Datenschutz- und Sicherheitsanlage

1. Zweck, Geltung und Abgrenzung

(1) Diese Anlage ergänzt die SaaS-Vertragsbedingungen, die Bestellübersicht, die Leistungsbeschreibung und den Auftragsverarbeitungsvertrag.

(2) Vertraglich geschuldet sind ausschließlich die in dieser Anlage ausdrücklich beschriebenen aktiven Maßnahmen, Verarbeitungsumgebungen, Dienste, Unterauftragnehmer, Zugriffskonzepte und Schutzmechanismen.

(3) Nicht in dieser Anlage aufgeführte Maßnahmen, Anbieter, Dienste, Funktionalitäten, Sicherheitszertifizierungen, Service-Level, Wiederherstellungszeiten, Wiederherstellungspunkte oder Verfügbarkeitsquoten sind nicht Vertragsbestandteil.

(4) Diese Anlage begründet keine Service-Level-Vereinbarung und keine bestimmte Verfügbarkeitsquote, Reaktionszeit, Bearbeitungszeit, Wiederherstellungszeit, Wiederherstellungspunkt oder Servicegutschrift.

(5) Geplante, vorbereitete oder optionale Maßnahmen sind nur dann vertraglich geschuldet, wenn sie ausdrücklich als aktive Standardmaßnahme in dieser Anlage oder in der Bestellübersicht bezeichnet werden.

(6) Kundendaten im Sinne dieser Anlage sind Kundendokumente, Plattformdaten, Projekt- und Sitzungsdaten, Eingaben, Prompts, Ausgaben, Metadaten und sonstige Inhalte oder Daten, die der Kunde oder seine Nutzer in die HAIZOP-Plattform einbringen oder die bei deren vertragsgemäßer Nutzung entstehen. Personenbezogene Daten sind hiervon nur solche Kundendaten, die personenbezogene Daten im Sinne der DSGVO enthalten.

2. Standard-Verarbeitungsumgebung

(1) Die HAIZOP-Plattform wird als internetbasierte Software bereitgestellt.

(2) Die Standardumgebung nutzt die in dieser Anlage aufgeführten Cloud-, Speicher-, Datenbank-, Sicherheits-, Kommunikations-, KI- und Supportdienste.

(3) Die Standardplattform ist auf eine Verarbeitung in europäischen Verarbeitungsräumen ausgerichtet, soweit dies nach den eingesetzten Diensten und deren Vertragsbedingungen möglich ist.

(4) Kundenspezifische lokale Installationen, private Cloud-Bereitstellungen, gesonderte Mandantenarchitekturen, kundenverwaltete Schlüssel oder abweichende Sicherheitsarchitekturen sind nicht Bestandteil des Standards und bedürfen einer gesonderten Vereinbarung.

3. Zugriffsschutz und Berechtigungen

(1) HAIZOP nutzt individuelle Benutzerkennungen für Nutzerkonten und interne Zugriffe.

(2) Zugriffe werden rollenbasiert und nach dem Grundsatz der Erforderlichkeit vergeben.

(3) Zugriffsrechte sind bei Wegfall des Bedarfs zu entziehen oder anzupassen.

(4) Administrations-, Entwicklungs-, Support- und Betriebszugriffe werden nach Zweck und Berechtigung getrennt, soweit dies in der jeweiligen Umgebung technisch vorgesehen ist.

(5) Vertriebsrollen erhalten keinen standardmäßigen administrativen Zugriff auf Kundendaten.

(6) Interne Zugriffe auf Kundendaten dürfen nur über individuell zugeordnete HAIZOP-, Cloud-, Support-, Odoo-, Workspace- oder Plattformkonten und freigegebene Arbeitsumgebungen erfolgen. Private Verbraucher-Konten, geteilte Konten, weitergegebene Tokens und nicht freigegebene Werkzeuge sind ausgeschlossen.

4. Mehr-Faktor-Authentifizierung und Geräteschutz

(1) Für produktive Plattformnutzer mit erhöhten oder bearbeitenden Berechtigungen sowie für interne Administrations-, Cloud-, Secret-, Support- und Plattformzugriffe ist Mehr-Faktor-Authentifizierung vorgesehen und, soweit technisch durchgesetzt, verpflichtend. Für freigegebene interne Cloud-PC-Zugriffe ist Mehr-Faktor-Authentifizierung nach technischer Bestätigung aktiv.

