

# Auftragsverarbeitungsvertrag (AVV)

## § 1 Gegenstand und Verhältnis zum Hauptvertrag

- (1) Dieser Auftragsverarbeitungsvertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Zusammenhang mit der Bereitstellung und Nutzung der HAIZOP-Plattform.
- (2) Dieser Auftragsverarbeitungsvertrag ergänzt die SaaS-Vertragsbedingungen, die Bestellübersicht, die Leistungsbeschreibung und die Datenschutz- und Sicherheitsanlage.
- (3) Bei Widersprüchen zwischen diesem Auftragsverarbeitungsvertrag und sonstigen Vertragsdokumenten geht dieser Auftragsverarbeitungsvertrag hinsichtlich der Verarbeitung personenbezogener Daten im Auftrag vor.
- (4) Die Datenschutz- und Sicherheitsanlage konkretisiert insbesondere technische und organisatorische Maßnahmen, Unterauftragnehmer, Drittlandbezüge, KI-Verarbeitung, Supportzugriffe, Protokollierung, Backup, Rückgabe und Löschung.

## § 2 Rollen der Parteien

- (1) Der Auftraggeber ist Verantwortlicher im Sinne des Datenschutzrechts, soweit personenbezogene Daten durch ihn oder seine Nutzer in die HAIZOP-Plattform eingebracht oder im Rahmen der Plattformnutzung verarbeitet werden.
- (2) Der Auftragnehmer verarbeitet personenbezogene Daten insoweit als Auftragsverarbeiter nach dokumentierter Weisung des Auftraggebers.
- (3) Soweit HAIZOP personenbezogene Daten zu eigenen Zwecken verarbeitet und dabei Zwecke und Mittel der Verarbeitung selbst bestimmt, insbesondere Vertragskontakt-, Abrechnungs-, Zahlungs-, Kommunikations- und gesetzliche Nachweisdaten, erfolgt diese Verarbeitung nicht als Auftragsverarbeitung, sondern in eigener datenschutzrechtlicher Verantwortlichkeit von HAIZOP.
- (4) Die Verarbeitung personenbezogener Daten des Auftraggebers zur Bereitstellung, zum Betrieb, zur Wartung, Sicherheit, Fehleranalyse und Unterstützung der HAIZOP-Plattform bleibt hiervon unberührt und erfolgt nach Maßgabe dieses Auftragsverarbeitungsvertrags.

## § 3 Art, Zweck und Umfang der Verarbeitung

- (1) Gegenstand der Verarbeitung ist die Bereitstellung, der Betrieb, die Wartung, die Sicherung, die Fehleranalyse und die Unterstützung bei der Nutzung der HAIZOP-Plattform.
- (2) Die Verarbeitung dient ausschließlich der Erbringung der vertraglich vereinbarten Leistungen gegenüber dem Auftraggeber.
- (3) HAIZOP verarbeitet personenbezogene Daten des Auftraggebers nicht zu eigenen Werbe-, Marktanalyse-, Benchmarking-, Produktentwicklungs-, Trainings- oder Verbesserungszwecken, soweit hierfür keine gesonderte ausdrückliche Vereinbarung oder gesetzliche Erlaubnis besteht.
- (4) Zulässig bleiben technische Protokollierungen, Sicherheitsanalysen, Missbrauchserkennung, Fehleranalysen, Kapazitäts- und Leistungsanalysen sowie abrechnungsrelevante Auswertungen, soweit sie für Bereitstellung, Betrieb, Sicherheit, Abrechnung, Nachweisführung oder vertragsgemäße Nutzung der HAIZOP-Plattform erforderlich sind. Soweit möglich und angemessen erfolgen solche Auswertungen aggregiert, pseudonymisiert oder ohne vollständige Inhaltsdaten.
- (5) Inhalt, Umfang, Kategorien personenbezogener Daten und Kategorien betroffener Personen ergeben sich aus Anlage 1.

