Auftragsverarbeitungsvertrag für den Zugang zum Gosign privacyRouter

Anlage 2 zum Rahmenwerk über den Zugang · Stand 08.11.2026

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 DSGVO. Er ist Anlage 2 des Rahmenwerks über den Zugang zum Gosign privacyRouter und gilt zusammen mit der Zusatzvereinbarung zur Verschwiegenheit nach § 203 Abs. 4 StGB für den Zugang zum Gosign privacyRouter (Anlage 3 des Rahmenwerks), die zugleich der Vertrag nach dem Berufsrecht der Kanzlei ist (für Rechtsanwälte § 43e Abs. 3 BRAO, für Patentanwälte § 39c Abs. 3 PAO, für Steuerberater und Steuerbevollmächtigte § 62a Abs. 3 StBerG, für Wirtschaftsprüfer § 50a Abs. 3 WPO, für Notare § 26a Abs. 3 BNotO), und mit der Liste der Unterauftragnehmer (Anlage 2 dieses Vertrags). Router, Portal, Konto, Guardrails und Schlüssel bezeichnen dasselbe wie im Rahmenwerk und in der Leistungsbeschreibung.

§ 1 Parteien

Verantwortlicher: die Kanzlei, die mit Gosign das Rahmenwerk über den Zugang zum Gosign privacyRouter schließt, nachfolgend „Kanzlei“.

Auftragsverarbeiter: Gosign GmbH, Hallerstraße 8, 20146 Hamburg, Amtsgericht Hamburg HRB 112197, vertreten durch die Geschäftsführer Bert Gogolin und Dieter Gogolin, nachfolgend „Gosign“. Kontakt in Datenschutzfragen: datenschutz@gosign.de.

Betreibt ein Dienstleister der Kanzlei die Anwendung, die den Zugang nutzt, bleibt er Dienstleister der Kanzlei mit eigenem Vertrag. Partei dieses Vertrags wird er nicht. Dasselbe gilt für den Anbieter einer Telefonleitung, über die Gespräche eine Anwendung der Kanzlei erreichen.

§ 2 Gegenstand und Dauer

(1) Gosign stellt der Kanzlei einen Zugang zum Router bereit, einer Programmierschnittstelle im Format von OpenAI und im Format der Anthropic Messages API, dazu einer Echtzeitschnittstelle für Sprachdialoge. Über den Zugang richtet die Anwendung der Kanzlei Anfragen an Sprachmodelle und erhält deren Antworten. Gosign leitet jede Anfrage über die in Anlage 2 genannten Unterauftragnehmer an das gewählte Modell weiter und gibt die Antwort zurück.

(2) Der Vertrag gilt, solange das Rahmenwerk besteht, und endet mit ihm.

§ 3 Art und Zweck der Verarbeitung

(1) **Art:** Entgegennehmen, Weiterleiten und Zurückgeben von Anfragen und Antworten; in der Variante mit Zwischenspeicher (§ 10 Abs. 6) Ablegen der Anfragen im Zwischenspeicher bei Google; Erfassen von Verbrauchsdaten; Löschen.

(2) **Zweck:** Bereitstellung des Zugangs zu den Modellen der für die Kanzlei freigegebenen Wege; Abrechnung, Budgets der Guardrails und Höchstbeträge der Schlüssel; Sicherheit des Betriebs; in der Variante mit Zwischenspeicher geringere Kosten und Wartezeit, wenn derselbe Anfang einer Anfrage wiederkehrt.

(3) Inhaltsdaten verarbeitet Gosign nicht zu eigenen Zwecken. Verbrauchsdaten verarbeitet Gosign für Abrechnung und Nachweis zugleich als Verantwortliche (Art. 6 Abs. 1 lit. c und f

DSGVO), ohne dafür die Nutzerkennung heranzuziehen. Vertragsdaten verarbeitet Gosign als Verantwortliche für die Durchführung des Vertrags (Art. 6 Abs. 1 lit. f DSGVO). Weder Gosign noch die Unterauftragnehmer nutzen Inhaltsdaten zum Training oder zur Feinabstimmung von Modellen.