(2) Unterstützt werden insbesondere zeitbasierte Einmalpasswörter und Passkey/WebAuthn. Für besonders berechtigte Administrations- und Owner-Zugriffe ist Passkey oder Hardware-Security-Key als stärkerer Faktor vorgesehen; mindestens zeitbasierte Einmalpasswörter bleiben während Rollout- und Wiederherstellungssituationen zulässig.

(3) Geschützte Plattform- und API-Kontexte können einen frischen Mehr-Faktor-Nachweis verlangen. Die aktuelle Step-up-Gültigkeit beträgt nach technischer Konfiguration zwei Stunden.

(4) Interne Arbeitsumgebungen mit Zugriff auf Kundendaten müssen durch individuelle Anmeldung, Bildschirmsperre, angemessene Sicherheitsupdates und verschlüsselte lokale Speicherung oder vergleichbare Schutzmaßnahmen abgesichert sein.

5. Mandantentrennung

(1) Kundendaten werden logisch nach Organisationen, Mandanten, Projekten und Ressourcen getrennt.

(2) Zugriffe innerhalb der Plattform werden anhand von Organisations-, Rollen- und Ressourcenberechtigungen geprüft.

(3) Eine Nutzung von Kundendaten eines Kunden für einen anderen Kunden findet nicht statt.

(4) KI-Aufrufe werden innerhalb der jeweils zugeordneten Organisation oder Verarbeitungseinheit ausgeführt. Eine kundenübergreifende Nutzung von Kundendaten im Rahmen der KI-Verarbeitung ist ausgeschlossen.

6. Verschlüsselung, Geheimhaltung und Schutz von Zugangsdaten

(1) Verbindungen zur Plattform und zu vertraglich eingebundenen Diensten werden transportverschlüsselt, soweit die jeweilige Verbindung dies technisch unterstützt.

(2) Ruhende Daten in Google Cloud SQL und Google Cloud Storage werden mit der plattformseitigen Google-Cloud-Verschlüsselung geschützt.

(3) HAIZOP verschlüsselt 2FA-Secrets und hierfür vorgesehene sensitive Anwendungsfelder anwendungsseitig mit AES-256-GCM.

(4) Produktive Backups werden vor der Ablage im vorgesehenen Backup-Speicher GPG-verschlüsselt, soweit die Backup-Pipeline hierfür eingesetzt wird.

(5) Produktive Laufzeit- und Betriebssecrets werden nicht im Repository gespeichert. Dazu gehören insbesondere Datenbankverbindungen, Authentifizierungs- und Sitzungsschlüssel, 2FA- und Feldverschlüsselungsschlüssel, Cron-Secrets sowie Backup- und Restore-Schlüssel.

(6) Secrets werden über Google Secret Manager oder die vorgesehenen Stage- und Deployment-Secrets verwaltet. Cloud-Run-Runtime-Service-Accounts erhalten nur stagebezogenen Zugriff auf die jeweils benötigten Secrets.

(7) Kundenverwaltete KMS-Schlüssel sind nicht Teil des Standardbetriebs und werden nur bei gesonderter Vereinbarung geschuldet.

7. Protokollierung und Nachvollziehbarkeit

(1) HAIZOP verarbeitet sicherheits-, betriebs- und nachweisrelevante Protokolldaten, soweit dies für Betrieb, Sicherheit, Fehleranalyse, Missbrauchserkennung, Nachvollziehbarkeit, Abrechnung, Auditierung oder Vertragserfüllung erforderlich ist.

(2) Erfasst werden insbesondere Plattform-Zugriffslogs, strukturierte Anwendungs- und Prozesslogs, Google-Cloud-Audit-Logs, Anwendungs-Audit-Trail, Login- und Geräte-Sicherheitslogs, Security Events, technische KI- und Workflow-Metadaten, Analysis-Run-Ledger, Webhook-Zustelllogs, Backup-/Restore-Nachweise, Queue-/Analysejob-Protokolle, Support-/Security-Tickets sowie Billing-/Provider-Ereignisse, soweit diese im Standardbetrieb anfallen.

