AAV-Vereinbarung

Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO

zwischen

Grensing Business Technology Consulting GmbH

(nachfolgend „Auftragsverarbeiter“)

und

dem Kunden gemäß Hauptvertrag

(nachfolgend „Verantwortlicher“)

Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV“) wird als Ergänzung zum SaaS-Vertrag über die Software „Safety Stock Simulator“ (nachfolgend „Hauptvertrag“) zwischen dem Auftragsverarbeiter und dem Verantwortlichen geschlossen.

Er regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen gemäß Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „DSGVO“) sowie den einschlägigen nationalen Datenschutzgesetzen.

Der Auftragsverarbeiter verarbeitet im Rahmen des Hauptvertrags ausschließlich Zugangsdaten der autorisierten Nutzer des Verantwortlichen. Eine Verarbeitung von Inhaltsdaten oder sonstigen Daten des Verantwortlichen findet nicht statt.

§ 1 Gegenstand, Dauer und Art der Verarbeitung

(1) Gegenstand: Gegenstand der Auftragsverarbeitung ist die Bereitstellung des cloudbasierten „Safety Stock Simulator“ im Wege des Software-as-a-Service (SaaS). Zur technischen Bereitstellung des Dienstes verarbeitet der Auftragsverarbeiter personenbezogene Daten der autorisierten Nutzer des Verantwortlichen.

(2) Dauer: Die Auftragsverarbeitung beginnt mit Inkrafttreten des Hauptvertrags und endet mit dessen Beendigung, unabhängig vom Beendigungsgrund. Regelungen zur Datenschutzlöschung nach Vertragsende bleiben davon unberührt (vgl. § 8 dieses AVV).

(3) Art der Verarbeitung: Die Verarbeitung umfasst das Erheben, Speichern, Verwenden, Übermitteln (im Rahmen der Authentifizierung) sowie das Löschen personenbezogener Daten. Eine Verarbeitung von Inhaltsdaten des Verantwortlichen findet nicht statt; hochgeladene Nutzerdaten werden nicht auf den Systemen des Auftragsverarbeiters gespeichert.

(4) Zweck: Die Verarbeitung erfolgt ausschließlich zum Zweck der Benutzerauthentifizierung und der technischen Bereitstellung des Zugangs zur Software.

§ 2 Kategorien betroffener Personen und Datenkategorien

(1) Betroffene Personen: Von der Verarbeitung betroffen sind ausschließlich die vom Verantwortlichen autorisierten Nutzer der Software, in der Regel Mitarbeiterinnen und Mitarbeiter des Verantwortlichen.

(2) Datenkategorien: Es werden ausschließlich folgende Datenkategorien verarbeitet:

- Name der Nutzerin / des Nutzers
- Geschäftliche E-Mail-Adresse
- Verschlüsseltes Passwort (gehasht und gesalzen; keine Speicherung im Klartext)
- Zeitstempel des letzten Anmeldevorgangs (technisches Protokoll)
- Ende des Gültigkeitszeitraums des Zugangs

(3) Keine besonderen Kategorien: Die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO (z. B. Gesundheitsdaten, biometrische Daten, politische Meinungen) findet nicht statt und ist nicht Gegenstand dieses Vertrags.

§ 3 Pflichten des Auftragsverarbeiters

(1) Weisungsgebundenheit: Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Europäischen Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. In einem solchen Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das jeweilige Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Vertraulichkeit: Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Technische und organisatorische Maßnahmen: Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die im Rahmen dieses Vertrags geltenden Maßnahmen sind in der Anlage (Technische und Organisatorische Maßnahmen) zu diesem AVV beschrieben.

(4) Keine unbefugte Weitergabe: Der Auftragsverarbeiter gibt personenbezogene Daten nicht ohne ausdrückliche Weisung des Verantwortlichen an Dritte weiter, soweit nicht gesetzliche Verpflichtungen entgegenstehen.

(5) Meldepflicht bei Datenpannen: Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Bekanntwerden, über Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO. Die Meldung enthält mindestens die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben, soweit diese zum Zeitpunkt der Meldung bereits bekannt sind.

(6) Unterstützungspflichten: Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erfüllung seiner Pflichten gemäß Art. 32–36 DSGVO (Datensicherheit, Meldepflichten, Datenschutz-Folgenabschätzung).

§ 4 Pflichten des Verantwortlichen

(1) Rechtsgrundlage: Der Verantwortliche stellt sicher, dass eine Rechtsgrundlage im Sinne von Art. 6 DSGVO für die Übermittlung der Nutzerdaten an den Auftragsverarbeiter vorliegt, insbesondere dass die Nutzung der Software durch sein Personal rechtlich zulässig ist.

