Entwurf — Stand 23.04.2026. Die finale juristische Prüfung und Freigabe erfolgt durch Nils Oehmichen, TÜV-zertifizierter Datenschutzbeauftragter nach DSB-GDDcert EU 4.0. Dieses Dokument dient der Vorab-Ansicht durch Interessenten und Kunden der frag.hugo Informationssicherheit GmbH.

Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

Entwurf — Stand 23.04.2026

Dieses Dokument ist ein Entwurf. Die finale juristische Prüfung und Freigabe erfolgt durch Nils Oehmichen, TÜV-zertifizierter Datenschutzbeauftragter nach DSB-GDDcert EU 4.0.

Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV") konkretisiert die datenschutzrechtlichen Pflichten der Vertragsparteien, die sich aus der im Hauptvertrag näher bezeichneten Auftragsverarbeitung ergeben. Er findet Anwendung auf alle Tätigkeiten, bei denen Beschäftigte oder Beauftragte des Auftragnehmers mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

Vertragsparteien:

Auftraggeber (Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO)

- Firma: _____
- Anschrift: _____
- Vertreten durch: _____
- E-Mail: _____
- Ansprechpartner Datenschutz: _____

— nachfolgend „Auftraggeber" —

Auftragnehmer (Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO)

- Firma: frag.hugo Informationssicherheit GmbH
- Anschrift: Spaldingstraße 64–68, 20097 Hamburg
- Vertreten durch die Geschäftsführer: Nils Oehmichen, Jens Hagel
- Handelsregister: Amtsgericht Hamburg
- E-Mail: info@fraghugo.de
- Datenschutzbeauftragter: Nils Oehmichen, nils@fraghugo.de (TÜV-zertifiziert nach DSB-GDDcert EU 4.0)

— nachfolgend „Auftragnehmer" —

— beide gemeinsam „Parteien" —

Bezugsvertrag: Dieser AVV ergänzt den zwischen den Parteien geschlossenen Hauptvertrag über die Nutzung eines oder mehrerer der folgenden Produkte der frag.hugo Informationssicherheit GmbH:

- **Hugo DSB** — Datenschutz-Plattform mit externem Datenschutzbeauftragten (Abonnement)
- **Hugo Shield** — NIS2-Lieferketten-Compliance-Plattform (Abonnement)
- **Hugo Check** — Website-DSGVO-Scanner (Abonnement)

Die konkrete Leistung und die davon betroffenen Datenkategorien sind in Anlage 1 spezifiziert.

---

§ 1 Gegenstand, Dauer und Spezifizierung des Auftrags

(1) Gegenstand des Auftrags sind die im Hauptvertrag sowie in Anlage 1 dieses AVV näher beschriebenen Leistungen, soweit bei deren Erbringung personenbezogene Daten des Auftraggebers durch den Auftragnehmer verarbeitet werden.

(2) Die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen ergeben sich aus Anlage 1. Änderungen der im Auftrag beschriebenen Verarbeitungstätigkeiten bedürfen der Textform.

(3) Die Dauer dieses AVV entspricht der Laufzeit des Hauptvertrags. Der AVV beginnt mit der ersten Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber und endet mit der vollständigen Rückgabe bzw. Löschung der Daten nach Maßgabe von § 11.

---

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach den dokumentierten Weisungen des Auftraggebers im Sinne des Art. 28 DSGVO. Der Auftraggeber bleibt im datenschutzrechtlichen Sinne Verantwortlicher für die Verarbeitung der Daten.

(2) Der Auftraggeber ist allein verantwortlich für die Beurteilung der Rechtmäßigkeit der Verarbeitung (Art. 6 Abs. 1 DSGVO) sowie für die Wahrung der Rechte der betroffenen Personen.