§ 4 Daten und betroffene Personen

(1) **Inhaltsdaten:** Eingaben (Texte, Dokumentauszüge, Bilder und Scans, gesprochene Sprache und Video, Werkzeugdefinitionen und Werkzeugergebnisse) und die Antworten der Modelle einschließlich gesprochener Antworten, Mitschriften, erzeugter Bilder und Einbettungen. Sie können beliebige personenbezogene Daten enthalten, auch besondere Kategorien nach Art. 9 DSGVO, Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO und Geheimnisse im Sinne des § 203 StGB. Gosign verarbeitet sie nur für die Dauer der einzelnen Anfrage und speichert sie nicht.

(2) **Verbrauchsdaten:** Kennung des Zugangs, der Guardrails und des Schlüssels, aufgerufenes Modell, Zeitpunkt, Anzahl der Token und Kosten der Anfrage, dazu eine Nutzerkennung, sofern die Anwendung der Kanzlei sie mitsendet. Verbrauchsdaten enthalten keine Inhalte. Angaben zu Mandaten oder Amtsgeschäften und Namen oder andere Angaben, die eine Person unmittelbar erkennen lassen, setzt die Kanzlei nicht in die Nutzerkennung.

(3) **Vertragsdaten:** Namen und Kontaktdaten der Ansprechpartner der Kanzlei und der Personen, die ihr Konto nutzen.

(4) **Betroffene Personen:** Mandanten oder Beteiligte der Kanzlei und Personen, die in Unterlagen zu Mandaten oder Amtsgeschäften vorkommen; Personen, die mit einer Anwendung der Kanzlei sprechen oder schreiben, etwa Anrufer; Beschäftigte der Kanzlei, die den Zugang nutzen; Ansprechpartner der Kanzlei und Personen, die ihr Konto nutzen. Welche Daten tatsächlich eingegeben werden, bestimmt die Kanzlei.

§ 5 Weisungen

(1) Gosign verarbeitet die Daten nur auf dokumentierte Weisung der Kanzlei, auch hinsichtlich einer Übermittlung in ein Drittland, es sei denn, Gosign ist durch das Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt Gosign der Kanzlei diese Anforderungen vor der Verarbeitung mit, sofern das Recht eine solche Mitteilung nicht verbietet. Dieser Vertrag, die Freigabe der Wege, die Einstellungen im Konto und die Anfragen selbst sind die Weisung, soweit dieser Vertrag nichts anderes bestimmt. Einstellungen im Konto, etwa zu Guardrails, Ausschlüssen, Budgets, Schlüsseln, neuen Modellen und der Variante mit Zwischenspeicher, hält das Konto mit Person und Zeit in der Prüfspur fest.

(2) Hält Gosign eine Weisung für rechtswidrig, informiert Gosign die Kanzlei unverzüglich und darf die Ausführung aussetzen, bis die Kanzlei sie bestätigt oder ändert (Art. 28 Abs. 3 UAbs. 2 DSGVO).

§ 6 Vertraulichkeit und Verschwiegenheit

(1) Gosign verpflichtet alle Personen, die Zugang zu den Daten erhalten können, in Textform zur Vertraulichkeit und zur Verschwiegenheit nach § 203 StGB und belehrt sie über die Strafbarkeit. Die Einzelheiten regelt die Zusatzvereinbarung.

(2) Zugriff auf die Systeme des Routers haben nur ausdrücklich autorisierte Personen mit Zugriffsort in Deutschland oder im EWR.

(3) Der Router speichert keine Inhalte, er verarbeitet sie nur für die Dauer der einzelnen Anfrage. Wer den Router betreibt oder administriert, ist nach Absatz 1 verpflichtet und belehrt. Einen Zugriff von Menschen auf Inhalte sieht der Betrieb des Routers nicht vor.

§ 7 Technische und organisatorische Maßnahmen

Gosign trifft die Maßnahmen nach Art. 32 DSGVO, die Anlage 1 beschreibt. Gosign darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt, und teilt wesentliche Änderungen mit.

