



HaiSoTec GmbH

AUFTRAGSVERARBEITUNGS VERTRAG (AVV) gemäß Art. 28 DSGVO

Auftragsverarbeitungsvertrags (AVV) - HaiSoTec-Plattform Dokument:

AVV_HaiSoTec_Plattform_V1.0

Version: 1.0 Stand: 15.03.2026

zwischen

HaiSoTec GmbH eine Gesellschaft mit beschränkter Haftung mit Sitz in Haigerloch, Deutschland
eingetragen im Handelsregister des Amtsgerichts Stuttgart unter HRB 802189 Geschäftsanschrift:
Freihofstraße 4, 72401 Haigerloch

-- im Folgenden "Auftragnehmer" --

und

dem jeweiligen Kunden / Auftraggeber -- im Folgenden "Auftraggeber" -- Die konkreten
Unternehmensdaten des Kunden / Auftraggeber ergeben sich aus:

den im HaiSoTec-System gespeicherten Registrierungsdaten
dem elektronischen Signatur Protokoll der Vertragsannahme
der zugeordneten Partner-ID im HaiSoTec-System

Diese Daten sind Bestandteil dieses Vertrags.

-- Auftraggeber und Auftragnehmer jeweils eine "Partei" und zusammen die

"Parteien" --



Inhaltsverzeichnis

PRÄAMBEL.....	3
§1. GEGENSTAND UND UMFANG DER BEAUFTRAGUNG.....	3
§2. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN.....	5
§3. BETROFFENENRECHTE.....	6
§4. PFLICHTEN DES AUFTRAGNEHMERS.....	7
§5. UNTERAUFTRAGSVERHÄLTNISSE.....	8
Hauptunter Auftragsverarbeiter:.....	9
§6. DATENVERARBEITUNG AUSSCHLIEßLICH IN DER EU.....	11
§7. KONTROLLRECHTE DES AUFTRAGGEBERS.....	12
§8. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS.....	13
§9. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN.....	14
§10. HAFTUNG UND SCHADENSERSATZ.....	15
§11. VERTRAGSLAUFZEIT UND BEENDIGUNG.....	17
§12. SCHLUSSBESTIMMUNGEN.....	18



PRÄAMBEL

Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Rahmen der Bereitstellung cloudbasierter Softwarelösungen der HaiSoTec-Plattform (nachfolgend "Plattform" oder "Dienste").

Die HaiSoTec-Plattform umfasst verschiedene Softwaremodule, die als Software-as-a-Service (SaaS) bereitgestellt werden. Die jeweils vom Auftraggeber genutzten Module ergeben sich aus dem zugrundeliegenden Lizenzvertrag bzw. Partnervertrag und sind in den produktspezifischen Anhängen zu dieser Vereinbarung näher beschrieben.

Im Rahmen dieser Leistungserbringung erhält der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO.

Zur Wahrung der geltenden datenschutzrechtlichen Anforderungen schließen die Parteien den nachfolgenden Vertrag.

§1. GEGENSTAND UND UMFANG DER BEAUFTRAGUNG

1.1 Gegenstand

Der Auftragnehmer stellt dem Auftraggeber cloudbasierte Softwarelösungen der HaiSoTec-Plattform zur Verfügung. Die Plattform besteht aus einzelnen Modulen, die unabhängig voneinander oder in Kombination genutzt werden können.

Die zum Zeitpunkt dieses Vertrages verfügbaren Module sind:

HaiSoTec-Tickets -- Ticket-Management-System (siehe Anhang A1)

HaiSoTec-Time -- Zeiterfassungssystem (siehe Anhang A2)

HaiSoTec-People -- Personal- und Organisationsmanagement (siehe Anhang A3)

HaiSoTec-Vorgano -- Auftrags- und Vorgangsverwaltung (siehe Anhang A4)

Alle Module basieren auf derselben technischen Plattform Architektur und nutzen die gleiche Infrastruktur, Sicherheitsstandards und Betriebsprozesse.

Der konkrete Umfang der vom Auftraggeber genutzten Module ergibt sich aus dem zugrunde liegenden Lizenzvertrag bzw. Partnervertrag.

1.2 Erweiterbarkeit

Der Auftragnehmer kann zukünftig weitere Module zur HaiSoTec-Plattform hinzufügen. Für jedes neue Modul wird ein produktspezifischer Anhang (Anhang A) erstellt, der die modulspezifischen



Vorbereitungstätigkeiten, Datenkategorien und Besonderheiten beschreibt.

Die Aufnahme eines neuen Moduls in diese Vereinbarung erfolgt durch:

- Erstellung eines neuen produktspezifischen Anhangs
- Schriftliche Mitteilung an den Auftraggeber
- Ergänzung der Modulliste in Abschnitt 1.1

Die übrigen Bestimmungen dieser Vereinbarung gelten für alle Module gleichermaßen und müssen nicht angepasst werden.

1.3 Verarbeitung personenbezogener Daten

Die Verarbeitung der personenbezogenen Daten des Auftraggebers (nachfolgend "Auftraggeberdaten") erfolgt gemäß den produktspezifischen Anhängen (Anhänge A1-A4) sowie der zentralen Beschreibung der Verarbeitung (Anhang B) dieses Vertrags.

Technische Durchführung: Der Zugriff auf die Plattform erfolgt ausschließlich über sichere, verschlüsselte Web Verbindungen (HTTPS/TLS 1.2+). Ein physischer Zugriff auf Kundensysteme oder Fernwartungssoftware wird nicht benötigt, da die Plattform vollständig cloud-basiert über Google Cloud Platform / Firebase bereitgestellt wird.

Hinweis zur SAP-Integration (sofern aktiviert): Für die SAP-Integration stellt der Auftraggeber eine virtuelle Maschine in seinem eigenen Netzwerk bereit, auf der Synchronisation Skripte ausgeführt werden. Die Integration erfolgt bidirektional:

- Lesend: SAP-Stammdaten (Geschäftspartner, Mitarbeiter, Arbeitstypen) werden nach BigQuery synchronisiert
- Schreibend: Arbeitszeit Einträge aus der HaiSoTec-Plattform werden zurück ins SAP-System geschrieben

Der Auftragnehmer hat Zugriff auf die synchronisierten SAP-Daten in BigQuery (lesend) und nutzt die vom Auftraggeber bereitgestellte VM für das Zurückschreiben von Zeiteintragung.

Die Verantwortung für die Sicherheit der virtuellen Maschine und der SAP-Zugangsdaten liegt beim Auftraggeber.

Der Auftragnehmer ist verpflichtet, die Auftraggeberdaten ausschließlich im Rahmen der dokumentierten Weisungen des Auftraggebers zu verarbeiten. Abweichende oder darüber hinausgehende Verarbeitungen sind untersagt.

1.4 Vorrang dieser Vereinbarung



Soweit andere Vereinbarungen zwischen Auftraggeber und Auftragnehmer abweichende Regelungen zum Schutz personenbezogener Daten enthalten, gilt vorrangig dieser Vertrag zur Auftragsverarbeitung.

§2. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

2.1 Sicherheitsmaßnahmen

Der Auftragnehmer trifft in seinem Verantwortungsbereich gemäß Anhang C (Technische und Organisatorische Maßnahmen -- TOM) dieses Vertrags alle erforderlichen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO zum Schutz der personenbezogenen Daten.

Die in Anhang C beschriebenen Maßnahmen gelten einheitlich für alle Module der HaiSoTec-Plattform, da sämtliche Module auf derselben technischen Infrastruktur und Sicherheitsarchitektur basieren.

Die vereinbarten technischen und organisatorischen Maßnahmen umfassen insbesondere:

- Zutrittskontrolle: Schutz durch Google Cloud Rechenzentren (ISO 27001, SOC 2, BSI C5 zertifiziert) Zugangskontrolle: Firebase Authentication (E-Mail/Passwort)
- Zugriffskontrolle: Rollenbasiertes Berechtigungssystem mit granularen Berechtigungen Weitergabekontrolle: HTTPS/TLS 1.2+ Verschlüsselung für alle Datenübertragungen Eingabekontrolle: Audit-Logging und Versionierung aller Änderungen
- Auftragskontrolle: Dieser Vertrag und dokumentierte Weisungen
- Verfügbarkeitskontrolle: Automatische Backups, Multi-Region-Replication, hohe Verfügbarkeit gemäß Google Cloud Infrastruktur
- Trennungskontrolle: Firestore Security Rules für mandantenfähige Datentrennung
- Verschlüsselung: AES-256 für Daten im Ruhezustand, TLS 1.2+ für

Daten in Übertragung

2.2 Anpassung der Maßnahmen

Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer ist berechtigt, künftig alternative, gleichwertige



Maßnahmen umzusetzen, sofern das festgelegte Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen.

§3. BETROFFENENRECHTE

3.1 Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich durch geeignete technische und organisatorische Maßnahmen bei der Bearbeitung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte gemäß Art. 15-22 DSGVO.

3.2 Verarbeitung nur auf Weisung

Der Auftragnehmer darf die im Auftrag verarbeiteten Daten nur auf Grundlage einer dokumentierten Weisung des Auftraggebers:

- auskunft geben
- übertragen (Datenportabilität)
- berichtigen
- löschen oder
- deren Verarbeitung einschränken

3.3 Weiterleitung von Anfragen

Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter.

3.4 Technische Umsetzung

Die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität werden nach dokumentierter Weisung des Auftraggebers wie folgt umgesetzt:

- Datenexport: JSON/CSV-Export aller personenbezogenen Daten eines Benutzers (manuell durch Auftragnehmer auf schriftliche Weisung)
- Datenlöschung: Anonymisierung personenbezogener Daten unter Beibehaltung von Geschäftsdaten (manuell durch Auftragnehmer auf schriftliche Weisung)
- Verarbeitungsfrist: Bearbeitung innerhalb von 5 Werktagen nach schriftlicher Weisung
- Anforderungsweg: Schriftliche Weisung per E-Mail an support@haisotec.de erforderlich



Diese Umsetzung gilt einheitlich für alle Module der HaiSoTec-Plattform.

§4. PFLICHTEN DES AUFTRAGNEHMER

4.1 Vertraulichkeit

Der Auftragnehmer gewährleistet die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, Art. 29 und Art. 32 Abs. 4 DSGVO. Er setzt für die Durchführung des Auftrags nur Beschäftigte ein, die:

- zur Vertraulichkeit verpflichtet wurden
- zuvor über die für sie relevanten Datenschutzbestimmungen informiert wurden
- regelmäßig zu Datenschutz und IT-Sicherheit geschult werden

4.2 Weisungsgebundene Verarbeitung

Der Auftragnehmer und jede ihm unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese ausschließlich gemäß den Weisungen des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, eine gesetzliche Verpflichtung zur Verarbeitung liegt vor.

4.3 Kooperation mit Aufsichtsbehörden

Der Auftraggeber und der Auftragnehmer kooperieren auf Anfrage mit der zuständigen Datenschutz Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben.

4.4 Meldung von Kontrollhandlungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich über:

- Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit diese den vorliegenden Vertrag betreffen
- Ermittlungen einer zuständigen Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens, die die Verarbeitung personenbezogener Daten im Zusammenhang mit der Auftragsverarbeitung betreffen

4.5 Regelmäßige Überprüfung

Der Auftragnehmer überprüft regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die Verarbeitung im Verantwortungsbereich des Auftragnehmers den Anforderungen des geltenden Datenschutzrechts entspricht und der Schutz der Rechte der betroffenen Personen gewährleistet ist.



4.6 Nachweispflicht

Der Auftragnehmer stellt sicher, dass die getroffenen technischen und organisatorischen Maßnahmen dem Auftraggeber auf Anfrage im Rahmen seiner Kontrollbefugnisse gemäß Nr. 7 dieses Vertrags nachgewiesen werden können.

4.7 Meldung von Datenschutzverletzungen

Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung, an den Auftraggeber. Die Meldung erfolgt an die im HaiSoTec-System angegebene E-Mail des Ansprechpartners.

Die Meldung umfasst mindestens:

- Art der Verletzung des Schutzes personenbezogener Daten
 - Kategorien und ungefähre Zahl der betroffenen Personen
 - Kategorien und ungefähre Zahl der betroffenen Datensätze
- Wahrscheinliche Folgen der Verletzung
 - Ergriffene oder vorgeschlagene Maßnahmen zur Behebung und Eindämmung
- Sofern identifizierbar: betroffene Module der HaiSoTec-Plattform

Der Auftragnehmer erstellt eine vollständige Dokumentation des Vorfalls und stellt diese dem Auftraggeber zur Verfügung.

4.8 Unterstützung bei Informationspflichten

Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich bei der Erfüllung der Informationspflichten gegenüber Aufsichtsbehörden und betroffenen Personen, indem er ihm unverzüglich sämtliche relevanten Informationen zur Verfügung stellt.

4.9 Datenschutz-Folgenabschätzung

Sollte der Auftraggeber verpflichtet sein, eine Datenschutz-Folgenabschätzung durchzuführen, unterstützt der Auftragnehmer ihn entsprechend der Art der Verarbeitung und den ihm vorliegenden Informationen. Dies gilt auch für etwaige Verpflichtungen zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

§5. UNTERAUFGTRAGSVERHÄLTNISSE

5.1 Definition von Unterauftragsverhältnissen

Unterauftragsverhältnisse im Sinne dieser Regelung beziehen sich auf Dienstleistungen, die sich direkt



auf die Erbringung der Hauptleistung (Bereitstellung der HaiSoTec-Plattform und ihrer Module) beziehen.

Nicht umfasst sind Nebenleistungen wie:

- Telekommunikationsleistungen
 - Post-/Transportdienstleistungen
- Allgemeine IT-Wartung, die nicht im Zusammenhang mit der Plattform steht

5.2 Genehmigte Unterauftragsverarbeiter

Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung für die Beauftragung der in Anhang D aufgeführten Unter-Auftragsverarbeiter.

Hauptunter Auftragsverarbeiter:

5.2.1 Google Cloud Platform (Google LLC)

Leistung: Cloud-Infrastruktur, Hosting, Datenbank (Firestore), Authentifizierung (Firebase Auth), Cloud, Functions, Storage, BigQuery

Standort: EU (Primär: Frankfurt, Deutschland; Belgien)

Datenverarbeitung: EU/EWR

Zertifizierungen: ISO 27001, ISO 27017, ISO 27018, SOC 2, BSI C5

Vertrag: Google Cloud Data Processing Addendum verfügbar unter:

<https://cloud.google.com/terms/data-processing-addendum>

Zweck: Bereitstellung der technischen Infrastruktur und Plattform für alle Module

5.2.2 Microsoft Corporation

Leistung: E-Mail-Integration über Microsoft 365 / Graph API

Standort: EU

Datenverarbeitung: EU/EWR

Verfügbarkeit: Für alle lizenzierten Benutzer der Module mit M365-Integration

Vertrag: Microsoft Products and Services Data Protection Addendum (DPA)

Zweck: E-Mail-basierte Ticket-Erstellung und -Verwaltung (sofern aktiviert)

5.3 Benachrichtigung über Änderungen

Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage im Voraus über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftrag Verarbeiten. Die Meldung erfolgt an die im HaiSoTec-System angegebene E-Mail des Ansprechpartners.



5.4 Widerspruchsrecht

Der Auftraggeber hat das Recht, innerhalb von 30 Tagen nach Benachrichtigung aus wichtigem datenschutzrechtlichen Grund gegen die Beauftragung eines neuen Unterauftragsverarbeiters Widerspruch zu erheben.

Bei berechtigtem Widerspruch ist der Auftragnehmer verpflichtet:

entweder auf die Beauftragung des Unterauftragsverarbeiters zu verzichten, oder dem Auftraggeber eine ordentliche Kündigung der Vereinbarung zu ermöglichen

5.5 Anforderungen an Unterauftragsverarbeiter

Wenn der Auftragnehmer einen Unterauftragsverarbeiter einsetzt, stellt er durch einen schriftlichen Vertrag sicher, dass:

- der Unterauftragsverarbeiter nur in dem Umfang auf Auftraggeberdaten zugreift und diese nutzt, wie es zur Erfüllung der ihm übertragenen Verpflichtungen erforderlich ist
- dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt werden wie dem Auftragnehmer nach diesem Vertrag
- der Unterauftragsverarbeiter alle Datenschutzerfordernungen einhält, die auch für den Auftragnehmer nach diesem Vertrag und den geltenden Datenschutzgesetzen gelten

5.6 Verantwortlichkeit und Haftung

Verantwortlichkeit gemäß DSGVO: Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung aller dem Unterauftragsverarbeiter übertragenen datenschutzrechtlichen Verpflichtungen verantwortlich (Art. 28 Abs. 4 DSGVO).

Haftungsbeschränkung: Die finanzielle Haftung des Auftragnehmers für Handlungen oder Unterlassungen der Unterauftragsverarbeiter (Google LLC, Microsoft Corporation) ist ausgeschlossen, soweit:

Der Auftragnehmer seine Auswahl Pflichten ordnungsgemäß erfüllt hat

Der Auftragnehmer die Sicherheits- und Datenschutzstandards der Unterauftragsverarbeiter überprüft hat

Die Schäden außerhalb der Kontrolle des Auftragnehmers liegen (Force Majeure)

Im Übrigen gelten die Haftungsregelungen gemäß §10 dieses Vertrags und des zugrundeliegenden Lizenzvertrags.



5.7 Datenverarbeitung innerhalb der EU

Alle Unterauftragsverarbeiter erbringen ihre Leistungen ausschließlich innerhalb der EU/des EWR:

- Google Cloud Platform: Datenverarbeitung ausschließlich in EU-Rechenzentren (Frankfurt, Belgien)
- Microsoft Corporation: Microsoft 365 EU Data Boundary (Datenverarbeitung in der EU)

Es erfolgt keine Übermittlung von Daten in Drittländer außerhalb der EU/des EWR.

§6. DATENVERARBEITUNG AUSSCHLIEßLICH IN DER EU

6.1 Verarbeitungsstandort

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR).

Konkrete Verarbeitungsstandorte:

- Primärer Standort: Frankfurt, Deutschland (Google Cloud EU-Region europe-west3) Sekundärer Standort: Belgien (Google Cloud EU-Region)
- Microsoft 365 Integration: EU Data Boundary (Datenverarbeitung ausschließlich in der EU) Diese Standorte gelten einheitlich für alle Module der HaiSoTec-Plattform.

6.2 Keine Datenübermittlung in Drittländer

Es erfolgt keine Übermittlung personenbezogener Daten in Drittländer außerhalb der EU/des EWR.

Alle Sub-Prozessoren (Google LLC, Microsoft Corporation) verarbeiten Daten ausschließlich in EU Rechenzentren:

- Google Cloud Platform ist vertraglich auf EU-Rechenzentren beschränkt (Regionswahl: europe-west3)
- Microsoft 365 nutzt die EU Data Boundary, wodurch Daten die EU nicht verlassen

6.3 Rechtliche Absicherung



Obwohl keine Drittlandübermittlung stattfindet, enthalten die Verträge mit den Sub-Prozessoren EU Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO (Durchführungsbeschluss (EU) 2021/914 der Kommission) als zusätzliche Absicherung für den Fall, dass sich rechtliche Rahmenbedingungen ändern sollten.

6.4 Änderungen der Verarbeitungsstandorte

Sollten sich die Verarbeitungsstandorte ändern oder eine Verarbeitung außerhalb der EU/des EWR erforderlich werden:

- Informiert der Auftragnehmer den Auftraggeber unverzüglich (mindestens 30 Tage im Voraus) Stellt der Auftragnehmer sicher, dass alle datenschutzrechtlichen Anforderungen (Kapitel V DSGVO, Art. 44–49) erfüllt werden
- Hat der Auftraggeber ein Widerspruchsrecht gemäß §5.4 dieses Vertrags

§7. KONTROLLRECHTE DES AUFTRAGGEBERS

7.1 Überprüfungsrecht

Der Auftraggeber ist berechtigt, nach vorheriger Ankündigung und Abstimmung mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende qualifizierte, unabhängige Prüfer durchführen zu lassen.

7.2 Auskunftsrechte

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Nachweismöglichkeiten

Der Nachweis der technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO kann erfolgen durch:

- Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung)
- Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. ISO 27001, SOC 2)
 - Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42

DSGVO Verfügbare Zertifizierungen/Nachweise:

- Google Cloud Platform: ISO 27001, ISO 27017, ISO 27018, SOC 2, BSI C5



- Firestore Security Rules Dokumentation
- Firebase Authentication Security Best Practices

7.4 Durchführung von Audits

Audits sind während der üblichen Geschäftszeiten durchzuführen und dürfen den laufenden Betrieb des Auftragnehmers nicht unverhältnismäßig beeinträchtigen.

7.5 Kosten

Die Kosten für Audits trägt grundsätzlich der Auftraggeber.

7.6 Vertraulichkeit

Der Prüfer ist zur Vertraulichkeit verpflichtet. Geschäftsgeheimnisse des Auftragnehmers sind zu wahren.

§8. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

8.1 Weisungsgebundene Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Grundlage dokumentierter Weisungen des Auftraggebers, es sei denn, er ist nach dem Recht eines Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtliche Anforderung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

8.2 Form der Weisungen

Weisungen können erteilt werden:

- Schriftlich: Per E-Mail oder Brief
- Über die Plattform: Durch Konfigurationseinstellungen und Admin-Funktionen innerhalb der genutzten Module
- Mündlich: Mit anschließender unverzüglicher schriftlicher Bestätigung (mindestens Textform)

8.3 Initiale Weisung



Die Festlegung der initialen Weisungen des Auftraggebers erfolgt im Rahmen dieses Vertrags und umfasst:

- Bereitstellung und Betrieb der genutzten Module der HaiSoTec-Plattform
- Verarbeitung der in den produktspezifischen Anhängen (Anhänge A1-A4) beschriebenen Daten Speicherung in EU-Rechenzentren
- Implementierung der vereinbarten Sicherheitsmaßnahmen
- Gewährung der Betroffenenrechte nach Weisung

8.4 Rechtmäßigkeitsprüfung

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen geltendes Datenschutzrecht. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange zu unterbrechen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§9. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

9.1 Keine unbefugten Kopien

Es erfolgt keine Erstellung von Kopien oder Duplikaten der Daten ohne Wissen des Auftraggebers. Hiervon ausgenommen sind:

- Zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderliche Sicherheitskopien (Backups) für Firestore-Daten
- Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind

Hinweis zu BigQuery-Daten: BigQuery-Daten sind eine direkte Synchronisation mit dem SAP-System des Auftraggebers und werden nicht separat gesichert. Diese Daten verbleiben unter der Kontrolle des SAP Systems.

9.2 Löschung nach Vertragsende

Nach Abschluss der vertraglich vereinbarten Verarbeitungstätigkeiten oder zu einem früheren Zeitpunkt nach Aufforderung durch den Auftraggeber -- spätestens aber mit Beendigung des Lizenzvertrags -- hat der Auftragnehmer innerhalb von 30 Tagen nach Vertragsende die Daten zur Rückgabe bzw. zum Export bereitzustellen.



Die endgültige Löschung sämtlicher personenbezogener Daten einschließlich Backups und Sicherheitskopien erfolgt innerhalb von 60 Tagen nach Vertragsende.

Im Einzelnen hat der Auftragnehmer:

- Entweder: Sämtliche personenbezogenen Daten und alle vorhandenen Kopien dem Auftraggeber auszuhändigen/zur Verfügung zu stellen
- Oder: Nach vorheriger Zustimmung des Auftraggebers alle personenbezogenen Daten zu löschen und die Löschung zu bestätigen

Dies gilt für alle genutzten Module der HaiSoTec-Plattform gleichermaßen.

9.3 Lösungsverfahren

Die Löschung erfolgt modulübergreifend durch:

- Anonymisierung personenbezogener Daten in allen Modulen (Tickets, Kommentare, Projekte, Aufträge, Zeiteinträge, Personalakten etc.)
- Vollständige Löschung von Benutzerprofilen aus Firebase Authentication
 - Löschung von Benutzer-Dokumenten aus der Firestore-Datenbank
 - Löschung hochgeladener Dateien aus Cloud Storage
 - Löschung aller Zugriffstokens und Sitzungsdaten

9.4 Aufbewahrungsfristen

Geschäftsdaten (Ticket-Inhalte, Projekte, Zeiterfassungen, Aufträge etc.) können in anonymisierter Form aufbewahrt werden, wenn:

- der Personenbezug vollständig entfernt wurde (Ersetzung durch "Gelöschter Benutzer") dies für legitime Geschäftszwecke erforderlich ist (Dokumentation, Abrechnung)
- gesetzliche Aufbewahrungspflichten bestehen

9.5 Löschungsnachweis

Der Auftragnehmer erstellt auf Anforderung des Auftraggebers ein Lösungsprotokoll, das bestätigt:

- Welche Daten in welchen Modulen gelöscht/anonymisiert wurden
- Zeitpunkt der Löschung/Anonymisierung
 - Methode der Löschung
- Verantwortliche Person



§10. HAFTUNG UND SCHADENSERSATZ

10.1 Haftung des Auftragnehmers

Der Auftragnehmer haftet gegenüber dem Auftraggeber für Schäden, die durch eine nicht rechtmäßige Verarbeitung oder eine gegen diesen Vertrag verstoßende Handlung verursacht werden, nach den gesetzlichen Bestimmungen.

10.2 Haftung bei Unterauftragsverarbeitern

Verantwortlichkeit für datenschutzrechtliche Compliance: Der Auftragnehmer bleibt verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben durch seine Unterauftragsverarbeiter und haftet für Datenschutzverstöße durch Unterauftragsverarbeiter, sofern er seine Auswahlpflichten oder Überwachungspflichten verletzt hat.

Haftungsbeschränkung bei ordnungsgemäßer Sorgfalt: Hat der Auftragnehmer seine Sorgfaltspflichten bei Auswahl und Überwachung der Unterauftragsverarbeiter ordnungsgemäß erfüllt, gelten für die finanzielle Haftung die Beschränkungen gemäß §5.6 und §10.3 dieses Vertrags sowie die Haftungsregelungen des zugrunde liegenden Lizenzvertrags.

10.3 Haftungsausschluss

Der Auftragnehmer haftet nicht für Schäden, die entstehen durch:

- Weisungen des Auftraggebers, gegen die der Auftragnehmer ordnungsgemäß Einwand erhoben hat Handlungen oder Unterlassungen, die außerhalb des Einflussbereichs des Auftragnehmers liegen Höhere Gewalt (siehe §10.5)
- Ausfälle oder Sicherheitsvorfälle der Unterauftragsverarbeiter (Google LLC, Microsoft Corporation), soweit:
 - Der Auftragnehmer seine Auswahlpflichten ordnungsgemäß erfüllt hat
 - Der Auftragnehmer die Sicherheits- und Datenschutzstandards überprüft hat
 - Diese außerhalb der Kontrolle des Auftragnehmers liegen

10.4 Haftungsbeschränkungen

Im Übrigen gelten die Haftungsregelungen des zugrunde liegenden Lizenzvertrags.

Hinweis zur Haftungshöhe: Der Auftragnehmer haftet grundsätzlich nur für tatsächlich eingetretene, nachgewiesene Schäden. Die Haftung ist der Höhe nach begrenzt auf die in den letzten 12 Monaten vor dem schadensbegründenden Ereignis tatsächlich gezahlte Netto-Lizenzgebühr, mindestens jedoch EUR 5.000,00. Diese Beiträge stellen keine Mindestschadenshöhe dar, sondern definieren ausschließlich die maximale Haftungsobergrenze. Bei Schäden unterhalb dieser Beträge haftet der



Auftragnehmer nur in Höhe des nachgewiesenen tatsächlichen Schadens.

Die vorstehenden Haftungsbeschränkungen gelten nicht bei Vorsatz, grober Fahrlässigkeit, bei Verletzung von Leben, Körper oder Gesundheit sowie bei Ansprüchen nach Art. 82 DSGVO.

10.5 Höhere Gewalt

Als höhere Gewalt im Sinne dieses Vertrags gelten insbesondere:

- Naturkatastrophen (Erdbeben, Überschwemmungen, Stürme)
- Krieg, Terrorismus, Aufruhr, Pandemien
- Streiks und Aussperrungen (außerhalb des Einflussbereichs des Auftragnehmers)
- Behördliche Anordnungen und Verbote
- Ausfall der Internet-Infrastruktur
- Ausfälle oder Sicherheitsvorfälle der Infrastruktur-Anbieter (Google Cloud Platform, Microsoft Corporation), soweit diese außerhalb der Kontrolle des Auftragnehmers liegen
- Cyberangriffe gegen die Infrastruktur-Anbieter oder das Internet im Allgemeinen

Bei höherer Gewalt ruhen die Verpflichtungen beider Parteien für die Dauer der Beeinträchtigung. Dauert die höhere Gewalt länger als 30 Tage, sind beide Parteien zur außerordentlichen Kündigung berechtigt.

§11. VERTRAGSLAUFZEIT UND BEENDIGUNG

11.1 Vertragsdauer

Dieser Vertrag tritt mit Unterzeichnung durch beide Parteien in Kraft und gilt für die Dauer des zugrundeliegenden Lizenzvertrags.

11.2 Ordentliche Kündigung

Dieser Vertrag endet automatisch mit der Beendigung des Lizenzvertrags. Eine gesonderte Kündigung ist nicht erforderlich.

11.3 Außerordentliche Kündigung

Beide Parteien sind berechtigt, diesen Vertrag aus wichtigem Grund außerordentlich und fristlos zu kündigen. Ein wichtiger Grund liegt insbesondere vor bei:

- Schwerwiegenden Verstößen gegen datenschutzrechtliche Bestimmungen
- Wiederholten Verstößen gegen Vertragspflichten trotz Abmahnung
- Insolvenz einer Partei

11.4 Folgen der Beendigung



Bei Beendigung dieses Vertrags gelten die Regelungen zur Löschung und Rückgabe gemäß §9 dieses Vertrags. Die Löschung erfolgt modulübergreifend für alle genutzten Module der HaiSoTec-Plattform.

§12. SCHLUSSBESTIMMUNGEN

12.1 Änderungen und Ergänzungen

Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

Die Ergänzung neuer produktspezifischer Anhänge (Anhänge A) bei Einführung weiterer HaiSoTec-Module gilt nicht als Änderung dieses Vertrags, sondern als Konkretisierung des Vertragsgegenstands.

12.2 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrags unwirksam oder undurchführbar sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung durch eine wirksame und durchführbare Regelung zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen oder undurchführbaren Bestimmung am nächsten kommt.

12.3 Anwendbares Recht

Auf diesen Vertrag findet ausschließlich das Recht der Bundesrepublik Deutschland Anwendung.

12.4 Gerichtsstand

Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist Hechingen, Deutschland, soweit gesetzlich zulässig.

12.5 Vorrang der DSGVO

Dieser Vertrag ist im Einklang mit den Vorgaben der DSGVO auszulegen. Im Zweifel haben die unmittelbar anwendbaren Vorgaben der DSGVO Vorrang.

12.6 Anhangsverzeichnis

Folgende Anhänge sind Bestandteil dieses Vertrags:



Anhang	Bezeichnung	Inhalt
A1	Produktspezifischer Anhang HaiSoTec-Tickets	Modulspezifische Verarbeitungsbeschreibung
A2	Produktspezifischer Anhang HaiSoTec-Time	Modulspezifische Verarbeitungsbeschreibung
A3	Produktspezifischer Anhang HaiSoTec-People	Modulspezifische Verarbeitungsbeschreibung
A4	Produktspezifischer Anhang HaiSoTec-Vorgano	Modulspezifische Verarbeitungsbeschreibung
B	Zentrale Beschreibung der Verarbeitung	Plattformübergreifende Verarbeitungsbeschreibung
C	Technische und Organisatorische Maßnahmen (TOM)	Zentrale TOM für alle Module
D	Genehmigte Unterauftragsverarbeiter	Liste der Sub-Prozessoren

Dieses Dokument ist Bestandteil des Auftragsverarbeitungsvertrags der HaiSoTec GmbH.



HaiSoTec GmbH

ANHANG A1: PRODUKTSPEZIFISCHER ANHANG HAISOTEC-TICKETS

Bestandteil des Auftragsverarbeitungsvertrags (AVV) der HaiSoTec GmbH

Dokument: ANHANG A1: PRODUKTSPEZIFISCHER ANHANG HAISOTEC-TICKETS_V1.0

Version: 1.0 Stand: 15.03.2026



HaiSoTec GmbH

Inhaltsverzeichnis

1. Modulbeschreibung.....	3
2. Modulspezifische Vorbereitungstätigkeiten.....	3
3. Modulspezifische Datenkategorien.....	4
4. Modulspezifische Kategorien betroffener Personen.....	5
5. Modulspezifische Integrationen.....	6
6. Modulspezifisches Berechtigungssystem.....	6
7. Besondere Kategorien personenbezogener Daten.....	7
8. Lösungsverfahren (modulspezifisch).....	7



1. Modulbeschreibung

1.1 Bezeichnung

HaiSoTec-Tickets

1.2 Produktcharakter

HaiSoTec-Tickets ist ein cloudbasiertes, webbasiert nutzbares System zur strukturierten Erfassung, Bearbeitung, Verwaltung, Dokumentation und Nachverfolgung von Tickets, Vorgängen, Aufgaben, Servicefällen, Meldungen und sonstigen ticket basierten Arbeitsprozessen.

1.3 Bereitstellung

Software-as-a-Service (SaaS) auf der HaiSoTec-Plattform. Dedizierte Einzelinstanz (Single-Instance) je Endkunde.

2. Modulspezifische Vorbereitungstätigkeiten

Zusätzlich zu den in ANHANG B: ZENTRALE BESCHREIBUNG DER VERARBEITUNG beschriebenen plattformübergreifenden Vorbereitungstätigkeiten umfasst HaiSoTec-Tickets folgende modulspezifische Verarbeitungen:

Verarbeitungstätigkeit	Beschreibung
Ticket-Management	Erstellung, Bearbeitung, Zuweisung und Nachverfolgung von Support-Tickets
Kommentar-Verwaltung	Kommunikation und Dokumentation zu Tickets
Zeiterfassung im Ticketkontext	Erfassung und Verwaltung von Arbeitszeiten für Tickets
Projekt-Verwaltung	Verwaltung von Projekten und deren Verknüpfung mit Tickets
Datei-Verwaltung	Upload und Speicherung von Ticket-Anhängen



Ticket-History	Änderungshistorie für Tickets (Wer hat was wann geändert)
SAP-Datenintegration	Bidirektionale Synchronisation mit SAP (sofern aktiviert)
E-Mail-Integration	Microsoft 365 E-Mail-Integration zur Ticket-Erstellung (sofern aktiviert)

3. Modulspezifische Datenkategorien

3.1 Ticket-Stammdaten

- Ticket-ID (systemgeneriert)
- Titel und Beschreibung
- Status, Priorität, Kategorie
- Erstellungsdatum, Fälligkeitsdatum
- Zugewiesene Bearbeiter (Benutzer-ID, Name)
- Ersteller (Benutzer-ID, Name)
- Projektbezug

3.2 Ticket-Kommunikationsdaten

- Kommentare (Inhalt, Autor, Zeitstempel)
- Interne Bearbeitungsvermerke
- Verlaufsinformationen

3.3 Zeiterfassungsdaten

- Erfasste Arbeitszeiten pro Ticket
- Zeitart (abrechenbar/nicht abrechenbar)
- Zugeordneter Mitarbeiter
- Beschreibung der Tätigkeit

3.4 Projektdaten

- Projektname, Projektbeschreibung
- Zugeordnete Teammitglieder
- Projektstatus

3.5 Dateianhang Daten

- Hochgeladene Dateien und Dokumente



- Dateiname, Dateityp, Dateigröße
- Upload-Zeitpunkt, Upload-Benutzer

3.6 SAP-Integrationsdaten (sofern aktiviert)

Aus SAP gelesene Daten:

- Geschäftspartner: Kundennummer, Kundenname, Adresse, Kontaktdaten, Zahlungsbedingungen, USt-ID Mitarbeiter: Mitarbeiter-ID, Name, Abteilung, Kontaktdaten
- Arbeitstypen: Code, Bezeichnung, Abrechnungsinformationen, Artikel-IDs
- Lieferarten: Code, Bezeichnung, Zusatzkosten-Konfiguration
- Artikel: Artikelnummer, Bezeichnung, