeichnung am Gerichtsregister zu prüfen. Unabhängig davon werden US-Übermittlungen zusätzlich auf Standardvertragsklauseln gestützt. **(5) Zugriffsort statt nur Speicherort.** Support-, Wartungs- und Administrationszugriffe auf produktive personenbezogene oder mandats- beziehungsweise patientenbezogene Daten erfolgen nicht aus Staaten außerhalb des EWR. Löst ein freigegebener Modell- oder Infrastrukturprovider konzernbedingt oder über Unterauftragnehmer eine Drittlandübermittlung aus, ist sie nur auf Grundlage eines Angemessenheitsbeschlusses, von Standardvertragsklauseln oder eines anderen zulässigen Transfermechanismus sowie dokumentierter zusätzlicher Maßnahmen zulässig. **(6) Werkzeuge, Websuche und Grounding.** Websuche, Grounding, externe Werkzeuge und Modelle mit abweichenden Aufbewahrungs-, Trainings- oder Speicherbedingungen erhalten keine Originalinhalte, keine personenbezogenen oder pseudonymisierten Daten und keine fremden Geheimnisse. Zulässig ist ihre Nutzung nur innerhalb eines ausdrücklich freigegebenen vertraulichen Pfads oder mit einem nach Anlage 5 erzeugten, tatsächlich anonymen und geheimnisfreien Analysepaket. **(7) Datensparsamkeit als Transferminimierung.**

§ 12 Logging, Monitoring, Umgebungstrennung

(1) Im Produktivbetrieb werden **keine** Inhalte von Anfragen, Antworten, Eingaben oder Dokumenten geloggt; erfasst werden nur technische Metadaten. **(2)** Debug-Logging ist im Produktivbetrieb deaktiviert; Inhaltsdaten erscheinen nicht in Fehlerausgaben. **(3)** Die Logging-Einstellungen werden im Freigabeprozess jeder Änderung geprüft. **(4)** Server-Logfiles der Auslieferung werden höchstens 72 Stunden vorgehalten und nicht mit anderen Daten zusammengeführt. **(5)** Getrennte Umgebungen für Entwicklung, Test und Produktion; in Entwicklung und Test werden ausschließlich synthetische oder anonymisierte Daten verwendet. [VON LEGAL/OPS ZU ERGÄNZEN: Bestätigung je Kundenumgebung] **(6)** Rollenbasierte Zugriffskontrolle; der Produktivzugriff ist beschränkt, Ausnahmen im Supportfall laufen über ein dokumentiertes Verfahren mit Vorab-Freigabe. Der zulässige Personenkreis und der Zugriffsort ergeben sich aus § 7 Absatz 4: ausschließlich ausdrücklich autorisierte Personen mit physischem Zugriffsort in Deutschland oder im EWR. Ein Zugriff aus einem Drittland ist nicht vorgesehen; er wäre nur nach vorheriger Vereinbarung in Textform und mit dokumentierter Ausnahmebegründung zulässig.

§ 13 Löschung, Rückgabe, Speicherdauer (Art. 28 Abs. 3 lit. g DSGVO)

(1) Nach Auftragsende Löschung **oder** Rückgabe nach Wahl des Verantwortlichen sowie Löschung der Kopien, außer bei gesetzlicher Speicherpflicht. **(2) Fristen im laufenden Betrieb:** a) *Variante A:* Entwurfsinhalte und Eingaben werden 72 Stunden nach Zustellung automatisch genullt, spätestens nach 14 Tagen; nicht zustellbare Vorgänge werden nach 14 Tagen vollständig gelöscht; der Arbeitsstand im Konto besteht, solange das Konto besteht, oder bis zum Löschverlangen [VON LEGAL/OPS ZU ERGÄNZEN: Inaktivitätsfrist]. b) *Variante B:* Server-Logfiles höchstens 72 Stunden (§ 12 Abs. 4); Formularinhalte verbleiben nach der Zustellung im Postfach des Verantwortlichen und unterliegen dessen Löschkonzept; von Gosign betriebene Zwischenspeicher werden nach der Zustellung geleert [VON LEGAL/OPS ZU ERGÄNZEN: je Kundenumgebung die Frist der Zwischenspeicher bestätigen]. **(3) Art. 11 Abs. 2 DSGVO:** Nach der Nullung ist eine Zuordnung nicht mehr möglich; Auskunft und Löschung sind mangels Identifizierbarkeit dann nicht mehr erfüllbar. **(4) Sicherungskopien** werden im Zyklus überschrieben; gelöschte Daten werden nicht in den Produktivbestand zurückgeführt. [VON LEGAL/OPS ZU ERGÄNZEN: Aufbewahrungsdauer der Sicherungen] **(5)** Nachweis auf Verlangen.