(3) Vollständige Prompts, vollständige Roh-Outputs oder vertrauliche Kundendaten werden nicht regulär in eigenen Debug-, Fehler-, Support- oder Telemetrie-Logs gespeichert, außer dies ist ausdrücklich dokumentiert oder für eine konkrete Supportanalyse freigegeben und vom Vertragszweck gedeckt.

(4) Einzelheiten zu Logarten, Zweck, Datenkategorien und Speicherfristen ergeben sich aus der Tabelle „Protokollierung und Speicherfristen“.

8. Supportzugriffe

(1) Interne Zugriffe von HAIZOP auf Kundendaten erfolgen nur, soweit sie für Support, Fehleranalyse, Sicherheit, Wartung, Betrieb, Wiederherstellung, Nachweisführung oder Vertragsdurchführung erforderlich sind.

(2) Supportzugriffe sind auf berechtigte Personen zu beschränken und erfolgen über freigegebene Konten und Arbeitsumgebungen.

(3) Anlass, Umfang und Bearbeitung von Support- und Sicherheitszugriffen werden angemessen dokumentiert, soweit dies technisch und organisatorisch vorgesehen ist.

(4) Odoo wird für CRM-/Helpdesk-Prozesse, Demo-/Kontaktanfragen und Supporttickets eingesetzt. Eine allgemeine Spiegelung von Plattform- oder Projektdaten nach Odoo findet nicht statt.

9. KI-gestützte Verarbeitung

(1) HAIZOP setzt KI-gestützte Funktionen nur im Rahmen der vertraglich vereinbarten Plattformleistungen ein.

(2) Zum Stand dieser Anlage wird für produktive KI-Inferenz der Standardplattform Google Cloud Vertex AI / Google Gemini über Google Cloud eingesetzt.

(3) Die Standardkonfiguration ist auf EU-Verarbeitung ausgerichtet. Die konkret eingesetzte Location für Google Cloud Vertex AI / Google Gemini ergibt sich aus der nachstehenden Unterauftragnehmer- und Verarbeitungsübersicht.

(4) Kundendaten, Kundendokumente, Prompts, Eingaben, Ausgaben und sonstige Kundeninhalte werden von HAIZOP nicht zum Training, Re-Training, zur Feinabstimmung oder zur Verbesserung von KI-Grundmodellen verwendet, sofern keine gesonderte ausdrückliche Vereinbarung besteht.

(5) HAIZOP verarbeitet Kundendaten nicht über private KI-Zugänge, Verbraucherzugänge oder nicht vertraglich eingebundene KI-Dienste.

(6) Nicht ausdrücklich in dieser Anlage als aktive Standardverarbeitung aufgeführte KI-, OCR- oder Dokumentenverarbeitungsdienste sind nicht Bestandteil der produktiven Standardverarbeitung.

10. Drittlandbezüge und Zugriff außerhalb des Europäischen Wirtschaftsraums

(1) HAIZOP richtet die Standardverarbeitung auf europäische Verarbeitungsräume oder die in dieser Anlage bezeichneten Regionen aus.

(2) Drittlandbezüge können sich insbesondere aus Google-Cloud-Vertrags- und Supportstrukturen, Google-Subprozessoren, Google Workspace / Gmail SMTP, Google Vertex AI / Gemini sowie autorisierten Support-, Entwicklungs-, Betriebs- oder Administrationszugriffen außerhalb des Europäischen Wirtschaftsraums ergeben.

(3) Ein Zugriff auf Kundendaten aus Staaten außerhalb des Europäischen Wirtschaftsraums darf nur durch vorab autorisierte, zur Vertraulichkeit verpflichtete und in die Weisungs- und Berechtigungsstruktur von HAIZOP eingebundene Personen erfolgen. Die jeweils zugriffsberechtigten Personen, Zugriffszwecke und Schutzmaßnahmen werden intern dokumentiert.