(3) Eine Verarbeitung zu anderen Zwecken als den im Hauptvertrag und in Anlage 1 festgelegten Zwecken ist dem Auftragnehmer untersagt, sofern nicht eine gesetzliche Verpflichtung eine solche Verarbeitung erfordert; in diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

---

§ 3 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers, es sei denn, er ist gesetzlich zu einer sonstigen Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Auftraggebers werden anfänglich durch den Hauptvertrag und diesen AVV festgelegt und können vom Auftraggeber danach in Textform geändert, ergänzt oder ersetzt werden (Einzelweisung). Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(3) Weisungsberechtigte Personen des Auftraggebers sind in Anlage 4 aufgeführt. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner teilt der Auftraggeber dem Auftragnehmer in Textform den Nachfolger bzw. den Vertreter mit.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, so hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(5) Mündliche Weisungen werden vom Auftragnehmer nur in dringenden Fällen angenommen und sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

---

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der Auftragserfüllung und der dokumentierten Weisungen des Auftraggebers. Kopien oder Duplikate der Daten werden ohne Kenntnis des

Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Der Auftragnehmer gewährleistet, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und sonstigen für den Auftragnehmer tätigen Personen sich vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet haben (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO) oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeitsverpflichtung wirkt auch nach Beendigung des Beschäftigungsverhältnisses fort.

(3) Der Auftragnehmer hat gemäß Art. 37 DSGVO einen Datenschutzbeauftragten benannt:

> **Nils Oehmichen** E-Mail: nils@fraghugo.de Qualifikation: TÜV-zertifizierter Datenschutzbeauftragter nach DSB-GDDcert EU 4.0

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(4) Die Umsetzung und Einhaltung aller für diesen Auftrag anwendbaren gesetzlichen Bestimmungen, insbesondere der DSGVO und des BDSG, sowie der vertraglichen Vereinbarungen und Weisungen des Auftraggebers im Hinblick auf den Datenschutz wird vom Auftragnehmer in seinem Verantwortungsbereich sichergestellt.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Erstellung und Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO), soweit dies erforderlich ist. Der Auftragnehmer führt ein eigenes Verzeichnis über alle Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gemäß Art. 30 Abs. 2 DSGVO.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn er Kontrollen oder Maßnahmen der Aufsichtsbehörden feststellt, die sich auf die Verarbeitung im Rahmen dieses Auftrags beziehen.

---

§ 5 Technische und organisatorische Maßnahmen (TOM)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO sicherzustellen. Die zum Zeitpunkt des Vertragsschlusses getroffenen technischen und organisatorischen Maßnahmen sind in Anlage 2 beschrieben.

(2) Die Parteien sind sich darüber einig, dass Veränderungen der technischen und organisatorischen Maßnahmen zulässig bleiben müssen, um sie an den technischen und organisatorischen Fortschritt anzupassen. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, stimmt der Auftragnehmer vorher mit dem Auftraggeber ab. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen darstellen und das Sicherheitsniveau nicht negativ beeinflussen, können vom Auftragnehmer ohne Abstimmung umgesetzt werden; das in Anlage 2 beschriebene Schutzniveau darf dabei nicht unterschritten werden.

(3) Der Auftragnehmer weist die Einhaltung der in Anlage 2 beschriebenen Maßnahmen auf Anforderung des Auftraggebers nach. Die Nachweispflicht kann u.a. durch die Vorlage aktueller Zertifikate, Testate oder Prüfberichte durch unabhängige Stellen erfüllt werden (z.B. ISO 27001 des Rechenzentrums, interne Prüfdokumentation).

---

§ 6 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorheriger Konsultationen.

(2) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO unverzüglich, spätestens jedoch innerhalb von **48 Stunden** nach Kenntniserlangung. Die Meldung erfolgt an die in Anlage 4 benannten Ansprechpartner des Auftraggebers.

(3) Die Meldung enthält, soweit möglich:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, einschließlich, soweit möglich, der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung;
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Können die Informationen nicht zeitgleich bereitgestellt werden, so können diese nach Abstimmung mit dem Auftraggeber schrittweise und ohne unangemessene weitere Verzögerung zur Verfügung gestellt werden.

---

§ 7 Unterstützung bei Betroffenenrechten (Art. 12 bis 22 DSGVO)

(1) Wendet sich eine betroffene Person mit Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs-, Übertragbarkeits- oder Widerspruchsansprüchen (Art. 12 bis 22 DSGVO) unmittelbar an den Auftragnehmer, so wird der Auftragnehmer dieses Ersuchen nicht selbst beantworten, sondern unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Rechte betroffener Personen, insbesondere durch geeignete technische und organisatorische Maßnahmen (z.B. Export-, Berichtigungs- und Löschfunktionen in der Plattform).

(3) Soweit die Unterstützungsleistung über den Leistungsumfang des Hauptvertrags hinausgeht und dem Auftragnehmer nicht aufgrund seines Fehlverhaltens zuzurechnen ist, kann der Auftragnehmer eine angemessene Vergütung verlangen.

---

§ 8 Unterauftragsverhältnisse (Subunternehmerverhältnisse)

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber erteilt hiermit die **allgemeine Genehmigung** zur Einbindung der in Anlage 3 namentlich aufgeführten Unterauftragnehmer (nachfolgend „Subprozessoren") im Sinne von Art. 28 Abs. 2 Satz 2 DSGVO.

(3) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung der Subprozessoren (Hinzuziehung, Ersetzung oder Wegfall) **mindestens 4 Wochen** vor Wirksamwerden der Änderung in Textform. Der Auftraggeber kann der Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb von 4 Wochen nach Zugang der Information widersprechen. Im Falle eines berechtigten Widerspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beanstandete Änderung erbringen oder — sofern ihm dies nicht zumutbar ist — dem Auftraggeber ein Sonderkündigungsrecht für den betroffenen Leistungsteil einräumen.

(4) Der Auftragnehmer hat bei der Auswahl der Subprozessoren deren Eignung und Zuverlässigkeit sorgfältig zu prüfen. Der Auftragnehmer stellt durch vertragliche Regelungen mit den Subprozessoren sicher, dass diese den gleichen datenschutzrechtlichen Verpflichtungen unterliegen wie der Auftragnehmer selbst im Verhältnis zum Auftraggeber. Insbesondere sind hinreichende Garantien dafür zu stellen, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung den Anforderungen der DSGVO entspricht.

(5) Kommt der Subprozessor seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Subprozessors.

§ 9 Drittlandübermittlung

(1) Eine Verarbeitung der personenbezogenen Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur unter Einhaltung der besonderen Voraussetzungen der Art. 44 ff. DSGVO.

(2) Soweit ein Subprozessor seinen Sitz in einem Drittland hat (vgl. Anlage 3), stützt der Auftragnehmer die Übermittlung vorrangig auf einen **Angemessenheitsbeschluss** der Europäischen Kommission im Sinne von Art. 45 DSGVO. Für Übermittlungen in die USA gilt das **EU-US Data Privacy Framework (DPF)** als primäre Rechtsgrundlage, sofern der jeweilige Subprozessor gültig DPF-zertifiziert ist.

(3) Sollte der Angemessenheitsbeschluss (insbesondere das DPF) für einen oder mehrere Subprozessoren wegfallen, seine Wirksamkeit verlieren oder der Subprozessor seine Zertifizierung verlieren, stützt der Auftragnehmer die Übermittlung auf die **Standardvertragsklauseln** der Europäischen Kommission gemäß Durchführungsbeschluss (EU) 2021/914 (Module 2 — Controller-to-Processor bzw. Modul 3 — Processor-to-Processor) in Kombination mit einer **Transfer Impact Assessment (TIA)** und gegebenenfalls zusätzlichen Garantien (z.B. Verschlüsselung, Pseudonymisierung, organisatorische Maßnahmen) entsprechend den Empfehlungen des Europäischen Datenschutzausschusses.

(4) Der Auftragnehmer dokumentiert für jeden Drittland-Subprozessor die jeweilige Rechtsgrundlage (primär und Fallback) in Anlage 3 und stellt dem Auftraggeber auf Anforderung die relevanten Nachweise (SCC-Vertragstexte, DPF-Zertifizierungslisten, TIA) zur Verfügung.

---

§ 10 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder der vertraglichen Vereinbarungen vor Beginn der Datenverarbeitung sowie regelmäßig während der Vertragslaufzeit zu überprüfen, soweit dies in angemessenem Umfang erforderlich ist.