§ 14 Unterstützung bei Betroffenenrechten (Art. 28 Abs. 3 lit. e DSGVO)

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte nachzukommen, insbesondere bei Anträgen nach Art. 12-23 DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch). (2) Wendet sich eine betroffene Person unmittelbar an Gosign, wird der Antrag unverzüglich an den Verantwortlichen weitergeleitet; eine eigene Beantwortung erfolgt nicht ohne Weisung. (3) Aufwand, der über Selbstbedienungs- und Exportfunktionen hinausgeht, wird gegebenenfalls nach den AGB vergütet.

§ 15 Unterstützung Sicherheit, Meldepflichten, DSFA (Art. 28 Abs. 3 lit. f, Art. 32-36 DSGVO)

(1) Unterstützung bei den Pflichten aus Art. 32-36 DSGVO. (2) **Meldung von Verletzungen des Schutzes personenbezogener Daten** an den Verantwortlichen **unverzüglich, spätestens 24 Stunden nach Kenntnis**, mit den nach Art. 33 Abs. 3 DSGVO verfügbaren Angaben; das entspricht § 9 der AGB und ermöglicht dem Verantwortlichen die Einhaltung seiner 72-Stunden-Frist. (3) Sofortmaßnahmen zur Eindämmung; die Meldung an die Aufsichtsbehörde und die Benachrichtigung Betroffener bleiben Sache des Verantwortlichen. (4) Informationen für eine Datenschutz-Folgenabschätzung auf Anfrage.

§ 16 Nachweise, Kontrollen, Audits (Art. 28 Abs. 3 lit. h DSGVO)

(1) Gosign stellt die zum Nachweis erforderlichen Informationen zur Verfügung. (2) Überprüfungen und Inspektionen werden ermöglicht und unterstützt, vorrangig durch: a) Testate, Zertifikate und Prüfberichte, soweit vorhanden; b) die dokumentierten Maßnahmen nach Anlage 2 nebst Konfigurationsnachweisen und geschwärzten Protokollauszügen; c) einen schriftlichen Audit-Fragebogen. (3) **Zertifizierungsstand:** Gosign führt derzeit weder ein Zertifikat nach ISO/IEC 27001 noch nach BSI-Grundschutz, TISAX oder SOC 2. Die Maßnahmen nach Anlage 2 orientieren sich an diesen Standards, ohne dass daraus eine Zertifizierung abgeleitet werden kann; „vorbereitet“ ist keine Zertifizierung. (4) **Vor-Ort-Prüfung** nach Vorankündigung von mindestens 14 Kalendertagen, zu Geschäftszeiten, höchstens einmal jährlich zuzüglich anlassbezogener Prüfungen, unter Wahrung der Vertraulichkeit (Mandats- und Geschäftsgeheimnisse), gegebenenfalls durch einen verschwiegenheitsverpflichteten Dritten. (5) Penetrationstests nach § 9 der AGB. (6) Hinweis auf Weisungsverstöße nach § 6 Abs. 4. (7) Aufwand, der über die Standardnachweise hinausgeht, wird gegebenenfalls nach den AGB vergütet.

§ 17 Pflichten des Verantwortlichen

(1) Allein verantwortlich für Rechtmäßigkeit und Zulässigkeit der Verarbeitung (Art. 5, 6, gegebenenfalls 9 DSGVO). (2) In Variante A: Beachtung des Hinweises, **keine echten Beschäftigtendaten** einzugeben. (3) Erfüllung der eigenen Informations-, Melde- und Dokumentationspflichten (Art. 13/14, 30, 33/34, 35 DSGVO); gegebenenfalls Einbindung der Arbeitnehmervertretung (§ 87 Abs. 1 Nr. 6 BetrVG, Art. 88 DSGVO). (4) Benennung weisungsberechtigter Ansprechpartner (Anlage 3) sowie Freistellung Gosigns von Ansprüchen Dritter aus rechtswidriger Datenüberlassung oder Weisung nach Maßgabe der Gesetze und der AGB.

§ 18 Haftung

(1) Im Außenverhältnis gilt Art. 82 DSGVO. (2) Im Innenverhältnis gilt § 11 der AGB, soweit mit zwingendem Datenschutzrecht vereinbar; die Haftung für Sub-Auftragsverarbeiter richtet sich nach § 9 Abs. 4 dieses Vertrags (Art. 28 Abs. 4 DSGVO). (3) Keine Beschränkung gegenüber betroffenen Personen (Art. 82 DSGVO) sowie bei Vorsatz, grober Fahrlässigkeit oder der Verletzung von Leben, Körper und Gesundheit.