§ 8 Unterauftragnehmer

(1) Die Kanzlei genehmigt die Unterauftragnehmer, die Anlage 2 nennt, auf dem Weg über Google mit den Unterauftragnehmern von Google nach Googles Liste, auf die Anlage 2 verweist. Google bezeichnet in diesem Vertrag die Gesellschaft von Google, die Anlage 2 für diesen Weg nennt. Anlage 2 gilt in der Fassung, die bei Wirksamwerden dieses Vertrags gilt, und danach in der nach Absatz 2 fortgeschriebenen Fassung, ohne neue Unterschrift; Gosign hält jede Fassung mit dem Tag ihres Wirksamwerdens im Konto unter Mitteilungen bereit. Weitere und ersetzte Unterauftragnehmer genehmigt die Kanzlei allgemein nach Maßgabe von Absatz 2 (Art. 28 Abs. 2 Satz 1 DSGVO). Jeder ist nach Art. 28 Abs. 4 DSGVO an dieselben Datenschutzpflichten gebunden und nach § 203 StGB zur Verschwiegenheit verpflichtet, mit der Pflicht, eigene Unterauftragnehmer ebenso zu verpflichten. Die Genehmigung gilt je Weg, nicht je Modellname oder Modellversion. Neue Modelle und Versionen, die über dieselben Unterauftragnehmer am selben Ort und mit denselben Zusagen zu Speicherung, Protokollierung, Training und Zugriffsmöglichkeiten verarbeitet werden, sind keine Änderung nach Absatz 2. Dasselbe gilt für die Modelle der Variante mit Zwischenspeicher nach § 10 Abs. 6.

(2) Einen neuen Weg und einen neuen oder ersetzten Unterauftragnehmer kündigt Gosign mindestens 30 Kalendertage vorher in Textform an, per Mail mit der Ankündigung als PDF und im Konto unter Mitteilungen, mit Firmierung, Aufgabe, Ort der Verarbeitung, Grundlage nach § 203 StGB und Zusagen zu Speicherung, Protokollierung und Training der beteiligten Unternehmen, bei einer Verarbeitung außerhalb der EU oder einem Unternehmen eines Konzerns mit Sitz außerhalb der EU auch mit dem Übermittlungsinstrument nach Kapitel V DSGVO. Die Frist beginnt mit dem Zugang dieser Angaben. Kündigt Google einen neuen Unterauftragnehmer an, gibt Gosign die Ankündigung unverzüglich in Textform an die Kanzlei weiter. Einen neuen Weg nutzt die Kanzlei erst, wenn sie ihn im Konto freischaltet. Die Kanzlei kann bis zum Ablauf der Frist, bei Google bis zum angekündigten Einsatz, aus datenschutzrechtlichem oder berufsrechtlichem Grund widersprechen, insbesondere wenn der Schutz der Geheimnisse am Ort der Verarbeitung dem Schutz im Inland nicht vergleichbar ist. Widerspricht sie, gehen Anfragen ihres Zugangs nicht über den neuen Weg oder das neue Unternehmen; ist das nicht möglich, sperrt Gosign den betroffenen Weg für ihren Zugang. Kommt binnen eines Monats nach dem Widerspruch keine Lösung zustande, kann die Kanzlei das Rahmenwerk über den Zugang und diesen Vertrag ganz oder für den betroffenen Weg ohne Einhaltung einer Frist in Textform kündigen. Endet der Zugang ganz, fallen Grundgebühr und Gebühren für weitere Schlüssel für die Kalendermonate nach dem Zugang der Kündigung nicht mehr an; nicht verbrauchtes Guthaben wird nicht erstattet (§ 7 Abs. 4 des Rahmenwerks).

(3) Gosign haftet für die Einhaltung der Pflichten durch die Unterauftragnehmer (Art. 28 Abs. 4 Satz 2 DSGVO).

(4) Ändert ein Unterauftragnehmer Speicherung, Protokollierung, Ort der Verarbeitung, Trainingsnutzung oder Zugriffsmöglichkeiten, sperrt Gosign den betroffenen Weg und informiert

die Kanzlei unverzüglich in Textform. Gelten die Zusagen danach nicht mehr unverändert, gibt Gosign den Weg nur nach Absatz 2 wieder frei, wie einen neuen Weg.

§ 9 Ort der Verarbeitung und Drittländer

(1) Der Router wird in Rechenzentren in Deutschland betrieben. Die Modelle bei Google ruft der Router ausschließlich über Endpunkte von Google in der EU auf, derzeit über die Multiregion eu. Endpunkte außerhalb der EU sind im Router nicht eingerichtet; ein Ausweichen dorthin findet nicht statt. Die Modelle des Wegs in Deutschland ruft der Router bei dem in der Liste der Unterauftragnehmer (Anlage 2) genannten Betreiber auf, der sie auf Servern in einem Rechenzentrum in Deutschland ausführt.