(2) Aktualität der Nutzerdaten: Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich über Änderungen am Nutzerkreis, insbesondere das Ausscheiden von Mitarbeiterinnen und Mitarbeitern, damit Zugangsdaten zeitnah deaktiviert oder gelöscht werden können.

(3) Weisungsrecht: Der Verantwortliche erteilt alle Weisungen zur Verarbeitung personenbezogener Daten in Textform. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

(4) Prüfung der TOMs: Der Verantwortliche hat sich vor Beginn der Verarbeitung und sodann regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters zu überzeugen.

§ 5 Unterauftragsverarbeiter

(1) Allgemeine Genehmigung: Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder den Austausch von Unterauftragsverarbeitern und gibt dem Verantwortlichen damit die Möglichkeit, Einwände zu erheben.

(2) Aktuelle Unterauftragsverarbeiter: Zum Zeitpunkt des Vertragsschlusses setzt der Auftragsverarbeiter folgende Unterauftragsverarbeiter ein:

Anbieter	Zweck	Sitz
iONOS SE, Eigendorfer Str. 57, 56410 Montabaur	Hosting / E-Mail / Benutzerauthentifizierung	Deutschland
Stripe Technology Company Limited (STC), One Wilton Park, Wilton Place, Dublin 2 D02 FX04, Irland	Zahlungsverkehr	Irland

(3) Weitergabe von Pflichten: Der Auftragsverarbeiter legt Unterauftragsverarbeitern dieselben Datenschutzpflichten auf, die zwischen dem Verantwortlichen und dem Auftragsverarbeiter vereinbart sind, insbesondere durch den Abschluss eines entsprechenden Vertrags gemäß Art. 28 DSGVO.

(4) Drittländer: Eine Übermittlung personenbezogener Daten an Unterauftragsverarbeiter in Drittländern außerhalb der EU/EWR ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Der Auftragsverarbeiter informiert den Verantwortlichen vorab über beabsichtigte Übermittlungen in Drittländer.

§ 6 Betroffenenrechte

(1) Unterstützungspflicht: Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung von Anfragen betroffener Personen, insbesondere im Hinblick auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO), Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie Datenübertragbarkeit (Art. 20 DSGVO).

(2) Vereinfachtes Verfahren: Aufgrund des minimalen Verarbeitungsumfangs (ausschließlich Zugangsdaten) kann der Verantwortliche Betroffenenanfragen in der Regel selbst bearbeiten. Der Auftragsverarbeiter stellt auf Anfrage die erforderlichen Informationen zeitnah zur Verfügung.

(3) Weiterleitung: Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter.

§ 7 Nachweispflichten und Audits

(1) Nachweispflicht: Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung, um die Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten nachzuweisen.

(2) Auditrecht: Der Verantwortliche ist berechtigt, die Einhaltung der Datenschutzpflichten durch den Auftragsverarbeiter zu überprüfen. Angesichts des minimalen Verarbeitungsumfangs wird vereinbart, dass diese Überprüfung vorrangig durch folgende Maßnahmen erfolgt:

- Vorlage eines ausgefüllten Datenschutz-Fragebogens durch den Auftragsverarbeiter
- Vorlage aktueller Zertifizierungen (z. B. ISO/IEC 27001) oder gleichwertiger Nachweise
- Schriftliche Auskunft des Auftragsverarbeiters zu konkreten Fragen des Verantwortlichen

(3) Vor-Ort-Audits: Vor-Ort-Audits beim Auftragsverarbeiter sind nur zulässig, wenn der Verantwortliche konkrete Anhaltspunkte für eine Verletzung datenschutzrechtlicher Pflichten darlegt und Audits nach Abs. 2 nicht ausreichend waren. Sie sind mit einer Frist von mindestens vier Wochen anzukündigen, auf das für die Überprüfung erforderliche Maß zu beschränken und auf Kosten des Verantwortlichen durchzuführen.

§ 8 Löschung und Rückgabe nach Vertragsende

(1) Löschung von Zugangsdaten: Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter die Zugangsdaten der Nutzer des Verantwortlichen innerhalb von 30 Tagen vollständig und unwiderruflich aus seinen Systemen. Dies entspricht der Regelung in § 3 Abs. 10 des Hauptvertrags.

(2) Keine Inhaltsdaten: Da der Safety Stock Simulator keine Inhaltsdaten des Verantwortlichen auf den Systemen des Auftragsverarbeiters speichert, beschränkt sich die Löschpflicht auf die in § 2 Abs. 2 dieses AVV genannten Datenkategorien.