§ 19 Beginn, Laufzeit, Beendigung

(1) Der Vertrag kommt mit der Bestätigung von Firma, Handlungsbefugnis und Vertragsversion vor der ersten Verarbeitung personenbezogener Daten zustande; Zeitpunkt und Version werden dokumentiert. (2) Die Laufzeit entspricht der Dauer der zugrunde liegenden Leistungsbeziehung und endet automatisch mit ihr. (3) **Nachwirkung:** §§ 7 und 13 sowie die Mitwirkung beim Nachweis. (4)

Versionierung: Anpassung bei geänderten Anforderungen; Information und gegebenenfalls erneute Akzeptanz; Versionskennzeichen vN-JJJJ-MM.

§ 20 Schlussbestimmungen

(1) Änderungen bedürfen mindestens der Textform, auch die Änderung dieser Klausel; Individualvereinbarungen gehen vor. **(2)** Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts; zwingendes Datenschutzrecht bleibt unberührt. **(3)** Gerichtsstand ist Hamburg, soweit zulässig und soweit der Verantwortliche Kaufmann oder juristische Person des öffentlichen Rechts ist. **(4)** Maßgeblich ist die deutsche Fassung. **(5)** Salvatorische Klausel. **(6)** Die Anlagen 1 bis 7 sind Bestandteil dieses Vertrags; das Anbieter- und Modellregister ist Anlage 5.

(7) Keine Rechte an Software und Arbeitsergebnissen. Dieser Vertrag begründet und verändert keine Eigentums-, Lizenz-, Quellcodezugangs-, Herausgabe- oder Nutzungsrechte an Software, Quellcode, Prompts, Regelwerken, Konfigurationen, Dokumentationen oder sonstigen Arbeitsergebnissen. Diese Rechte richten sich ausschließlich nach den vereinbarten Leistungs- und Servicebedingungen sowie den einbezogenen AGB der Gosign GmbH.

Anlage 1 - Beschreibung der Verarbeitung

Variante A - KI-Leistungen

Merkmal	Festlegung
Gegenstand	Verarbeitung personenbezogener Daten zur Bereitstellung von BV-Konto und BV-KI-Drafter
Art	Erheben, Speichern, Übermitteln an den Modell-Provider, Zustellen, Löschen und Nullen (§ 3)
Zweck	Speicherung des Arbeitsstands; Entwurfserzeugung und Zustellung; Missbrauchsbegrenzung
Dauer	Dauer der Nutzung; Löschmechanik nach § 13 (72 Stunden, längstens 14 Tage)
Betroffene	Beschäftigte und Bewerber, Arbeitnehmervertreter, gegebenenfalls Mandanten und Dritte, Nutzer (§ 4)
Datenkategorien	Stamm-, Kontakt- und Metadaten; Eingabeinhalte, Modellantworten, gegebenenfalls Dokumente und Vektordaten (§ 5)
Art. 9 DSGVO	Nicht vorgesehen; möglich durch Freitexteingabe (§ 5 Abs. 2)

Variante B - Website-Betrieb

Merkmal	Festlegung
Gegenstand	Verarbeitung personenbezogener Daten beim Hosting und Betrieb des Webauftritts
Art	Erheben, Speichern, Auslesen, Weiterleiten zur Zustellung, Löschen (§ 3)
Zweck	Auslieferung des Webauftritts; Zustellung der Formulareingänge; Mail-Betrieb; Betriebsprotokolle; Pflege des redaktionellen Systems
Dauer	Dauer des Betriebsauftrags; Logfiles höchstens 72 Stunden (§ 13 Abs. 2 lit. b)
Betroffene	Besucher, Formularabsender, Korrespondenzpartner, Redakteure des Verantwortlichen (§ 4)
Datenkategorien	Formularinhalte, Kommunikationsinhalte der Zustellung, Verbindungs- und Protokolldaten, Zugangsdaten der Redaktion, redaktionelle Inhaltsdaten (§ 5)
Art. 9 DSGVO	Nicht vorgesehen; möglich durch Freitextfelder eines Formulars (§ 5 Abs. 2)

Anlage 2 - Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Jede Maßnahme trägt einen Status. Eine Aufzählung ohne Status liest sich, als sei alles davon in Betrieb — und der Verantwortliche stützt auf diese Anlage seine Auswahlentscheidung nach Art. 28 Abs. 1 DSGVO und seine Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.

Bedeutung der Status: *Umgesetzt* — technisch oder organisatorisch belegt. *Umgesetzt mit benannter Einschränkung* — in Betrieb, mit der in der Zeile genannten Grenze. *Leistung des Infrastruktur-Anbieters* — wird nicht von Gosign erbracht, sondern vom eingesetzten Anbieter; Nachweis über dessen Auftragsverarbeitungsvertrag und Testate. *Je Kundenumgebung zu bestätigen* — hängt vom konkreten Kundensystem ab und wird dort abgenommen. *Offen* — vereinbart, aber noch nicht nachgewiesen.

Für beide Varianten:

Kontrollbereich	Maßnahme	Status
Zutritt und Rechenzentrum	Physische Sicherung, Zutrittskontrolle und Umgebungsschutz der Rechenzentren	Leistung des Infrastruktur-Anbieters
Transportverschlüsselung	TLS 1.2/1.3 für alle Verbindungen, erzwungene Weiterleitung von HTTP auf HTTPS, HSTS	Umgesetzt
Zugriff nach Bedarf	Rollenbasierte Rechte, Need-to-know, getrennte Umgebungen für Entwicklung und Produktion	Umgesetzt
Mandantentrennung	Zeilenschutz mit Standard-Verweigerung auf den Tabellen mit Kundendaten; die LesePfade verlangen die Mandanten-Kennung als Pflichtangabe und haben kein Gegenstück ohne sie	Umgesetzt
Quellcode und Auslieferung	Selbst gehostetes GitLab, geschützte Branches, Änderungen am Produktivstand ausschließlich über Merge Request mit automatisierten Prüfungen	Umgesetzt
Zugangsdaten	Secrets liegen ausserhalb des Quellcodes in der Laufzeitumgebung; ein automatischer Scan blockiert Commits mit Zugangsdaten vor dem Push	Umgesetzt
Protokollierung ohne Inhalte	Betriebsprotokolle enthalten technische Metadaten, keine Formular-, Nachrichten- oder Dokumentinhalte	Umgesetzt
Aufbewahrung der Auslieferungsprotokolle	Server-Logfiles der Auslieferung höchstens 72 Stunden, keine Zusammenführung mit anderen Daten	Umgesetzt
Datensparsamkeit und Privacy by Design	Cookielose Auslieferung ohne Dritt-Tracker; kurze Löschrufen; keine Speicherung der Roh-IP	Umgesetzt
Prüfung bei jeder Freigabe	Protokollierungs- und Datenschutzeinstellungen werden bei jeder Änderung automatisiert geprüft, bevor sie produktiv wird	Umgesetzt
Zugriffsort	Verarbeitung und administrativer Zugriff auf Produktivdaten ausschließlich aus Deutschland oder dem EWR Verbindlich geregelt in § 7 Absatz 4; der Nachweis erfolgt über die Verpflichtungs- und Belehrungserklärungen sowie die Zugriffsprotokolle.	Offen
Sicherung und Wiederherstellung	Sicherungszyklus, Aufbewahrungsdauer und ein dokumentierter Wiederherstellungstest [VON LEGAL/OPS ZU ERGÄNZEN: Zyklus, Aufbewahrung, Datum des letzten Wiederherstellungstests]	Offen
Turnusmäßige Auftragskontrolle	Regelmäßige Kontrolle der Sub-Auftragsverarbeiter mit dokumentiertem Ergebnis [VON LEGAL/OPS ZU ERGÄNZEN: Turnus und letzte Kontrolle]	Offen

Variante A - KI-Leistungen

Kontrollbereich	Maßnahme	Status
Nullung der Inhalte	Eingaben und Entwurfsinhalte werden 72 Stunden nach Zustellung automatisch genullt, spätestens nach 14 Tagen; die Zeile bleibt als inhaltsfreie Audit-Spur bestehen	Umgesetzt
Missbrauchsbegrenzung	Die dafür erhobene E-Mail-Adresse wird verschlüsselt gespeichert	Umgesetzt
Keine Nutzung zum Training	Vertraglicher Ausschluss der Nutzung zu Trainings-, Fine-Tuning- oder Modellverbesserungszwecken, mit Weitergabe der Beschränkung an den Modell-Provider	Umgesetzt mit benannter Einschränkung
Retention beim Modell-Provider	Zero- beziehungsweise No-Retention ist projekt- und modellbezogen nachzuweisen; sie ersetzt weder die Prüfung des Auftragsverarbeitungsvertrags noch die berufsrechtliche Bewertung. Der Status je Anbieter steht in Anlage 4; besteht eine anbieterseitige Missbrauchs- oder Sicherheitsüberwachung ohne genehmigte Ausnahme, gilt der Pfad nicht als Zero Retention [VON LEGAL/OPS ZU ERGÄNZEN: Status je Ressource dieser Kundenumgebung bestätigen]	Je Kundenumgebung zu bestätigen
Schlüsselverwaltung und Speicherregion	Speicherregion der persistenten Bestände: Deutschland, je Anbieter und Dienst in Anlage 4 ausgewiesen. [VON LEGAL/OPS ZU ERGÄNZEN: eingesetzte Verschlüsselungsverfahren und Schlüsselverwaltung je Umgebung]	Offen