(2) Google gehört einem US-Konzern an. Mögliche Zugriffe nach US-Recht und Übermittlungen an Unterauftragnehmer von Google außerhalb der EU sind deshalb nach Art. 28, 32 und 44 ff. DSGVO zu bewerten, auch wenn der Vertragspartner von Gosign bei Google in der EU sitzt und die Verarbeitung in der EU erfolgt. Übermittlungen an seine Unterauftragnehmer außerhalb der EU stützt Google auf die Übermittlungsinstrumente seines Cloud Data Processing Addendum; die Kanzlei weist Gosign an, diese Übermittlungen zuzulassen. Das gilt auch für Eingaben, Ausgaben und Zwischenspeicher der Variante nach § 10 Abs. 6. Für die Hashwerte der Variante nach § 10 Abs. 6 gilt das nicht; nur sie verarbeitet Google als Verantwortlicher nach der Google Cloud Privacy Notice, die eine Verarbeitung auch außerhalb der EU vorsieht, und stützt Übermittlungen dafür auf eigene Grundlagen. Das tragende Instrument und die ergänzenden Maßnahmen weist der Baustein zum Drittlandtransfer aus. Von einem Herausgabeverlangen einer Behörde eines Drittstaats unterrichtet Gosign die Kanzlei unverzüglich, soweit dies zulässig ist. Ob der Schutz der Geheimnisse in dem Staat, in dem eine Dienstleistung erbracht wird, dem Schutz im Inland vergleichbar ist (§ 43e Abs. 4 BRAO, § 39c Abs. 4 PAO, § 62a Abs. 4 StBerG, § 50a Abs. 4 WPO), prüft die Kanzlei. Gosign stellt ihr dafür die Angaben zur Verfügung, die Google zum Ort der Verarbeitung und zu seinen Unterauftragnehmern macht.

(3) Gosign nimmt Support- und Administrationszugriffe auf den Router nur aus Deutschland oder einem anderen Staat des EWR vor. Für Zugriffe durch Beschäftigte und Unterauftragnehmer von Google gelten dessen Vertragsbedingungen und das Professional Secrecy Addendum (Germany).

(4) Bei Anfragen auf dem Weg über Google ist Google Vertragspartner und für die Inferenz der einzige Unterauftragnehmer. Google gibt Eingaben und Antworten nach seiner Dokumentation auch bei Partnermodellen nicht an Dritte weiter. Anthropic, der Hersteller der Claude-Modelle, erhält danach und nach der schriftlichen Auskunft von Google vom 10.08.2026 keine Inhalte dieser Anfragen und ist deshalb nicht als Unterauftragnehmer aufgeführt, ebenso wenig die Hersteller anderer Modelle bei Google. Modelle und Funktionen, bei denen Google Inhalte über den Arbeitsspeicher hinaus speichert oder an den Hersteller eines Modells weitergibt, schaltet Gosign nicht frei, ausgenommen den Zwischenspeicher der Variante nach § 10 Abs. 6. Bindet Google weitere Personen ein, die Zugang zu Berufsgeheimnissen erhalten können, verpflichtet Google sie nach Ziffer 3 des Professional Secrecy Addendum in Textform zur Verschwiegenheit.

(5) Auf dem Weg in Deutschland werden Inhalte nur in Deutschland verarbeitet. Die Hersteller der offenen Modelle sind nicht beteiligt und erhalten keine Inhalte, und kein Unternehmen auf diesem Weg gehört einem US-Konzern an. Wer auf diesem Weg Kenntnis nehmen kann und mit welcher Urkunde er nach § 203 StGB verpflichtet ist, nennt die Liste der Unterauftragnehmer (Anlage 2).

§ 10 Speicherung, Protokollierung und Löschung

(1) Der Router speichert keine Inhaltsdaten. Seine Protokolle enthalten nur Verbrauchsdaten.

(2) Verbrauchsdaten bewahrt Gosign für Abrechnung und Nachweis bis zum Ablauf von zwölf Monaten nach Ende des Abrechnungsmonats auf und löscht sie danach. Rechnungen unterliegen den gesetzlichen Aufbewahrungsfristen.