(2) Die Überprüfung erfolgt nach folgender Eskalationsstufe:

1. **Testate und Zertifikate:** Der Auftragnehmer stellt dem Auftraggeber auf Anforderung aktuelle Testate, Zertifikate und Prüfberichte (z.B. ISO 27001 des Rechenzentrums, interne TOM-Dokumentation) zur Verfügung. Dies ist die primäre Nachweismethode.
2. **Schriftliche Auskunft / Fragebogen:** Genügen Testate nach Einschätzung des Auftraggebers nicht, kann der Auftraggeber einen datenschutzrechtlichen Fragebogen (z.B. gemäß BITKOM-Standard) übersenden, den der Auftragnehmer innerhalb angemessener Frist (in der Regel 4 Wochen) beantwortet.
3. **Vor-Ort-Prüfung:** Verbleiben nach Stufe 1 und 2 begründete Zweifel, ist der Auftraggeber berechtigt, sich zu den üblichen Geschäftszeiten nach **rechtzeitiger Voranmeldung (mindestens 4 Wochen)** ohne Störung des Betriebsablaufs selbst von der Einhaltung der Verpflichtungen aus diesem AVV zu überzeugen. Der Auftraggeber kann hierfür eine geeignete, zur Verschwiegenheit verpflichtete dritte Person (z.B. einen unabhängigen Sachverständigen) beauftragen. Mitbewerber des Auftragnehmers sind ausgeschlossen.

(3) Der Auftragnehmer weist auf Anforderung des Auftraggebers nach, dass er seinen datenschutzrechtlichen Pflichten nachgekommen ist. Er stellt dem Auftraggeber hierzu die erforderlichen Informationen zur Verfügung, insbesondere die Dokumentation der technischen und organisatorischen Maßnahmen.

(4) Soweit der Aufwand der Unterstützung der Kontrollen über den Leistungsumfang des Hauptvertrags hinausgeht, kann der Auftragnehmer eine angemessene Vergütung verlangen. Eine Auskunfts- oder Prüfpflicht des Auftragnehmers auf Kosten des Auftragnehmers besteht, wenn die Prüfung auf begründeten Verdacht auf eine Verletzung des Datenschutzes durch den Auftragnehmer zurückzuführen ist.

---

§ 11 Löschung und Rückgabe personenbezogener Daten

(1) Kopien oder Duplikate der Daten werden ohne Kenntnis des Auftraggebers nicht erstellt. Ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten (insbesondere HGB und AO) erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder nach Beendigung des Hauptvertrags — je nachdem, welches Ereignis früher eintritt — hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Die Auswahl obliegt dem Auftraggeber.

(3) Die Löschung bzw. Rückgabe erfolgt **innerhalb von 30 Tagen** nach Beendigung des Hauptvertrags, sofern der Auftraggeber nichts anderes in Textform anweist.

(4) Von der Löschungspflicht ausgenommen sind Daten, für die gesetzliche Aufbewahrungspflichten gelten (insbesondere nach §§ 257 HGB und §§ 146, 147 AO). Solche Daten werden bis zum Ablauf der jeweiligen Aufbewahrungsfrist gesperrt und anschließend unverzüglich gelöscht.

(5) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

---

§ 12 Haftung

(1) Für die Haftung der Parteien gegenüber betroffenen Personen gilt Art. 82 DSGVO.

(2) Im Innenverhältnis der Parteien gilt: Die Parteien stellen sich gegenseitig von Ansprüchen Dritter und behördlichen Sanktionen frei, soweit die jeweilige Partei ihre Pflichten aus diesem AVV oder der DSGVO schuldhaft verletzt hat und diese Pflichtverletzung ursächlich für die Inanspruchnahme bzw. Sanktion ist.

(3) Eine über Art. 82 DSGVO und die vorstehenden Regelungen hinausgehende Haftungsbegrenzung bleibt dem Hauptvertrag vorbehalten; im Zweifel gehen die dortigen Regelungen vor, soweit sie mit zwingendem Datenschutzrecht vereinbar sind.