Variante B - Website-Betrieb

Kontrollbereich	Maßnahme	Status
Zustellung der Formulare	Eingänge werden beim Routing-Dienst ohne Zwischenspeicherung verarbeitet und über eine verschlüsselte Verbindung an das benannte Postfach übergeben	Umgesetzt
Ablage der Meldungen	Selbst betriebene Datenbank in der EU; Zeilenschutz mit Standard-Verweigerung, kein Lesezugriff mit einem öffentlichen Schlüssel	Umgesetzt
Zugänge zum redaktionellen System	Personengebundene Konten mit Zwei-Faktor-Authentisierung, soweit das eingesetzte System sie unterstützt	Je Kundenumgebung zu bestätigen
Aktualisierung des redaktionellen Systems	Aktualisierungen des Systems und seiner Erweiterungen nach dokumentiertem Wartungsplan	Je Kundenumgebung zu bestätigen

Anlage 3 - Ansprechpartner

Rolle	Verantwortlicher	Gosign
Weisungsberechtigt / Datenschutz	[ANGABE FEHLT: Weisungsberechtigte Person], [ANGABE FEHLT: Erreichbarkeit der weisungsberechtigten Person]	datenschutz@gosign.de
Technisch	[ANGABE FEHLT: Technischer Ansprechpartner des Verantwortlichen]	datenschutz@gosign.de (Weiterleitung an den technischen Betrieb)
Datenschutzbeauftragter	[ANGABE FEHLT: Datenschutzbeauftragter des Verantwortlichen]	Nicht bestellt (§ 38 Abs. 1 BDSG); datenschutz@gosign.de

Anlage 4 - Genehmigte Sub-Auftragsverarbeiter

Diese Anlage wird aus dem **Anbieter-Register** erzeugt (docs/vertragsvorlagen/anbieter-register.md). Sie ist keine zweite Liste: Wer einen Verarbeitungsort ändert, ändert ihn im Register, und diese Anlage folgt. Eine von Hand gepflegte Kopie wäre spätestens beim ersten Wechsel der ältere von zwei Ständen.

Variante A — KI-Leistungen

#	Sub-AV	Zweck	Ort	Datenklasse	Aufbewahrung	Transfer-Mechanismus	Freigabe seit
1	OpenRouter, Inc.	Vermittlung der Modellanfrage zur Entwurfserzeugung	USA [ZU ERGÄNZEN: EU-Endpunkt prüfen]	P	keine Aufbewahrung über die Anfrage hinaus [ZU ERGÄNZEN: projekt- und modellbezogen bestätigen]	Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)	2026-08-20

Variante B — Website-Betrieb

#	Sub-AV	Zweck	Ort	Datenklasse	Aufbewahrung	Transfer-Mechanismus	Freigabe seit
1	Cloudflare, Inc.	Auslieferung und Routing des Webauftritts, Zwischenverarbeitung der Formulareingänge ohne Persistenz, Schlüssel-Wert-Speicher für Abonnements	EU/global [ZU ERGÄNZEN: Region des Schlüssel-Wert-Speichers]	P	Server-Logfiles höchstens 72 Stunden	Data Privacy Framework, soweit zertifiziert, und/oder Standardvertragsklauseln	2026-08-20
2	Google [ZU ERGÄNZEN: Firmierung und Anschrift der Vertragspartei des Workspace-Vertrags]	Mail-Betrieb über Google Workspace in EU-Konfiguration	EU (IE)	V	nach dem Löschkonzept des Verantwortlichen	Auftragsverarbeitungsvertrag; bei Zugriff aus den USA Data Privacy Framework und/oder Standardvertragsklauseln	2026-08-20
3	Brevo [ZU ERGÄNZEN: Firmierung und Anschrift der Vertragspartei]	Versand angeforderter Inhalte (Report- und Newsletter-Zustellung)	EU [ZU ERGÄNZEN: Verarbeitungsstandort]	P	bis zum Widerruf des Abonnements	Auftragsverarbeitungsvertrag [ZU ERGÄNZEN: Transfermechanismus bestätigen]	2026-08-20
4	Serverbetreiber der selbst betriebenen Datenbank [ZU ERGÄNZEN: Firmierung]	Speicherung der über Formulare eingegangenen Meldungen	EU [ZU ERGÄNZEN: Standort]	V	nach den Fristen in § 13 des Vertrags	[ZU ERGÄNZEN]	2026-08-20

Abgrenzung (§ 9 Abs. 5): Im Standardbetrieb werden alle genannten Anbieter als Sub-Auftragsverarbeiter von Gosign geführt. Eigene Anbieterverträge des Verantwortlichen bleiben nach § 2 Abs. 3a außerhalb dieser Kette.