(3) Bei Google sind für das Projekt, über das der Router die Modelle bei Google aufruft, die Protokollierung von Eingaben zur Missbrauchsüberwachung (Ausnahme von Google) und die Protokollierung von Anfragen und Antworten ausgeschaltet. Anforderungen eines Zwischenspeichers (Prompt-Caching) entfernt der Router aus jeder Anfrage, bevor er sie weiterleitet, außer in der Variante mit Zwischenspeicher nach Absatz 6. Den Zwischenspeicher, den Google bei Gemini ohne Anforderung führt, hat Gosign für das Projekt abgeschaltet. Die Wiederaufnahme abgebrochener Sprachdialoge, für die Google Inhalte bis zu 24 Stunden speichern würde, lässt der Router nicht zu. Bei Google schaltet Gosign nur Modelle frei, bei denen Eingaben nach Zusagen und Dokumentation von Google ohne Anforderung nicht über die einzelne Anfrage hinaus zwischengespeichert werden oder bei denen dies für das Projekt abgeschaltet ist; ändert sich das, gilt § 8 Abs. 4.

(4) Für die Modelle auf dem Weg in Deutschland sichert der Betreiber Gosign vertraglich Zero Retention zu: Nach seinen technischen und organisatorischen Maßnahmen verarbeitet er Eingaben und Antworten nur flüchtig im Arbeitsspeicher und im Speicher der Grafikprozessoren und schreibt sie weder auf Datenträger noch in Datenbanken, Protokolle, Auslagerungsspeicher oder temporäre Dateien. Ein Zugriff auf diesen Speicher ist danach nicht möglich und findet auch zur Fehleranalyse, Überwachung oder im Support nicht statt. Wiederholte Eingaben hält der Server dabei kurzzeitig im Speicher der Grafikprozessoren vor; die Antwort weist sie als cached_tokens aus, berechnet wird der volle Preis. Ändert sich etwas an diesen Zusagen, gilt § 8 Abs. 4.

(5) Nach Vertragsende gibt Gosign der Kanzlei die Nutzerkennungen in den Verbrauchsdaten auf ihren Wunsch heraus, löscht sie in jedem Fall binnen 30 Tagen und bestätigt die Löschung in Textform. Die übrigen Verbrauchsdaten löscht Gosign mit Ablauf der Frist nach Absatz 2, soweit keine gesetzliche Aufbewahrungspflicht besteht. Inhaltsdaten liegen bei Gosign nicht vor. Einträge im Zwischenspeicher der Variante nach Absatz 6 laufen bei Google spätestens eine Stunde nach ihrer letzten Nutzung ab, auch wenn die Kanzlei die Variante abschaltet oder der Vertrag endet; die Hashwerte verarbeitet Google als Verantwortlicher, ihre Löschung richtet sich nach der Google Cloud Privacy Notice, und eine Frist dafür sagt Google nicht zu.

(6) In der Variante mit Zwischenspeicher für eine Stunde (§ 3 Abs. 6 des Rahmenwerks) lässt der Router bei Anfragen an ein Modell der Variante die Anforderung eines Zwischenspeichers durch, die die Anwendung sendet, und setzt die Dauer des Zwischenspeichers auf eine Stunde; bei allen anderen Modellen entfernt er sie (Absatz 3). Die Variante läuft über dasselbe Projekt mit derselben Ausnahme von der Protokollierung zur Missbrauchsüberwachung wie der Weg über Google ohne Zwischenspeicher. Eingaben und Ausgaben verarbeitet Google auch in der Variante als Unterauftragnehmer nach dem Cloud Data Processing Addendum am Endpunkt in der EU. Fordert die Anwendung einen Zwischenspeicher an, legt Google die Anfrage ab der Mindestlänge, die der Hersteller je Modell festlegt, bis zu der angeforderten Stelle, etwa mit Anweisungen an das Modell, Werkzeugen und dem bisherigen Verlauf, im Zwischenspeicher ab, auch wenn sie sich nicht wiederholt, und hält sie bis zu einer Stunde nach ihrer letzten Nutzung vor; jede Nutzung verlängert die Frist. Eine Möglichkeit, Einträge vor Ablauf der Frist zu löschen,