> *Hinweis zum Entwurfsstand: Die konkrete Ausgestaltung der vertraglichen Haftungsregelung (insbesondere etwaige Haftungsbegrenzungen) bedarf der abschließenden juristischen Prüfung durch den Datenschutzbeauftragten Nils Oehmichen und ggf. der anwaltlichen Abstimmung. Dieser Entwurf enthält bewusst keine eigene summenmäßige Begrenzung.*

---

§ 13 Schlussbestimmungen

(1) **Schriftform / Textform:** Nebenabreden zu diesem AVV sowie Änderungen und Ergänzungen bedürfen der Textform; dies gilt auch für die Abbedingung dieses Formerfordernisses. Einzelweisungen nach § 3 können auch in Textform erteilt werden.

(2) **Rang- und Auslegungsregel:** Bei Widersprüchen zwischen den Regelungen dieses AVV und den Regelungen des Hauptvertrags gehen die Regelungen dieses AVV vor, soweit es um Fragen des Datenschutzes geht.

(3) **Anlagen:** Die Anlagen 1 bis 4 sind Bestandteil dieses Vertrags.

(4) **Anwendbares Recht:** Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

(5) **Gerichtsstand:** Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist, soweit gesetzlich zulässig, **Hamburg**.

(6) **Salvatorische Klausel:** Sollte eine Bestimmung dieses Vertrags unwirksam oder undurchführbar sein oder werden, so bleibt die Wirksamkeit des Vertrags im Übrigen hiervon unberührt. Die Parteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung durch eine wirksame und durchführbare Regelung zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung möglichst nahekommt. Entsprechendes gilt für Regelungslücken.

Unterschriften

Auftraggeber	**Auftragnehmer (frag.hugo Informationssicherheit GmbH)**
Ort, Datum: _____	Ort, Datum: Hamburg, _____
Unterschrift: _____	Unterschrift: _____
Name in Druckbuchstaben: _____	Name in Druckbuchstaben: _____
Funktion: _____	Funktion: Geschäftsführer

Anlage 1 — Leistungsbeschreibung und Gegenstand der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber je nach gebuchtem Produkt die nachstehenden Leistungen zur Verfügung. Gegenstand der Auftragsverarbeitung sind nur die tatsächlich gebuchten Leistungen.

1.1 Hugo DSB (Datenschutz-Plattform mit externem DSB)

Leistungsbeschreibung:

SaaS-Plattform zur Verwaltung der Datenschutz-Compliance eines Unternehmens (VVT, AVV-Verwaltung, Datenpannen-Register, DSAR-Bearbeitung, TOMs, Löschkonzept, DSFA, Hinweisgeberschutz, NIS2, AI Act) ergänzt um die persönliche Betreuung durch den externen Datenschutzbeauftragten sowie optionale KI-gestützte Schulungsmodule und Phishing-Simulation für die Mitarbeiter des Auftraggebers.

Art der Verarbeitung: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln, Löschen.

Zweck der Verarbeitung: Bereitstellung der Plattform-Funktionen; Durchführung von Schulungen und Phishing-Simulationen; Erbringung der DSB-Dienstleistung.

Kategorien betroffener Personen:

- Mitarbeiter des Auftraggebers (Plattform-Nutzer, Schulungsteilnehmer)
- Ansprechpartner auf Kundenseite (interne DSB, Geschäftsführung)
- Ggf. betroffene Personen im Rahmen von VVT-Einträgen oder Datenpannen (indirekt, als Metadaten)
- Hinweisgeber im Rahmen des Meldeportals (pseudonym)

Kategorien personenbezogener Daten:

- Stammdaten (Name, E-Mail, Funktion, Telefon)
- Login- und Authentifizierungsdaten
- Nutzungs- und Protokolldaten (Login-Zeitstempel, IP-Adresse, Audit-Log)
- Schulungsfortschritte und Quiz-Ergebnisse
- Phishing-Simulationsergebnisse (Klick/Kein Klick, Lerneinheit absolviert)
- Inhalte von VVT-Einträgen, Datenpannen-Meldungen, DSAR-Vorgängen (soweit vom Auftraggeber eingegeben)
- Hinweise im Meldeportal (verschlüsselt)

Besondere Kategorien nach Art. 9 DSGVO: Nicht regelhaft vorgesehen. Sofern der Auftraggeber in den Freitextfeldern der Plattform besondere Kategorien erfasst, liegt dies in dessen alleiniger Verantwortung.