Anlage 5 - Modellklassen, Routingregeln und Modellregister

Diese Anlage legt fest, welche Inhalte an welche Art von Modell gelangen dürfen. Sie gilt unabhängig davon, welches Modell gerade eingesetzt wird; die konkreten Modelle führt das Provider- und Modellregister.

1. Datenklassen

Klasse	Inhalt	Zulässiger Pfad
V	Originale personenbezogene Daten, Mandatsinformationen, fremde Geheimnisse sowie Originalanhänge	Nur ein schriftlich freigegebener vertraulicher Verarbeitungspfad
P	Pseudonymisierte oder minimierte Inhalte; sie bleiben personenbezogen und möglicherweise geheimnisbehaftet	Nur ein freigegebener Verarbeitungspfad; die Pseudonymisierung ersetzt die Freigabe nicht
A	Tatsächlich anonyme, synthetische, öffentliche und geheimnisfreie Inhalte	Anbieterneutral, sofern der Anbieter im Register geführt ist
G	Nicht sicher einzuordnende, unzulässige oder nicht ausreichend bereinigte Inhalte	Keine Übermittlung an einen Anbieter

Im Zweifel wird gesperrt. Lässt sich der Schutzbedarf eines Inhalts nicht sicher feststellen, gilt Klasse G. Die Unsicherheit führt nicht zur nächstniedrigen Klasse, sondern zur Verweigerung — sonst trüge das Risiko derjenige, der es am wenigsten überblickt.

Erzeugung statt Filterung. Soll ein Inhalt an einen Pfad geringerer Schutzstufe, wird dafür ein eigenes, minimiertes Paket **erzeugt** — statt ein Original zu filtern und weiterzureichen. Die Prüfung beantwortet damit nicht die Frage „darf das Original hinaus“, sondern „konnte ein regelkonformes Paket entstehen“. Ein Fehler in der Prüfung führt deshalb zur rein menschlichen Bearbeitung des Vorgangs, nicht zu einer Weitergabe.

Grenzen der automatischen Prüfung. Eine automatisierte Erkennung kann Mandatsbezug und indirekte Identifizierbarkeit nicht mit Sicherheit ausschließen; Gosign sagt eine vollständige Erkennung nicht zu. Die Vermeidung an der Quelle bleibt die tragende Kontrolle — der Verantwortliche weist seine Mitarbeitenden an, nicht erforderliche vertrauliche Inhalte gar nicht erst einzubringen. Die technische Prüfung ist das Auffangnetz dahinter, nicht ihr Ersatz.

Zero-Retention und EU-Region sind notwendige, aber nicht hinreichende Kriterien. Sie ersetzen weder die Prüfung des Auftragsverarbeitungsvertrags noch die berufsrechtliche Bewertung eines Pfades.

2. Durchsetzung

Die Zuordnung von Datenklasse, Provider, Modell, Region, Aufbewahrung, Werkzeugfreigaben und Regelwerksversion wird serverseitig erzwungen, nicht im Endgerät oder in der Oberfläche. Zugangsdaten der Provider verbleiben serverseitig. Inhaltsdaten werden nicht in technischen Vermittlungsprotokollen gespeichert.

3. Modellregister

Das Register ist Bestandteil dieses Vertrags und wird dem Verantwortlichen auf Anforderung in der jeweils geltenden Fassung übergeben. Aus ihm entsteht Anlage 4; eine zweite, von Hand gepflegte Liste im Vertragstext gibt es bewusst nicht.

Das Register führt je Eintrag: Anbieter, Zweck, Verarbeitungsort, zulässige Datenklasse, Aufbewahrung, Transfermechanismus und Freigabedatum, dazu ein Änderungsprotokoll mit Datum, altem und neuem Stand.

Ein Eintrag ist nicht freigabefähig, solange eine Pflichtangabe offen ist. Das ist keine Formalie: Ohne diese Angaben kann der Verantwortliche sein Widerspruchsrecht nach Art. 28 Abs. 2 DSGVO nicht ausüben, weil ihm die Grundlage für die Beurteilung fehlt. Ein Modellwechsel innerhalb eines freigegebenen Providers wird dort dokumentiert und bedarf keiner Vertragsänderung, solange die in § 9 Absatz 6 genannten Merkmale unverändert bleiben.