nennt Google nicht. Google führt den Zwischenspeicher je Projekt, hier für das Projekt, über das der Router die Modelle für alle Kunden aufruft; Kennungen der Kanzlei, etwa Nutzerkennungen und Metadaten, entfernt der Router vor der Weiterleitung, sodass Google vom Router nicht erfährt, welche Kanzlei anfragt. Den Zwischenspeicher behandelt Gosign als Teil der Anfrage wie die Eingaben als Kundendaten; nach seiner Dokumentation nimmt Google nur die Hashwerte von den Schutzmaßnahmen für Kundendaten aus. Als Schlüssel des Zwischenspeichers bildet Google Hashwerte der Anfragen, nach seiner Dokumentation nur für Anfragen, die einen Zwischenspeicher anfordern. Diese Hashwerte verarbeitet Google als Dienstdaten nach der Google Cloud Privacy Notice, für die Google selbst Verantwortlicher ist, und nicht als Kundendaten nach dem Cloud Data Processing Addendum; die Schutzmaßnahmen für Kundendaten gelten für sie nicht, und § 8 Abs. 1 Satz 5 und § 9 Abs. 2 erfassen sie nicht. Nach seiner Dokumentation zum Zwischenspeicher nutzt Google die Hashwerte für keinen anderen Zweck als den Zwischenspeicher; die Google Cloud Privacy Notice nennt für Dienstdaten weitere Zwecke und für die meisten Arten eine Aufbewahrung bis zu 180 Tagen, eine Frist für die Hashwerte sagt Google nicht zu. Aus einem Hashwert lässt sich der Text einer Anfrage nicht zurückrechnen; enthält die Anfrage personenbezogene Daten, sind ihre Hashwerte pseudonymisierte personenbezogene Daten. Wo Google den Zwischenspeicher und die Hashwerte hält, sagt Google nicht zu; die Hashwerte darf Google als Dienstdaten nach der Google Cloud Privacy Notice auch außerhalb der EU verarbeiten. Anfragen über die Variante leitet Gosign nur auf Weisung der Kanzlei (§ 5) weiter. Weisung sind die Freischaltung im Konto und die Wahl von Modellen mit Zwischenspeicher für ihre Guardrails; sie umfasst, dass Google die Anfragen vorhält und die Hashwerte bildet und in eigener Verantwortung verarbeitet. Ob die Kanzlei Google die Hashwerte offenlegen darf, insbesondere bei Daten nach Art. 9 und 10 DSGVO, beurteilt sie selbst, und in ihren Informationen nach Art. 13 und 14 DSGVO nennt sie Google als Empfänger, soweit diese Vorschriften es verlangen. Betrifft eine Änderung nach § 8 Abs. 4 nur den Zwischenspeicher oder die Hashwerte, sperrt Gosign nur die Variante. Die Variante ist kein neuer Weg im Sinne von § 8 Abs. 2.

§ 11 Unterstützung der Kanzlei

(1) Gosign unterstützt die Kanzlei bei Anträgen betroffener Personen nach Art. 12 bis 23 DSGVO. Wendet sich eine betroffene Person an Gosign, leitet Gosign den Antrag unverzüglich an die Kanzlei weiter. Anträge zu Daten, die Gosign als Verantwortliche verarbeitet, beantwortet Gosign selbst.

(2) Gosign meldet der Kanzlei eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie verfügbar sind, und unterstützt die Kanzlei bei der Benachrichtigung betroffener Personen (Art. 34 DSGVO).

(3) Gosign unterstützt die Kanzlei mit den erforderlichen Informationen bei Datenschutz-Folgenabschätzung und vorheriger Konsultation (Art. 35 und 36 DSGVO).

§ 12 Nachweise und Kontrollen

(1) Gosign stellt alle Informationen zum Nachweis der Pflichten aus Art. 28 DSGVO und aus der Zusatzvereinbarung bereit, insbesondere die Urkunden der Unterauftragnehmer nach § 203 StGB. Die Nachweise stehen im Konto (§ 2 Abs. 3 des Rahmenwerks).

(2) Gosign ermöglicht Überprüfungen einschließlich Inspektionen durch die Kanzlei oder einen von ihr beauftragten, zur Verschwiegenheit verpflichteten Prüfer, nach Ankündigung von mindestens 14 Kalendertagen und zu Geschäftszeiten, in der Regel einmal jährlich, aus gegebenem Anlass auch öfter.

§ 13 Haftung und Schlussbestimmungen

(1) Im Außenverhältnis gilt Art. 82 DSGVO, im Innenverhältnis § 11 der AGB der Gosign GmbH, soweit zwingendes Datenschutzrecht nicht entgegensteht.

(2) Die Pflichten zur Verschwiegenheit und zur Löschung wirken über das Vertragsende hinaus.

(3) Dieser Vertrag gilt zusammen mit der Zusatzvereinbarung. Für den Schutz der Geheimnisse geht die strengere Regelung vor; im Übrigen geht dieser Vertrag den AGB vor.