(4) Der Zugriff ist auf dokumentierte Zwecke wie Entwicklung, Betrieb, Support, Sicherheit, Fehleranalyse, Bearbeitung von Sicherheitsvorfällen, Wiederherstellung und dokumentierte Betriebsentscheidungen beschränkt. Eine Verarbeitung zu eigenen Zwecken, eine Weitergabe oder Zugänglichmachung an nicht autorisierte Dritte, die Nutzung nicht freigegebener Werkzeuge sowie Training, Re-Training, Feinabstimmung oder Verbesserung von KI-Modellen mit Kundendaten sind ausgeschlossen, soweit keine gesonderte ausdrückliche Vereinbarung besteht.

(5) Zugriffe außerhalb des Europäischen Wirtschaftsraums erfolgen nur über individuelle, verwaltete Konten, mit Mehr-Faktor-Authentifizierung, rollenbasierten Berechtigungen, dem Grundsatz der Erforderlichkeit und angemessener Protokollierung. Dauerhafte lokale Kopien von Kundendaten, Uploads, Datenbankauszügen, Protokolldaten oder Exporten außerhalb der freigegebenen HAIZOP-Verarbeitungsumgebung sind nicht Bestandteil der Standardverarbeitung und bedürfen einer ausdrücklichen Freigabe.

(6) Soweit für Drittlandbezüge geeignete Garantien erforderlich sind, werden die jeweils erforderlichen Transfermechanismen in dieser Anlage oder in der gesonderten SCC- und Transferdokumentation dokumentiert. Je nach Fall können hierzu insbesondere Angemessenheitsbeschlüsse, das EU-U.S. Data Privacy Framework, Standardvertragsklauseln, Transferprüfungen und ergänzende Schutzmaßnahmen gehören.

11. Rückgabe, Export, Archivierung, Löschung und Sicherungskopien

(1) Nach Vertragsende gelten die in den SaaS-Vertragsbedingungen, der Bestellübersicht und dem Auftragsverarbeitungsvertrag vereinbarten Rückgabe-, Export-, Archivierungs- und Löschregelungen.

(2) Der Standard sieht ein 90-tägiges Exportfenster für technisch verfügbare wesentliche HAIZOP-Projekt- und Report-Exportfunktionen vor.

(3) 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.

(4) Während einer Auslese-, Archivierungs- oder Löschphase wird die Verarbeitung auf Rückgabe, Export, Archivierung, Löschung, Abwicklung, Sicherheit und Nachweiszwecke beschränkt.

(5) Nachweis- und Auditdaten zu Reports, Exporten, Freigaben, Analysevorgängen und wesentlichen Nutzerentscheidungen können nach Vertragsende gespeichert werden, soweit dies für Sicherheit, Nachvollziehbarkeit, Abrechnung, Auditierung, Rechtsverteidigung, Legal-Hold oder gesetzliche Nachweispflichten erforderlich ist. Vorrangig werden hierfür Metadaten, Hashwerte, Zeitstempel, Versionsstände, Statusinformationen und Audit-Trail-Einträge verwendet. Vollständige Inhaltsdaten oder Reportkopien werden nur gespeichert, soweit der jeweilige Zweck dies konkret erfordert.

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

12. Backup, Restore und Notfallprozesse

(1) Produktionsdaten werden nach aktueller technischer Konfiguration durch Google-Cloud-SQL-Backups und einen dedizierten Google-Cloud-Storage-Backup-Bucket gesichert.

(2) Nach aktueller technischer Bestätigung besteht im aktiven Google-Cloud-Projekt ein dedizierter Google-Cloud-Storage-Backup-Bucket mit der Bezeichnung haizop-backups-euw3-nomadic-tracker-497320-r6 in der Region europe-west3. Ein gesonderter Nachweis erfolgreicher produktiver Backup-Läufe wird intern dokumentiert.

(3) Cloud-SQL-Backups rotieren nach Anzahl. Zum Stand dieser Anlage bestehen 7 retained backups und 7 Tage Point-in-Time-Recovery für Produktion.

(4) Die Backup-Pipeline ist darauf ausgelegt, verschlüsselte Backups zu erzeugen und Restore-Prüfungen gegen eine temporäre PostgreSQL-Umgebung zu ermöglichen. Restore-Prozesse erfolgen nach aktueller Konfiguration mit Wiederherstellung in der Google-Cloud-Region europe-west3.

(5) Backup- und Restore-Angaben beschreiben Sicherheits- und Betriebsmaßnahmen. Sie begründen ohne gesondertes Service-Level-Agreement keine garantierten Wiederherstellungszeiten oder Wiederherstellungspunkte.