Anlage 6 - Verfahren der Modellfreigabe

1. Vor der Aktivierung

Jeder Provider- und Modellpfad durchläuft vor der produktiven Aktivierung eine dokumentierte Prüfung. Geprüft und schriftlich festgehalten werden:

- Vertragsrolle des Providers und vorliegende Vertragsinstrumente - Erbringungsort der Leistung, nicht nur der Speicherort der Daten - Aufbewahrung, insbesondere ob eine Zero- oder No-Retention-Konfiguration projekt- und modellbezogen bestätigt ist - Ausschluss der Nutzung zu Training oder Modellverbesserung - Mögliche Zugriffe des Providers auf Inhalte, einschließlich einer Missbrauchs- oder Sicherheitsüberwachung - Unterauftragnehmer des Providers und deren Standorte - Transfermechanismus und ergänzende Maßnahmen bei Drittlandbezug - Berufsrechtliche Bewertung, soweit der Verantwortliche einer Verschwiegenheitspflicht unterliegt

2. Freigabe und Inbetriebnahme

Die Aktivierung erfolgt erst nach schriftlicher Freigabe des Verantwortlichen. Zur Inbetriebnahme wird ein Protokoll geführt, das die technischen Nachweise zum Zeitpunkt der Aktivierung festhält. Eine spätere Aktivierung vertraglich bereits geregelter Funktionen erfordert keinen neuen Vertrag, sofern die Umsetzung diesen Regelungen entspricht und das Protokoll vorliegt.

3. Entzug

Ergeben sich Anhaltspunkte, dass ein Provider die vereinbarten Bedingungen nicht mehr erfüllt, wird der Pfad ausgesetzt und der Verantwortliche in Textform unterrichtet. Die Wiederaufnahme setzt eine erneute Prüfung und Freigabe voraus.

Anlage 7 - Löschung, Sicherung und Aufbewahrung im Support

1. Grundsatz: Arbeitsbereich, kein führendes Archiv

Die KI-Umgebung ist Arbeits- und Assistenzsystem. Ergebnisse, Entscheidungsgrundlagen und Nachweise, die für die Akte oder die gesetzliche Dokumentation erforderlich sind, übernimmt der Verantwortliche in sein führendes System. Der Gesprächsverlauf in der KI-Umgebung wird nicht pauschal als aufbewahrungspflichtiges Archiv behandelt.

2. Löschung durch den Nutzer

Die Löschkette umfasst Datenbankeintrag, Einbettungs- beziehungsweise Vektorrepräsentation und das physische Dateiobjekt. [VON LEGAL/OPS ZU ERGÄNZEN: Datum des dokumentierten Ende-zu-Ende-Löschtests für diese Umgebung]

3. Ende des Mandats oder der Behandlung

Das Ende führt nicht automatisch zur Sofortlöschung. Der Verantwortliche prüft, ob Inhalte noch für die Bearbeitung, die Akte, gesetzliche Aufbewahrung oder Rechtsansprüche erforderlich sind. Aufbewahrungspflichtige Inhalte verbleiben im führenden System; nicht mehr erforderliche Arbeitskopien in der KI-Umgebung werden gelöscht.

4. Widerspruch gegen die KI-Nutzung

Widerspricht eine betroffene Person der KI-Nutzung oder nimmt der Verantwortliche einen Vorgang von der KI-Verarbeitung aus, wird dies als Sperre für die künftige Nutzung gekennzeichnet. Bestehende Arbeitskopien werden geprüft und, soweit nicht aufbewahrungspflichtig, gelöscht.

5. Sicherungen und Support

[VON LEGAL/OPS ZU ERGÄNZEN: Aufbewahrungsdauer der Sicherungen und der Supportinhalte je Umgebung]

Sicherungen folgen der Löschung mit dem Ablauf ihres Zyklus. Supportinhalte werden nicht länger aufbewahrt, als es die Bearbeitung des Vorgangs erfordert.

Offene Punkte

Der Entwurf hält seine Lücken sichtbar. Jede offene Stelle im Text steht hier mit dem nächsten Schritt und der Seite, die ihn geht.

Offene Stelle	Nächster Schritt	Zuständig
bestätigen, ob im Einzelfall eine Messlösung mitbetreut wird - dann als eigene Zweckposition aufnehmen	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
bestätigen, ob Datei-Uploads im Funktionsumfang	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
bestätigen, ob eine Pipeline mit Personenbezug aktiv ist; sonst „nicht einschlägig“	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
Namen und Erreichbarkeiten	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
ob aktiv	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
für diese Kundenumgebung Region und Rechenzentrum je Dienst bestätigen	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
Bestätigung je Kundenumgebung	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
Inaktivitätsfrist	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
je Kundenumgebung die Frist der Zwischenspeicher bestätigen	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
Aufbewahrungsdauer der Sicherungen	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
Zyklus, Aufbewahrung, Datum des letzten Wiederherstellungstests	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
Turnus und letzte Kontrolle	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
Status je Ressource dieser Kundenumgebung bestätigen	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
eingesetzte Verschlüsselungsverfahren und Schlüsselverwaltung je Umgebung	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
EU-Endpunkt prüfen	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher
projekt- und modellbezogen bestätigen	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher
Region des Schlüssel-Wert-Speichers	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher
Firmierung und Anschrift der Vertragspartei des Workspace-Vertrags	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher
Firmierung und Anschrift der Vertragspartei	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher
Verarbeitungsstandort	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher
Transfermechanismus bestätigen	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher
Firmierung	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher
Standort	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher

Offene Stelle	Nächster Schritt	Zuständig
ohne nähere Bezeichnung	Beim Vertragsschluss erfragen und in die Fassung des Kunden eintragen	Verantwortlicher
Datum des dokumentierten Ende-zu-Ende-Löschtests für diese Umgebung	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)
Aufbewahrungsdauer der Sicherungen und der Supportinhalte je Umgebung	Angabe durch Legal/Ops verifizieren und vor der Freigabe eintragen	Gosign (Legal/Ops)

Unterzeichnung

Der Vertrag kommt mit der Zeichnung durch beide Parteien zustande und gilt ab dem Datum der zuletzt geleisteten Unterschrift. Solange der Vermerk auf jeder Seite die ausstehende anwaltliche Freigabe nennt, ist dieser Text **nicht zur Zeichnung bestimmt**.

Verantwortlicher	Auftragsverarbeiter
[ANGABE FEHLT: Firma des Verantwortlichen]	Gosign GmbH, Hallerstraße 8, 20146 Hamburg
Ort, Datum:	Ort, Datum:
Unterschrift:	Unterschrift:
[ANGABE FEHLT: Vertretungsberechtigte Person], [ANGABE FEHLT: Funktion der vertretungsberechtigten Person]	Bert Gogolin, Geschäftsführer, oder Dieter Gogolin, Geschäftsführer

ENTWURF - noch nicht abschließend; einzelne Stellen sind zu ergänzen. Vor der Freigabe werden alle mit ERGÄNZEN gekennzeichneten Stellen gefüllt, die Anlagen 1 bis 4 bestätigt und der Stand des Angemessenheitsbeschlusses (C-703/25 P) geprüft. Stand: **v1-2026-08**.

Änderungsprotokoll

Diese Fassung entstand aus dem internen Arbeitsentwurf gosign-avv-entwurf-v2-2026-06, der ausschließlich die KI-Leistungen beschrieb. Geändert wurde:

Änderung	Grund	Beleg
Zweite Leistungsvariante „Website-Betrieb“ in §§ 3, 4, 5 sowie den Anlagen 1, 2 und 4 ergänzt	Der Vertrag beschrieb eine Verarbeitung, die für Website- und Betriebskunden nicht stattfindet	Datenschutzerklärung der Gosign GmbH, Abschnitte zu Hosting, Formularen, Mail-Betrieb und Protokolldaten
Anlage 4 nach Varianten getrennt; die Variante A verweist auf die Subprozessorenliste des 203-Vertragskits, statt sie zu wiederholen	Zwei Listen für dieselbe Leistung driften auseinander; der Verantwortliche stützt darauf sein Widerspruchsrecht nach Art. 28 Abs. 2 DSGVO	subprozessoren.md des 203-Vertragskits
§ 16 Abs. 3 neu: ausdrückliche Nicht-Zusage zu ISO/IEC 27001, BSI-Grundschutz, TISAX und SOC 2	Der Vorentwurf ließ die Zertifizierungsfrage offen; eine offene Stelle in einem Vertrag wird im Zweifel zugunsten des Lesers ausgelegt	Es liegt keine Zertifizierungsurkunde vor; die Aussage ist eine Nicht-Zusage, keine Zusicherung
§ 2 Abs. 4 um den Vorrang dieses Vertrags vor den AGB in datenschutzrechtlichen Fragen ergänzt	AGB § 13 und dieser Vertrag regeln denselben Gegenstand	AGB der Gosign GmbH, § 13

Keine Vermutung ersetzt eine Angabe. Offene Stellen sind als solche stehengeblieben und mit dem Vermerk ERGÄNZEN gekennzeichnet; gefüllt wurde ausschließlich, was aus den oben genannten Belegen hervorgeht.

Quellen

- Art. 28 DSGVO (dsgvo-gesetz.de, dejure.org) - AVV-Muster zu Art. 28 Abs. 3 DSGVO (LfDI Baden-Württemberg) - EU-US Data Privacy Framework, Stand 2026; T-553/23 (Latombe) abgewiesen am 03.09.2025; C-703/25 P anhängig - AGB der Gosign GmbH § 13 (Auftragsverarbeitung), § 9 (Sicherheit), § 6.6 (kein Training) - Datenschutzerklärung der Gosign GmbH (Auftragsverarbeiter, Speicherfristen)