## § 4 Weisungen des Auftraggebers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, soweit keine gesetzliche Pflicht zur Verarbeitung besteht.
- (2) Die Weisungen ergeben sich zunächst aus diesem Auftragsverarbeitungsvertrag, den SaaS-Vertragsbedingungen, der Bestellübersicht, der Leistungsbeschreibung und der Datenschutz- und Sicherheitsanlage.

- (3) Zusätzliche Weisungen müssen in Textform erfolgen und dürfen den vertraglich vereinbarten Leistungsumfang nicht überschreiten.
- (4) Soweit zusätzliche Weisungen zu einem Mehraufwand führen, darf HAIZOP eine angemessene Vergütung verlangen, sofern der Mehraufwand nicht auf einer Pflichtverletzung von HAIZOP beruht.
- (5) Der Auftragnehmer informiert den Auftraggeber, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Der Auftragnehmer darf die Ausführung der betreffenden Weisung aussetzen, bis die Weisung bestätigt, geändert oder zurückgenommen wurde.
- (6) Weisungsberechtigt sind ausschließlich die in der Bestellübersicht oder in Anlage 2 benannten Personen des Auftraggebers. HAIZOP darf angemessene Authentifizierung und Nachweise der Weisungsberechtigung verlangen.

## **§ 5 Pflichten des Auftragnehmers**

- (1) Der Auftragnehmer verpflichtet sich, personenbezogene Daten nur im Rahmen dieses Auftragsverarbeitungsvertrags und der dokumentierten Weisungen zu verarbeiten.
- (2) Der Auftragnehmer verpflichtet die mit der Verarbeitung befassten Personen zur Vertraulichkeit oder stellt sicher, dass sie einer angemessenen gesetzlichen oder vertraglichen Verschwiegenheitspflicht unterliegen.
- (3) Der Auftragnehmer hält geeignete technische und organisatorische Maßnahmen nach Maßgabe der Datenschutz- und Sicherheitsanlage ein.
- (4) Der Auftragnehmer unterstützt den Auftraggeber nach Maßgabe dieses Auftragsverarbeitungsvertrags bei der Erfüllung datenschutzrechtlicher Pflichten.
- (5) Der Auftragnehmer legt personenbezogene Daten des Auftraggebers nicht ohne Berechtigung offen.
- (6) Der Auftragnehmer setzt Unterauftragnehmer nur nach Maßgabe dieses Auftragsverarbeitungsvertrags ein.
- (7) Der Auftragnehmer gibt personenbezogene Daten nach Ende der Verarbeitung nach Maßgabe dieses Auftragsverarbeitungsvertrags zurück oder löscht sie, soweit keine gesetzliche Aufbewahrungspflicht oder ein berechtigter Nachweiszweck entgegensteht.

## **§ 6 Technische und organisatorische Maßnahmen**

- (1) Die vom Auftragnehmer geschuldeten technischen und organisatorischen Maßnahmen ergeben sich aus der Datenschutz- und Sicherheitsanlage.
- (2) Die Datenschutz- und Sicherheitsanlage enthält ausschließlich die zum Zeitpunkt ihrer Einbeziehung vertraglich geschuldeten technischen und organisatorischen Maßnahmen.
- (3) Nicht in der Datenschutz- und Sicherheitsanlage aufgeführte geplante, vorbereitete oder optionale Maßnahmen sind nicht Vertragsbestandteil.
- (4) Der Auftragnehmer darf technische und organisatorische Maßnahmen ändern, wenn das vereinbarte Schutzniveau dadurch insgesamt nicht wesentlich unterschritten wird.
- (5) Wesentliche Änderungen mit nachteiliger Auswirkung auf das Schutzniveau teilt der Auftragnehmer dem Auftraggeber in Textform mit.
- (6) Kundenverwaltete Schlüssel, kundenspezifische Sicherheitsarchitekturen, gesonderte lokale Instanzen, private Cloud-Bereitstellungen oder über den Standardbetrieb hinausgehende Sicherheitsmaßnahmen sind nur geschuldet, wenn sie ausdrücklich vereinbart sind.

## **§ 7 Zugriff durch Personal und beauftragte Personen**

- (1) Zugriff auf personenbezogene Daten des Auftraggebers erhalten nur Personen, soweit dies für Bereitstellung, Betrieb, Wartung, Sicherheit, Support, Fehleranalyse, Abrechnung, Nachweisführung oder eine dokumentierte Weisung erforderlich ist.
- (2) Zugriffe erfolgen rollenbasiert und nach dem Grundsatz der Erforderlichkeit. Geteilte Konten, private Verbraucher-Konten, nicht freigegebene Werkzeuge und dauerhafte lokale Kopien von Kundendaten sind nicht Bestandteil der Standardverarbeitung.

(3) Personen mit Zugriff werden zur Vertraulichkeit verpflichtet und dürfen personenbezogene Daten des Auftraggebers nicht für eigene Zwecke, private Auswertungen, Weitergabe an Dritte, Training von KI-Modellen oder sonstige vertragsfremde Zwecke verwenden.

(4) Soweit Personen oder Dienstleister außerhalb des Europäischen Wirtschaftsraums Zugriff auf personenbezogene Daten des Auftraggebers erhalten können, erfolgt dies nur, soweit der Zugriff in diesem Auftragsverarbeitungsvertrag, der Datenschutz- und Sicherheitsanlage oder Anlage 3 beschrieben ist und die jeweils erforderlichen Drittlandmechanismen und Zugriffsbeschränkungen eingehalten werden.

(5) Der Auftragnehmer stellt sicher, dass Zugriffspersonen entweder seiner unmittelbaren Weisung und Vertraulichkeitspflicht unterliegen oder nach Maßgabe der Regelungen zu Unterauftragnehmern einbezogen sind.

## **§ 8 KI-gestützte Verarbeitung**

(1) Die Plattform kann KI-gestützte Funktionen enthalten, soweit diese in der Leistungsbeschreibung beschrieben oder in der Bestellübersicht vereinbart sind.

(2) Personenbezogene Daten des Auftraggebers dürfen durch KI-gestützte Funktionen nur verarbeitet werden, soweit dies zur Erbringung der vereinbarten Plattformleistungen erforderlich ist.

(3) Der Auftragnehmer verwendet personenbezogene Daten des Auftraggebers, Kundendokumente, Prompts, Eingaben, Ausgaben oder sonstige Kundeninhalte nicht zum Training, zur Feinabstimmung oder zur Verbesserung von KI-Grundmodellen, soweit hierfür keine gesonderte ausdrückliche Vereinbarung besteht.

(4) Einzelheiten zu eingesetzten KI-Diensten, Unterauftragnehmern, Datenflüssen und Drittlandbezügen ergeben sich aus der Datenschutz- und Sicherheitsanlage.

## **§ 9 Unterstützung bei Betroffenenrechten**

(1) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren und technisch Möglichen bei der Erfüllung von Anfragen betroffener Personen.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer und betrifft die Anfrage eine Verarbeitung im Auftrag des Auftraggebers, leitet der Auftragnehmer die Anfrage an den Auftraggeber weiter, soweit eine Zuordnung möglich ist.

(3) Der Auftragnehmer beantwortet solche Anfragen nicht eigenständig, soweit er hierzu nicht gesetzlich verpflichtet ist.

## **§ 10 Unterstützung bei Sicherheitspflichten**

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei dessen Pflichten zur Sicherheit der Verarbeitung, zur Meldung von Datenschutzverletzungen und zu Datenschutz-Folgenabschätzungen.

(2) Soweit Unterstützungsleistungen über die vertraglich geschuldete Leistung hinausgehen, darf HAIZOP eine angemessene Vergütung verlangen, sofern der Unterstützungsbedarf nicht auf einer Pflichtverletzung von HAIZOP beruht.

## **§ 11 Datenschutzverletzungen**

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich nach Bekanntwerden, möglichst innerhalb von 24 Stunden, über Verletzungen des Schutzes personenbezogener Daten, soweit diese personenbezogene Daten des Auftraggebers betreffen.

(2) Die Mitteilung enthält, soweit verfügbar: Art der Verletzung, betroffene Datenkategorien, betroffene Personengruppen, voraussichtliche Folgen, ergriffene oder vorgeschlagene Maßnahmen sowie einen Ansprechpartner für Rückfragen.

(3) Sind zum Zeitpunkt der Erstmeldung noch nicht alle Informationen verfügbar, übermittelt der Auftragnehmer weitere Informationen ohne unangemessene Verzögerung nach.

(4) Meldungen an Aufsichtsbehörden oder betroffene Personen nimmt der Auftragnehmer für den Auftraggeber nur nach dokumentierter Weisung des Auftraggebers vor, soweit keine gesetzliche Pflicht des Auftragnehmers entgegensteht.

## **§ 12 Unterauftragnehmer**

- (1) Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz von Unterauftragnehmern, soweit diese in der Datenschutz- und Sicherheitsanlage oder in Anlage 3 dieses Auftragsverarbeitungsvertrags aufgeführt sind.
- (2) Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen bei Unterauftragnehmern, insbesondere über deren Hinzunahme oder Ersetzung.
- (3) Der Auftraggeber kann einer Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Kalendertagen nach Zugang der Mitteilung widersprechen.
- (4) Widerspricht der Auftraggeber berechtigt und kann keine angemessene Lösung gefunden werden, ist jede Partei berechtigt, den von der Änderung betroffenen Leistungsteil außerordentlich zu kündigen.
- (5) Der Auftragnehmer verpflichtet Unterauftragnehmer vertraglich auf Datenschutzpflichten, die den Pflichten dieses Auftragsverarbeitungsvertrags im Wesentlichen entsprechen.
- (6) HAZOP bleibt gegenüber dem Auftraggeber nach Maßgabe der gesetzlichen Vorschriften und der vertraglichen Haftungsregelungen für die Einhaltung der datenschutzrechtlichen Pflichten der eingesetzten Unterauftragnehmer verantwortlich.
- (7) Eigenständig Verantwortliche, Zahlungsdienstleister, Kommunikationsdienste, Berater, Banken, Behörden und kundenseitig aktivierte Integrationen sind nicht allein deshalb Unterauftragnehmer, weil sie im Zusammenhang mit der Vertragsdurchführung Daten erhalten oder verarbeiten.

## **§ 13 Drittlandübermittlungen**

- (1) Eine Übermittlung personenbezogener Daten in ein Land außerhalb des Europäischen Wirtschaftsraums erfolgt nur, soweit die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- (2) Drittlandbezüge können sich insbesondere aus dem Einsatz von Cloud-, KI-, Support-, Kommunikations- oder sonstigen Unterauftragnehmern sowie aus autorisierten Zugriffen durch Personen außerhalb des Europäischen Wirtschaftsraums ergeben.
- (3) Einzelheiten zu Drittlandbezügen, eingesetzten Unterauftragnehmern, Datenverarbeitungsorten, Zugriffsorten und eingesetzten Garantien ergeben sich aus der Datenschutz- und Sicherheitsanlage, Anlage 3 sowie der jeweils gesondert geführten SCC- und Transferdokumentation. Soweit Standardvertragsklauseln, Transferprüfungen oder zusätzliche Schutzmaßnahmen erforderlich sind, werden diese gesondert dokumentiert oder in der Datenschutz- und Sicherheitsanlage ausgewiesen.
- (4) Soweit sich Drittlandbezüge ändern, informiert der Auftragnehmer den Auftraggeber nach Maßgabe der Regelungen zu Unterauftragnehmern.

## **§ 14 Kontroll- und Nachweisrechte**

- (1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage angemessene Informationen zur Verfügung, die zur Prüfung der Einhaltung dieses Auftragsverarbeitungsvertrags erforderlich sind.
- (2) Die Nachweiserbringung erfolgt vorrangig durch digitale Dokumentationen, elektronische Nachweise, technische Beschreibungen, Sicherheitsinformationen, Unterauftragnehmerinformationen, geeignete Berichte, Zertifikate, Auskünfte oder sonstige geeignete Unterlagen, soweit diese zur Prüfung erforderlich und verfügbar sind.
- (3) Soweit digitale oder dokumentenbasierte Nachweise zur Klärung eines konkreten berechtigten Prüfungsanlasses nicht ausreichen, kann der Auftraggeber eine strukturierte Remote-Prüfung, insbesondere durch schriftliche Rückfragen, Videotermin oder Einsichtnahme in geeignete Nachweise, verlangen.
- (4) Vor-Ort-Kontrollen sind nur zulässig, wenn digitale oder dokumentenbasierte Nachweise sowie eine Remote-Prüfung zur Klärung eines konkreten berechtigten Prüfungsanlasses nicht ausreichen und die Kontrolle mit angemessener Vorankündigung während der üblichen Geschäftszeiten durchgeführt wird.
- (5) Kontrollen dürfen Betriebs- und Geschäftsgeheimnisse, Sicherheitsinteressen, Rechte Dritter, Rechte anderer Kunden und den Schutz personenbezogener Daten anderer Kunden nicht unangemessen beeinträchtigen. Ein Anspruch auf Einsicht in Quellcode, nicht offengelegte Sicherheitsarchitekturen, vollständige Cloud-Verwaltungskonsolen, Zugangsdaten, Schlüssel, Secrets, interne Schwachstelleninformationen oder Daten anderer Kunden besteht nicht.

(6) Soweit Nachweise oder Kontrollen Unterauftragnehmer, Cloud-Dienstleister oder sonstige Dritte betreffen, erfolgt der Nachweis vorrangig durch die von diesen bereitgestellten Vertragsunterlagen, Sicherheitsinformationen, Zertifikate, Auditberichte oder sonstigen geeigneten Nachweise. Ein unmittelbares Prüfungsrecht des Auftraggebers bei Unterauftragnehmern oder deren Rechenzentren besteht nur, soweit dies gesetzlich zwingend erforderlich oder ausdrücklich gesondert vereinbart ist.

(7) Beauftragt der Auftraggeber einen Dritten mit einer Kontrolle, hat er diesen vorab zur Vertraulichkeit zu verpflichten. Wettbewerber von HAIZOP sowie Personen, bei denen ein berechtigter Zweifel an Unabhängigkeit, Vertraulichkeit oder fachlicher Eignung besteht, dürfen nicht mit Kontrollen beauftragt werden.

## **§ 15 Rückgabe und Löschung**

(1) Nach Ende der Erbringung der Verarbeitungsleistungen gibt der Auftragnehmer personenbezogene Daten des Auftraggebers nach dokumentierter Weisung zurück oder löscht sie, soweit keine gesetzliche Pflicht zur weiteren Speicherung, kein zur Vertragsdurchführung, Abrechnung, Sicherheit, Rechtsverteidigung oder gesetzlichen Nachweispflicht erforderlicher Nachweiszweck und kein dokumentierter Legal-Hold-Grund entgegensteht.

(2) Soweit Nachweis-, Audit-, Sicherheits-, Rechtsverteidigungs- oder Legal-Hold-Zwecke eine weitere Speicherung erfordern, beschränkt HAIZOP die weitere Verarbeitung auf das hierfür erforderliche Maß. Soweit möglich, werden vollständige Inhaltsdaten vermieden und stattdessen Metadaten, Hashwerte, Zeitstempel, Versionsstände, Exportprotokolle oder sonstige geeignete Nachweisdaten verwendet.

(3) Nach Vertragsende steht dem Auftraggeber für einen Zeitraum von 90 Kalendertagen eine technisch verfügbare Exportmöglichkeit für die in der Plattform noch vorhandenen personenbezogenen Daten zur Verfügung, soweit in den SaaS-Vertragsbedingungen oder der Bestellübersicht nichts Abweichendes vereinbart ist.

(4) Erfolgt innerhalb des Exportfensters keine abweichende Weisung des Auftraggebers, ist der Auftragnehmer berechtigt, personenbezogene Daten nach Maßgabe der Vertragsdokumente zu löschen.

(5) Aktive Kundendaten werden grundsätzlich innerhalb von 90 Kalendertagen nach Vertragsende in den Löschprozess aufgenommen. Soweit die Löschung oder Anonymisierung einzelner Datenkategorien nicht vollautomatisiert erfolgt, wird sie nach dem dokumentierten Löschprozess durchgeführt.

(6) Sicherungskopien werden nach den in der Datenschutz- und Sicherheitsanlage dokumentierten Löschzyklen gelöscht, überschrieben oder außer Betrieb genommen, soweit keine gesetzliche Pflicht zur weiteren Speicherung besteht.

(7) Gesetzliche Aufbewahrungspflichten, Zahlungs-, Steuer-, Abrechnungs-, Audit-, Sicherheits- und Nachweiszwecke bleiben unberührt, soweit HAIZOP die betreffenden Daten nicht mehr als Auftragsverarbeiter, sondern in eigener Verantwortlichkeit oder aufgrund gesetzlicher Pflichten verarbeitet.

## **§ 16 Mitwirkung des Auftraggebers**

(1) Der Auftraggeber ist verantwortlich für die Rechtmäßigkeit der Verarbeitung, die Zulässigkeit der in die Plattform eingebrachten Daten, die Information betroffener Personen, die Erfüllung eigener Dokumentations- und Nachweispflichten, die Erteilung rechtmäßiger Weisungen und die Prüfung, ob die Plattform für die vom Auftraggeber beabsichtigten Verarbeitungsvorgänge geeignet ist.

(2) Der Auftraggeber darf keine personenbezogenen Daten in die Plattform einbringen, deren Verarbeitung für den vereinbarten Leistungszweck nicht erforderlich oder nicht zulässig ist.

(3) Der Auftraggeber ist verantwortlich für die ordnungsgemäße Verwaltung seiner Nutzer, Rollen, Berechtigungen und internen Zugriffskonzepte.

## **§ 17 Haftung**

(1) Die Haftung der Parteien im Zusammenhang mit diesem Auftragsverarbeitungsvertrag richtet sich nach den gesetzlichen Vorschriften und den zwischen den Parteien vereinbarten Haftungsregelungen, soweit diese wirksam anwendbar sind.

(2) Zwingende Ansprüche betroffener Personen und zwingende datenschutzrechtliche Verantwortlichkeiten bleiben unberührt.

## § 18 Laufzeit

(1) Dieser Auftragsverarbeitungsvertrag gilt für die Dauer der Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

(2) Endet der Hauptvertrag, endet dieser Auftragsverarbeitungsvertrag, sobald keine personenbezogenen Daten mehr im Auftrag des Auftraggebers verarbeitet werden und alle Rückgabe-, Lösch-, Archivierungs- und Nachweispflichten erfüllt sind.

## § 19 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrags bedürfen der Textform, soweit keine strengere Form gesetzlich vorgeschrieben ist.

(2) Sollte eine Bestimmung dieses Auftragsverarbeitungsvertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Im Übrigen gelten die Schlussbestimmungen des Hauptvertrags, soweit dieser Auftragsverarbeitungsvertrag keine vorrangige Regelung enthält.

### Vertragsparteien

| Rolle         | Angaben                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------|
| Auftraggeber  | Der in der jeweiligen Bestellübersicht bezeichnete Kunde / Auftraggeber.                                 |
| Auftragnehmer | HAIZOP GmbH, Tschaikowskistraße 21, 04105 Leipzig, vertreten durch Christian Machens                     |
| Hauptvertrag  | SaaS-Vertragsbedingungen, Bestellübersicht und Leistungsbeschreibung in der jeweils einbezogenen Fassung |

### Anlage 1: Beschreibung der Verarbeitung

| Kategorie                                    | Beschreibung                                                                                                                                                                                                                                                                                        |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gegenstand der Verarbeitung                  | Bereitstellung, Betrieb, Wartung, Sicherheit, Fehleranalyse und Unterstützung bei der Nutzung der HAZOP-Plattform.                                                                                                                                                                                  |
| Zweck der Verarbeitung                       | Unterstützung des Auftraggebers bei HAZOP-bezogenen Arbeitsabläufen innerhalb der HAZOP-Plattform.                                                                                                                                                                                                  |
| Art der Verarbeitung                         | Erheben, Erfassen, Organisieren, Ordnen, Speichern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Abgleichen, Einschränken, Löschen und Vernichten personenbezogener Daten, soweit dies zur Leistungserbringung erforderlich ist.                                                   |
| Kategorien personenbezogener Daten           | Nutzerstammdaten; Anmelde- und Berechtigungsdaten; Nutzungs-, Geräte-, Verbindungs-, Sicherheits- und Audit-Log-Daten; Support- und Kommunikationsdaten; Projekt- und Sitzungsdaten; personenbezogene Daten in Kundendokumenten, Analyseinhalten, Prompts, Eingaben und Ausgaben, soweit enthalten. |
| Kategorien betroffener Personen              | Nutzer des Auftraggebers; Ansprechpartner des Auftraggebers; Teilnehmer dokumentierter Sitzungen; Beschäftigte oder Beauftragte des Auftraggebers; sonstige Personen, deren Daten der Auftraggeber in die Plattform einbringt.                                                                      |
| Besondere Kategorien personenbezogener Daten | Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nicht Zweck der HAZOP-Plattform. Bringt der Auftraggeber solche Daten dennoch ein, bleibt er für deren Rechtmäßigkeit, Erforderlichkeit und Zulässigkeit verantwortlich.                                                         |

## Eigenständige Verarbeitungen von HAIZOP

| Verarbeitung                                                  | Beschreibung                                                                                                                                                                                                      |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vertragskontakt- und Kommunikationsdaten                      | Kommunikation mit Ansprechpartnern des Kunden zur Vertragsanbahnung, Vertragsdurchführung und Vertragsverwaltung.                                                                                                 |
| Abrechnungs- und Zahlungsdaten                                | Rechnungsadresse, Vertragsbezug, Zahlungsstatus, buchhalterische Daten und gesetzlich aufbewahrungspflichtige Unterlagen.                                                                                         |
| Gesetzliche Nachweise                                         | Daten, die HAIZOP aufgrund gesetzlicher Aufbewahrungs-, Nachweis- oder Mitwirkungspflichten verarbeitet.                                                                                                          |
| Sicherheits- und Betriebsdaten ohne vollständige Inhaltsdaten | Technische Sicherheits-, Stabilitäts-, Missbrauchs- und Betriebsdaten, soweit HAIZOP diese zur eigenen System- und Informationssicherheit verarbeitet und keine vollständigen inhaltlichen Kundendaten verwendet. |

## Anlage 2: Weisungsberechtigte Personen

| Regelung                     | Beschreibung                                                                                                                                                                                                                                                                                                                                                                          | Status                                                                      |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Weisungsberechtigte Personen | Weisungsberechtigt sind die in der Bestellübersicht benannten Personen des Auftraggebers. Fehlt eine Benennung in der Bestellübersicht, sind die vom Auftraggeber in Textform benannten administrativen Hauptkontakte oder Datenschutz-/Sicherheitskontakte weisungsberechtigt. HAIZOP darf eine angemessene Authentifizierung und einen Nachweis der Weisungsberechtigung verlangen. | Kundenbezogen in der Bestellübersicht oder per Textformbenennung zu führen. |

## Anlage 3: Unterauftragnehmer, Drittlandbezüge und Abgrenzungen

| Kategorie / Dienst / Zugriff                                    | Einordnung und Zweck                                                                                              | Daten / Drittlandbezug                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Teil A: Unterauftragnehmer</b>                               |                                                                                                                   |                                                                                                                                                                                                                                                                                                 |
| Google Ireland Limited / Google Cloud Platform                  | Hosting, Datenbank, Speicher, Logging, Monitoring, Secret-Verwaltung, Deployment-Artefakte und Backups.           | Standardbetrieb für zentrale produktive Plattformkomponenten nach aktueller technischer Bestätigung in der Google-Cloud-Region europe-west3, Frankfurt am Main, Deutschland; mögliche Google-/Subprozessor- und Supportzugriffe außerhalb EU/EWR nach Google-Vertrags- und Transfermechanismen. |
| Google Ireland Limited / Google Cloud Vertex AI / Google Gemini | KI-Inferenz im Rahmen der vereinbarten Plattformfunktionen.                                                       | Vertex-AI-/Gemini-Location eu nach aktueller Konfiguration; Kundendaten, Prompts und Ausgaben werden nicht zum Training, Re-Training oder Fine-Tuning von KI-Grundmodellen genutzt, soweit keine gesonderte ausdrückliche Vereinbarung besteht.                                                 |
| Google Ireland Limited / Google Workspace und Gmail SMTP        | Kommunikations- und E-Mail-Dienst für Vertrags-, System-, Support- und Kommunikationsprozesse, soweit eingesetzt. | Kann Kommunikations- und Supportdaten betreffen; Drittlandbezüge nach Google-Vertrags- und Transfermechanismen.                                                                                                                                                                                 |

| Kategorie / Dienst / Zugriff                                 | Einordnung und Zweck                                                                                                                   | Daten / Drittlandbezug                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HAIZOP Odoo Helpdesk/CRM und zugrunde liegende Infrastruktur | Support-, CRM-, Demo-, Kontakt- und Ticketprozesse über haizop.odoo.com; keine allgemeine Spiegelung von Plattform- oder Projektdaten. | Demo-, Support- und Kommunikationsdaten, soweit vom Kunden oder seinen Nutzern eingebracht. HAIZOP ist Vertragspartner und Rechnungsempfänger. Nach aktueller technischer Auskunft: Region EU-West3 / Europa.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Teil B: Autorisierte Drittlandzugriffe</b>                |                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Daniel Sebastian Schindowski, Guatemala                      | Persönlicher technischer Dienstleister für Entwicklung, Betrieb, Support, Sicherheit, Fehleranalyse und Incident-Unterstützung.        | Autorisierter technischer Drittlandzugriff auf personenbezogene Daten des Auftraggebers kann, soweit für die Leistungserbringung erforderlich, nach Maßgabe dieses Auftragsvertrags, der Datenschutz- und Sicherheitsanfrage, der gesonderten SCC- und Transferdokumentation und der freigegebenen Zugriffsmatrix erfolgen. Der Zugriff ist auf erforderliche technische Zwecke beschränkt; eine Weitergabe an weitere Personen oder Unternehmen, eine dauerhafte lokale Speicherung sowie eine Nutzung privater Werkzeuge sind ausgeschlossen. Für freigegebene interne Cloud-PC-Zugriffe ist MFA nach technischer Bestätigung aktiv. |
| <b>Teil C: Eigenständig Verantwortliche / Abgrenzungen</b>   |                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Stripe Payments Europe Ltd.                                  | Zahlungsdienstleister im Rahmen eigener Zahlungs- und Abrechnungsprozesse.                                                             | Nicht pauschal Unterauftragnehmer für Kunden-Plattformdaten. Verarbeitung richtet sich nach eigener Rollenverteilung und Zahlungsprozess.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Steuerberater, Rechtsberater, Banken, Behörden               | Empfänger im Rahmen gesetzlicher, vertraglicher, Abrechnungs-, Nachweis- oder Rechtsverfolgungszwecke.                                 | Keine Plattform-Unterauftragnehmer im Sinne des AVV.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Unterschriften

| Partei        | Unterschrift | Name / Funktion                    |
|---------------|--------------|------------------------------------|
| Auftraggeber  | _____        | Name / Funktion                    |
| Auftragnehmer | _____        | Christian Machens, Geschäftsführer |