1.2 Hugo Shield (NIS2-Lieferketten-Compliance)

Leistungsbeschreibung: SaaS-Plattform zur Erfassung, Bewertung und Nachverfolgung der Cybersecurity-Compliance von Lieferanten und Dienstleistern des Auftraggebers im Rahmen der NIS2-Anforderungen.

Art der Verarbeitung: Erheben, Speichern, Ordnen, Auslesen, Übermitteln (innerhalb der Plattform), Löschen.

Zweck der Verarbeitung: Erfüllung der NIS2-Sorgfaltspflichten gegenüber Lieferanten; Risikobewertung; Audit-Dokumentation.

Kategorien betroffener Personen:

- Ansprechpartner beim Auftraggeber (Einkauf, IT-Sicherheit)
- Ansprechpartner bei Lieferanten des Auftraggebers (Kontaktdaten aus Fragebogen-Rücklauf)

Kategorien personenbezogener Daten:

- Stammdaten (Name, Firma, E-Mail, Funktion)
- Nutzungs- und Protokolldaten
- Inhalte von Lieferanten-Fragebögen (enthalten i.d.R. organisatorische Angaben, aber auch Ansprechpartner-Daten)
- Audit-Log

Besondere Kategorien nach Art. 9 DSGVO: Nicht vorgesehen.

1.3 Hugo Check (Website-DSGVO-Scanner, Abo)

Leistungsbeschreibung: Automatisierter Scanner, der die öffentlich zugängliche Website des Auftraggebers auf DSGVO-relevante technische Merkmale (Cookies, Third-Party-Ressourcen, Security-Headers, Impressum, Datenschutzerklärung) prüft und ein Ergebnis-Report erstellt.

Art der Verarbeitung: Erheben, Speichern, Auslesen, Übermitteln (Report an den Auftraggeber).

Zweck der Verarbeitung: Bereitstellung des Scan-Ergebnisses; Dokumentation des Compliance-Status im Zeitverlauf (Pro-/Agentur-Abo).

Kategorien betroffener Personen:

- Ansprechpartner beim Auftraggeber (Account-Inhaber)

Kategorien personenbezogener Daten:

- Stammdaten (Name, E-Mail)
- Zu scannende Domain(s)
- Scan-Historie und Ergebnisse (kann inzidentell personenbezogene Daten enthalten, z.B. Namen in Impressumszeilen der zu scannenden Website)
- Nutzungs- und Protokolldaten

Besondere Kategorien nach Art. 9 DSGVO: Nicht vorgesehen.

Anlage 2 — Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

1. Vertraulichkeit — Zutrittskontrolle (physisch)

Die Verarbeitung personenbezogener Daten erfolgt in den Rechenzentren der Hetzner Online GmbH in Falkenstein und Nürnberg (Deutschland). Die Rechenzentren sind **ISO 27001-zertifiziert** und verfügen über mehrstufige physische Zugangskontrollen (Vereinzelungsanlagen, Videoüberwachung, 24/7-Sicherheitsdienst, Protokollierung). Die frag.hugo-Geschäftsräume (Hamburg) unterliegen einer Schlüsselordnung mit dokumentierter Ausgabe.

2. Vertraulichkeit — Zugangskontrolle (logisch)

- Authentifizierung über starke Passwörter (Mindestlänge, Komplexitätsanforderungen)
- **Multi-Faktor-Authentifizierung (MFA)** für administrative Zugänge
- Passwort-Hashing mit **Argon2** (bzw. bcrypt in Legacy-Pfaden)
- Automatisches Session-Timeout
- Sperrung bei Fehlversuchen

3. Vertraulichkeit — Zugriffskontrolle

- **Rollenbasiertes Berechtigungskonzept (RBAC)** mit den Rollen `admin`, `editor` und `mitarbeiter`
- **Row-Level-Security (RLS)** auf Datenbank-Ebene (Supabase/PostgreSQL) zur Mandantentrennung
- Least-Privilege-Prinzip bei der Vergabe administrativer Rechte
- Protokollierung administrativer Zugriffe