(4) Änderungen bedürfen der Textform; die Annahme im Portal wahrt sie. Es gilt deutsches Recht. Für den Gerichtsstand gilt § 8 Abs. 3 des Rahmenwerks.

(5) Dieser Vertrag wird mit seiner Annahme im Portal oder mit der Unterzeichnung des Rahmenwerks wirksam, je nachdem, was früher liegt.

Anlage 1: Technische und organisatorische Maßnahmen

- **Zugang:** Jede Kanzlei verwaltet eigene Guardrails und Schlüssel in ihrem Konto. Ein Schlüssel erreicht nur die Modelle seiner Guardrails, auf Wunsch nur einen Teil davon, und trägt auf Wunsch einen Höchstbetrag; Guardrails tragen ein Budget. Ist ein Budget oder ein Höchstbetrag erreicht, weist der Router weitere Anfragen ab.
- **Konto:** Anmeldung nur mit zweitem Faktor. Die Rolle einer Person begrenzt, was sie im Konto tun darf. Schlüssel speichert das Konto nur als Prüfwert und zeigt sie beim Ausstellen genau einmal. Änderungen stehen mit Person und Zeit in einer Prüfspur, die sich nicht ändern lässt.
- **Übertragung:** verschlüsselt (TLS) zwischen der Anwendung der Kanzlei und dem Router sowie zwischen dem Router und den Modellbetreibern.
- **Speicherung:** keine Inhaltsdaten im Router; Protokolle nur mit Verbrauchsdaten. Anforderungen eines Zwischenspeichers (Prompt-Caching) entfernt der Router aus jeder Anfrage, außer in der Variante mit Zwischenspeicher, die die Kanzlei für einzelne Guardrails selbst wählt; dort lässt er die Anforderung der Anwendung durch und setzt die Dauer des Zwischenspeichers auf eine Stunde, und Google speichert jede Anfrage bis zu der angeforderten Stelle bis zu einer Stunde nach ihrer letzten Nutzung und bildet Hashwerte, die Google als Verantwortlicher verarbeitet (§ 10 Abs. 6). Der Betreiber der Modelle in Deutschland verarbeitet Inhalte nur flüchtig im Arbeitsspeicher und hält wiederholte Eingaben kurzzeitig im Speicher der Grafikprozessoren vor (§ 10 Abs. 4).
- **Trennung:** Verbrauchsdaten werden je Zugang, Guardrails und Schlüssel geführt; Anfragen verschiedener Kunden führt der Router nicht zusammen. Kennungen der Kanzlei entfernt der Router vor der Weiterleitung an Google, sodass Google vom Router nicht erfährt, welche Kanzlei anfragt; den Zwischenspeicher der Variante führt Google für das Projekt, das allen Kunden gemeinsam ist (§ 10 Abs. 6).
- **Wege:** Im Router sind nur Endpunkte in der EU und in Deutschland eingerichtet. Modelle, die beim Anbieter eine Pflichtspeicherung voraussetzen (bei Google als „Advanced AI“ oder als „Google Frontier Model“ geführt), sind nicht freigeschaltet.
- **Betrieb und Administration:** Rechenzentren des in Anlage 2 genannten Betreibers des Routers in Deutschland; rollenbasierte Administration nur durch autorisierte Personen mit

Zugriffsort in Deutschland oder im EWR.

- **Personal:** Verpflichtung auf Vertraulichkeit und nach § 203 StGB in Textform, mit Belehrung über die Strafbarkeit.
- **Unterauftragnehmer:** Maßnahmen nach deren Auftragsverarbeitungsverträgen; Verpflichtung nach § 203 StGB auf jeder Stufe der Kette (Anlage 2). Das Rechenzentrum der Modelle in Deutschland ist nach ISO/IEC 27001 zertifiziert.

Anlage 2: Unterauftragnehmer

Die genehmigten Unterauftragnehmer nennt die Liste der Unterauftragnehmer, die dem Rahmenwerk als Anlage 4 beigefügt ist, mit Firmierung, Aufgabe, Ort der Verarbeitung und Grundlage nach § 203 StGB. Sie ordnet die Unternehmen den Wegen zu, nicht Modellnamen oder Modellversionen. Sie gilt in der nach § 8 Abs. 2 fortgeschriebenen Fassung, frühere Fassungen stehen im Konto unter Mitteilungen.