13. Sicherheitsvorfälle und Sicherheitskontakt

(1) HAIZOP unterhält einen internen Prozess zur Bewertung, Bearbeitung und Dokumentation sicherheitsrelevanter Vorfälle.

(2) Verletzungen des Schutzes personenbezogener Daten werden nach Maßgabe des Auftragsverarbeitungsvertrags an den Kunden gemeldet.

(3) Security-Alerting, Backup-/Restore-Auditierung und ein dokumentierter Incident-Response-Prozess mit Eskalationswegen, Sicherheitsansprechpartner und Notfallweg außerhalb üblicher Geschäftszeiten sind vorgesehen.

(4) Als Sicherheitskontakt ist security@haizop.de vorgesehen.

14. Aktualisierung dieser Anlage

(1) HAIZOP darf technische und organisatorische Maßnahmen ändern, wenn das vereinbarte Schutzniveau dadurch insgesamt nicht wesentlich unterschritten wird.

(2) Wesentliche Änderungen mit nachteiliger Auswirkung auf das Schutzniveau, Änderungen von Unterauftragnehmern oder Änderungen von Drittlandbezügen richten sich nach dem Auftragsverarbeitungsvertrag.

(3) Eine aktualisierte Fassung dieser Anlage wird Vertragsbestandteil, wenn sie nach Maßgabe der Vertragsdokumente wirksam einbezogen wird.

Standardverarbeitung und Verarbeitungsräume

Bereich	Standardverarbeitung	Verarbeitungsraum / Region
Plattformbetrieb	Cloud-Infrastruktur, Anwendungskomponenten, Datenbank-, Speicher-, Sicherheits- und Plattformdienste.	Google Cloud; zentrale produktive Plattformkomponenten nach aktueller technischer Bestätigung in der Google-Cloud-Region europe-west3, Frankfurt am Main, Deutschland, soweit nach Dienst und Konfiguration anwendbar.
Dateiablage	Speicherung hochgeladener Kundendokumente und zugehöriger Metadaten in privaten, stage-getrennten Buckets.	Google Cloud Storage; Region europe-west3, Frankfurt am Main, Deutschland, nach aktueller produktiver Konfiguration; Uniform Bucket-Level Access und Public Access Prevention.
Datenbank	Produktive Plattformdatenbank und automatische Datenbank-Backups.	Google Cloud SQL; Retention und Point-in-Time-Recovery nach technischer Konfiguration.
KI-Inferenz	KI-gestützte Verarbeitung für vertraglich beschriebene Plattformfunktionen.	Google Cloud Vertex AI / Google Gemini; Vertex-AI-/Gemini-Location eu nach aktueller Standardkonfiguration.
Backups	Verschlüsselte logische Offsite-Backups und Backup-/Restore-Nachweise.	Google-Cloud-SQL-Backups sowie dedizierter Google-Cloud-Storage-Backup-Bucket haizop-backups-euw3-nomadic-tracker-497320-r6 in der Region europe-west3; Backup-Laufnachweise werden intern dokumentiert.

Aktive technische und organisatorische Maßnahmen

Bereich	Aktive Standardmaßnahme
Zugriff	Individuelle Konten, rollenbasierte Berechtigungen, Erforderlichkeitsprinzip, Entzug von Rechten bei Wegfall des Bedarfs. Privilegierte administrative Zugriffe sind auf namentlich berechtigte Personen zu beschränken, zweckgebunden zu nutzen und regelmäßig zu überprüfen.

Bereich	Aktive Standardmaßnahme
Mehr-Faktor-Authentifizierung	MFA für produktive Nutzerrollen mit erhöhten oder bearbeitenden Berechtigungen und interne Administrations-, Cloud-, Secret-, Support- und Plattformzugriffe, soweit technisch durchgesetzt. Für freigegebene interne Cloud-PC-Zugriffe ist MFA nach technischer Bestätigung aktiv.
Mandantentrennung	Logische Trennung nach Organisationen, Mandanten, Projekten und Ressourcen; keine kundenübergreifende Nutzung von Kundendaten.
Transportverschlüsselung	Transportverschlüsselte Verbindungen zur Plattform und zu eingebundenen Diensten, soweit technisch unterstützt.
Verschlüsselung ruhender Daten	Google-Cloud-plattformseitige Verschlüsselung für Cloud SQL und Cloud Storage.
Anwendungsseitige Verschlüsselung	AES-256-GCM für 2FA-Secrets und hierfür vorgesehene sensitive Anwendungsfelder.
Backups	GPG-verschlüsselte produktive Backups vor Ablage im vorgesehenen Backup-Speicher, soweit die Backup-Pipeline hierfür eingesetzt wird.
Secrets	Verwaltung produktiver Laufzeit- und Betriebssecrets über Google Secret Manager bzw. Stage- und Deployment-Secrets; keine Speicherung produktiver Secrets im Repository.
Geräteschutz	Freigegebene Arbeitsumgebungen mit individueller Anmeldung, Bildschirmsperre, angemessenen Updates und verschlüsselter lokaler Speicherung oder vergleichbarem Schutz.
Supportzugriffe	Zweckgebundene, rollenbeschränkte und angemessen dokumentierte interne Zugriffe für Support, Fehleranalyse, Sicherheit, Wartung, Betrieb und Wiederherstellung.

Protokollierung und Speicherfristen

Log- oder Nachweiskategorie	Typischer Inhalt	Standardfrist / Löschlogik
Google Cloud Logging _Default	Technische Cloud-, Anwendungs-, Prozess- und Betriebslogs, soweit in _Default geführt.	30 Tage nach aktueller zentraler Konfiguration.
Google Cloud Logging _Required	Von Google verpflichtend geführte Cloud-Audit- und Administrationslogs.	400 Tage nach aktueller Google-Cloud-Konfiguration.
Anwendungs-Audit-Trail	Zentrale Workflow-Ereignisse wie KI-Analyse, Freigaben, Exporte, Uploads, Statuswechsel und administrative Operationsereignisse.	Je nach Kategorie 365 Tage oder bis zu 10 Jahre, soweit Audit-, Sicherheits-, Abrechnungs-, Steuer- oder Nachweiszwecke dies erfordern.
KI- und Workflow-Metadaten	Technische KI- und Workflow-Metadaten, Modell-/Provider-Informationen, Task-Typen, Prompt-Versionen, Erfolgs-/Fehlerstatus.	Standardmäßig 365 Tage; Fehler- und Debugtextfelder werden standardmäßig nach 30 Tagen redigiert.
Security Events	Sicherheitsereignisse, Login-/Geräteinformationen, Missbrauchs- oder Incident-Indikatoren.	In Prozesslogs grundsätzlich 30 Tage, soweit sie nicht zusätzlich als Audit-, Support- oder Incident-Nachweis persistiert werden.
Backup-/Restore-Nachweise	Backup-Läufe, Restore-Validierungen, technische Nachweise zur Wiederherstellung.	Nach Sicherheits-, Audit- und Nachweiszweck, je nach Kategorie 365 Tage oder bis zu 10 Jahre.
Support- und Security-Tickets	Supportanfragen, Security-Hinweise, technische Kommunikation und Bearbeitungsnachweise.	Nach Vorgangs-, Nachweis-, Abrechnungs- und Aufbewahrungszweck; keine allgemeine Spiegelung von Plattform- oder Projektdaten nach Odoo.

Backup und Löschzyklen

Datenbereich	Regelung
90-Tage-Exportfenster	Für wesentliche HAIZOP-Projekt- und Report-Exportfunktionen technisch umgesetzt und produktiv deployt; Exportmöglichkeit nach Vertragsende für 90 Kalendertage nach Maßgabe der Vertragsdokumente.

Datenbereich	Regelung
Aktive Kundendaten	Aufnahme in den Löschprozess grundsätzlich innerhalb von 90 Kalendertagen nach Vertragsende; Löschung oder Anonymisierung nach dokumentiertem Löschprozess.
Google Cloud SQL Backups	Derzeit 7 retained backups und 7 Tage Point-in-Time-Recovery für Produktion.
Offsite-Backups	Dedizierter Google-Cloud-Storage-Backup-Bucket haizop-backups-euw3-nomadic-tracker-497320-r6 in der Region europe-west3. Produktive Retention und Backup-Laufnachweise werden intern dokumentiert.
Restore-Test	Ein Restore-Test der aktiven Production-Offsite-Pipeline wurde am 16. Juni 2026 erfolgreich durchgeführt.
Wiederherstellungszeit / Wiederherstellungspunkt	Keine vertragliche Standardzusage von Wiederherstellungszeit oder Wiederherstellungspunkt ohne gesondertes Service-Level-Agreement.

Unterauftragnehmer, Empfänger und Abgrenzungen

Dienst / Empfänger	Einordnung und Zweck	Drittlandbezug / Hinweis
Google Ireland Limited / Google Cloud Platform	Unterauftragnehmer für Hosting, Datenbank, Speicher, Logging, Monitoring, Secret-Verwaltung, Deployment-Artefakte und Backups.	Standardbetrieb mit EU-/EWR-Bezug nach Konfiguration; mögliche Google-/Subprozessor- und Supportzugriffe außerhalb EU/EWR nach Google-Vertrags- und Transfermechanismen.
Google Ireland Limited / Google Cloud Vertex AI / Google Gemini	Unterauftragnehmer für KI-Inferenz im Rahmen der vereinbarten Plattformfunktionen.	Location eu nach aktueller Konfiguration; Kundendaten, Prompts und Outputs werden nicht zum Training, Re-Training oder Fine-Tuning von KI-Grundmodellen genutzt.
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.
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.
Autorisierter technischer Drittlandzugriff durch in Anlage 3 des AVV ausgewiesene Person(en)	Zweckgebundener technischer Zugriff für Entwicklung, Betrieb, Support, Sicherheit, Fehleranalyse oder Unterstützung bei Sicherheitsvorfällen.	Zugriff nur nach dokumentierten Vorgaben von HAIZOP und nach Maßgabe des AVV, dieser Anlage, der gesonderten SCC- und Transferdokumentation und der freigegebenen Zugriffsmatrix. 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.
Stripe Payments Europe Ltd.	Zahlungsdienstleister und Empfänger im Rahmen eigener Abrechnungs- und Zahlungsprozesse von HAIZOP, soweit im Bestellprozess eingesetzt.	Nicht pauschal Unterauftragnehmer für Kunden-Plattformdaten; Zahlungs- und Abrechnungsdaten nach eigener Rollenverteilung.
Steuerberater, Rechtsberater, Banken, Behörden	Empfänger im Rahmen gesetzlicher, vertraglicher, Abrechnungs-, Nachweis- oder Rechtsverfolgungszwecke.	Keine Plattform-Unterauftragnehmer im Sinne des AVV.

Nicht Bestandteil der produktiven Standardverarbeitung

Bereich	Abgrenzung
Service-Level	Keine Verfügbarkeitsquote, Reaktionszeit, Bearbeitungszeit, Wiederherstellungszeit, Wiederherstellungspunkt oder Servicegutschrift ohne gesondertes Service-Level-Agreement.
Kundenverwaltete Schlüssel	Kundenverwaltete KMS-Schlüssel sind nicht Teil des Standardbetriebs und werden nur bei gesonderter Vereinbarung geschuldet.
Private Cloud / lokale Instanz	Private-Cloud-, On-Premise- oder lokale Instanz-Bereitstellungen sind nicht Bestandteil der Standardplattform.
Nicht gelistete KI-/OCR-Dienste	Nicht ausdrücklich als aktive Standardverarbeitung in dieser Anlage aufgeführte KI-, OCR- oder Dokumentenverarbeitungsdienste sind nicht Vertragsbestandteil.
Consumer-KI-Zugänge	Private oder Consumer-KI-Zugänge sowie nicht freigegebene Werkzeuge dürfen nicht für Kundendaten eingesetzt werden.

Ansprechpartner

Rolle	Kontakt
Sicherheitskontakt HAIZOP	security@haizop.de
Supportkontakt HAIZOP	Ticketsystem der HAIZOP-Plattform; ergänzend benannter Supportkanal.
Weisungsberechtigter Datenschutzkontakt des Kunden	Gemäß Bestellübersicht oder AVV.
Sicherheitskontakt des Kunden	Gemäß Bestellübersicht.