4. Vertraulichkeit — Trennungskontrolle

- **Mandantentrennung** per Schema bzw. `organization_id` auf DB-Ebene
- Logische Trennung von Produktiv-, Staging- und Entwicklungsumgebungen
- Getrennte Verarbeitung für unterschiedliche Zwecke

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

- Wo der Verarbeitungszweck es zulässt (insbesondere Analytics, Fehlerprotokolle), werden Daten pseudonymisiert bzw. anonymisiert verarbeitet

6. Integrität — Weitergabekontrolle

- Transport-Verschlüsselung **TLS 1.3** bei allen externen Verbindungen
- HTTP Strict Transport Security (HSTS) mit `includeSubDomains` und `preload`
- Referrer-Policy `strict-origin-when-cross-origin`
- API-Zugriffe über authentifizierte, zeitlich begrenzte Tokens

7. Integrität — Eingabekontrolle

- **Audit-Log** im Hugo-Shield-Modul (`shield_audit_log`) und Zeitstempel (`updated_at`) in Profil- und Verarbeitungs-Tabellen
- Nachvollziehbarkeit, welcher Nutzer wann welchen Datensatz verändert hat

- Schreibschutz historischer Einträge

8. Verfügbarkeit — Datensicherung

- **Tägliche Snapshot-Backups** der Datenbank auf Hetzner-Ebene
- Retention: 7 Tage Rolling-Backup
- Backup-Verschlüsselung

9. Verfügbarkeit — Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c DSGVO)

- **Recovery Point Objective (RPO): 24 Stunden**
- **Recovery Time Objective (RTO): 4 Stunden**
- Restore-Prozedur ist intern dokumentiert und wird regelmäßig geübt

10. Auftragskontrolle

- Schriftliche Verträge (AVV / DPA) mit allen Subprozessoren (siehe Anlage 3)
- Vertragliche Verpflichtung der Subprozessoren auf das gleiche Datenschutzniveau
- Dokumentation und regelmäßige Überprüfung der Subprozessor-Eignung

11. Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- **Verschlüsselung at rest:** Festplattenverschlüsselung mittels LUKS auf den Hetzner-Hosts
- **Verschlüsselung in transit:** TLS 1.3 für alle externen und internen Verbindungen zwischen den Diensten
- Verschlüsselte Aufbewahrung sensibler Secrets (Env-Vars, API-Keys)

12. Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DSGVO)

- **Cloudflare**-basierter DDoS-Schutz
- Rate-Limiting auf Anwendungs- und Gateway-Ebene (Supabase)
- Monitoring und Alerting

13. Regelmäßige Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- **ISO 27001-Audit** des Hetzner-Rechenzentrums (jährlich durch Hetzner)
- **Interne TOM-Review** mindestens jährlich
- Anlassbezogene Reviews nach Sicherheitsvorfällen oder wesentlichen Änderungen
- Software-Dependency-Scanning und Patch-Management

14. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

- Datenminimierung in der Datenerhebung (nur erforderliche Felder)
- Datenschutzfreundliche Default-Einstellungen (z.B. Opt-in für nicht erforderliche Cookies)
- Privacy-by-Design im Entwicklungsprozess (Design-Reviews)

15. Vertraulichkeitsverpflichtung der Mitarbeiter (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO)

- Alle Mitarbeiter und externen Dienstleister des Auftragnehmers sind vor Aufnahme der Tätigkeit schriftlich zur Vertraulichkeit verpflichtet
- Die Verpflichtung wirkt über die Beendigung des Beschäftigungsverhältnisses hinaus
- Regelmäßige Sensibilisierungs-Schulungen

16. Unterstützung bei Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

- Der Auftragnehmer stellt dem Auftraggeber auf Anforderung die für eine DSFA erforderlichen Informationen bereit (Art der Verarbeitung, TOMs, Risikobewertung der eingesetzten Technik)

17. Benennung des Datenschutzbeauftragten (Art. 37 DSGVO)

- **Nils Oehmichen**
- E-Mail: `nils@fraghugo.de`
- Qualifikation: **TÜV-zertifiziert nach DSB-GDDcert EU 4.0**

Anlage 3 — Subprozessoren

Der Auftraggeber genehmigt den Einsatz der nachfolgenden Subprozessoren im Sinne von § 8 Abs. 2 dieses AVV. Der Auftragnehmer ist verpflichtet, dem Auftraggeber Änderungen mindestens 4 Wochen im Voraus mitzuteilen.

Nr.	Subprozessor	Sitz	Rolle / Leistung	Primäre Rechtsgrundlage der Übermittlung	Fallback / Zusatzgarantien
1	**Hetzner Online GmbH**	Falkenstein und Nürnberg (Deutschland)	Hosting, Rechenzentrum, Infrastruktur (ISO 27001)	EU-intern, kein Drittlandtransfer	—
2	**Supabase (Self-Hosted auf Hetzner-Infrastruktur)**	Self-Hosted durch den Auftragnehmer auf Hetzner-Servern (Deutschland)	Datenbank-, Authentifizierungs- und Storage-Software	Self-Hosted; **kein Datentransfer an Supabase Inc.** (nur die Open-Source-Software wird genutzt)	—
3	**Resend Inc.**	USA	Versand transaktionaler E-Mails	**DPF-Zertifizierung** (gültig seit 10.07.2023, Angemessenheitsbeschluss der EU-Kommission)	SCC 2021/914 Modul 2 + Transfer Impact Assessment (TIA)
4	**Brevo (Sendinblue SAS)**	Frankreich	CRM, Meeting-Buchungen, Marketing-E-Mails	EU-intern, kein Drittlandtransfer	—
5	**Stripe, Inc.**	USA	Zahlungsabwicklung für Abonnements	**DPF-Zertifizierung**	SCC 2021/914 + TIA
6	**OpenAI, L.L.C.**	USA	KI-Funktionen in Hugo DSB Professional und Enterprise (Enterprise-API mit **Zero Data Retention**)	**DPF-Zertifizierung** + vertragliches Zero-Retention-Agreement (keine Trainingsnutzung, keine Persistenz der Prompts/Responses durch OpenAI)	SCC 2021/914 + TIA
7	**Cloudflare, Inc.**	USA	CDN, DNS, DDoS-Schutz, WAF	**DPF-Zertifizierung**	SCC 2021/914 + TIA

Hinweise:

- Nebenleistungen im Sinne von § 8 Abs. 1 dieses AVV (Telekommunikation, Post, Wartung, Entsorgung von Datenträgern etc.) gelten nicht als Unterauftragsverhältnisse und sind nicht in dieser Liste geführt.
- **Microsoft Clarity** (Session-Recordings, Heatmaps) ist **kein Subprozessor** dieses AVV, sondern wird **ausschließlich auf den Marketing-Webseiten der frag.hugo Informationssicherheit GmbH (fraghugo.de)** mit **expliziter Einwilligung des jeweiligen Website-Besuchers** (Opt-in-Cookie-Banner) eingesetzt. Microsoft Clarity erfasst **keine** Kundendaten aus den Hugo-Apps (Hugo DSB, Hugo Shield, Hugo Check).

Anlage 4 — Weisungsberechtigte und Ansprechpartner

Weisungsberechtigte des Auftraggebers

Der Auftraggeber benennt die nachfolgenden Personen als weisungsberechtigt im Sinne von § 3 Abs. 3 dieses AVV:

Nr.	Name	Funktion	E-Mail	Telefon
1	_____	_____	_____	_____
2	_____	_____	_____	_____

Ansprechpartner für Datenschutz-Vorfälle (Auftraggeber)

Meldungen nach § 6 dieses AVV (Datenpannen) werden an folgende Adresse(n) gerichtet:

Name	Funktion	E-Mail	Telefon (24/7)
_____	_____	_____	_____

Ansprechpartner des Auftragnehmers

Funktion	Name	E-Mail
Datenschutzbeauftragter	Nils Oehmichen	nils@fraghugo.de
Technik / IT-Sicherheit	Jens Hagel	jens@fraghugo.de
Allgemein	—	info@fraghugo.de

Ende des Auftragsverarbeitungsvertrags — Entwurf Stand 23.04.2026 — finale juristische Prüfung durch Nils Oehmichen (TÜV-zertifizierter DSB nach DSB-GDDcert EU 4.0) vorbehalten.