(3) Protokolldaten: Technische Protokolldaten (Logs) werden nach Maßgabe der gesetzlichen Aufbewahrungspflichten gelöscht, spätestens jedoch 12 Monate nach Vertragsende.

(4) Löschbestätigung: Auf Anfrage des Verantwortlichen bestätigt der Auftragsverarbeiter die erfolgte Löschung in Textform.

§ 9 Schlussbestimmungen

(1) Vorrang: Im Falle von Widersprüchen zwischen diesem AVV und dem Hauptvertrag in datenschutzrechtlichen Fragen geht dieser AVV vor.

(2) Schriftform: Änderungen und Ergänzungen dieses AVV bedürfen der Textform. Mündliche Nebenabreden bestehen nicht.

(3) Anwendbares Recht: Für diesen AVV gilt das Recht der Bundesrepublik Deutschland sowie unmittelbar anwendbares EU-Recht, insbesondere die DSGVO.

(4) Salvatorische Klausel: Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(5) Bestandteil des Hauptvertrags: Dieser AVV ist als Anlage Bestandteil des Hauptvertrags und gilt ab dem Zeitpunkt des Inkrafttretens des Hauptvertrags.

Anlage: Technische und Organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO – Stand: 20.03.2026

Die folgenden Maßnahmen beschreiben den Mindeststandard, den der Auftragsverarbeiter zum Schutz der im Rahmen des Hauptvertrags verarbeiteten personenbezogenen Daten (Zugangsdaten autorisierter Nutzer) einsetzt.

Maßnahme	Beschreibung
Transportverschlüsselung	Alle Datenübertragungen zwischen dem Browser des Nutzers und dem Server erfolgen ausschließlich über HTTPS mit TLS 1.2 oder höher. HTTP-Verbindungen werden automatisch auf HTTPS umgeleitet.
Passwortsicherheit	Passwörter werden ausschließlich als Hash-Wert gespeichert. Eine Speicherung im Klartext findet zu keinem Zeitpunkt statt.
Zugriffskontrolle	Der Zugriff auf die Anwendung ist ausschließlich nach erfolgreicher Authentifizierung möglich. Jede Nutzer-Session wird durch ein serverseitig verwaltetes Token gesichert. Sessions werden nach Inaktivität automatisch beendet.
Berechtigungsmanagement	Administrative Zugriffe auf die Produktionssysteme sind auf autorisierte Mitarbeiter des Auftragsverarbeiters beschränkt und werden nach dem Prinzip der minimalen Rechtevergabe (Least Privilege) vergeben.
Rechenzentrumsicherheit	Die Software wird in einem zertifizierten Rechenzentrum betrieben (mindestens ISO/IEC 27001 oder gleichwertig). Der physische Zutritt ist auf autorisiertes Personal beschränkt (Zutrittskontrollsystem, Videoüberwachung).
Datentrennung	Die Daten verschiedener Kunden werden logisch getrennt gespeichert und verarbeitet. Ein Zugriff zwischen Kundenmandanten ist technisch ausgeschlossen.
Protokollierung	Anmeldevorgänge werden protokolliert (Zeitstempel, IP-Adresse). Protokolldaten werden ausschließlich zur Erkennung von Sicherheitsvorfällen verwendet und nach 12 Monaten gelöscht.

Datensicherung	Der Auftragsverarbeiter führt regelmäßige Backups der Systemdatenbank durch. Die Wiederherstellbarkeit wird regelmäßig getestet. Zugangsdaten können im Falle eines Systemausfalls aus Backups wiederhergestellt werden.
Löschkonzept	Nach Vertragsende werden Zugangsdaten innerhalb von 30 Tagen vollständig gelöscht. Technische Protokolldaten werden nach 12 Monaten automatisch gelöscht.
Mitarbeitersensibilisierung	Mitarbeiter des Auftragsverarbeiters mit Zugang zu Produktionssystemen werden regelmäßig zum Thema Datenschutz und IT-Sicherheit geschult und sind zur Vertraulichkeit verpflichtet.
Incident Management	Der Auftragsverarbeiter unterhält einen definierten Prozess zur Erkennung, Bewertung und Meldung von Sicherheitsvorfällen. Bei Datenpannen wird der Verantwortliche binnen 24 Stunden informiert.

Der Auftragsverarbeiter überprüft und aktualisiert die TOMs regelmäßig sowie anlassbezogen bei wesentlichen Änderungen der Verarbeitungsumgebung. Wesentliche Änderungen werden dem Verantwortlichen rechtzeitig mitgeteilt.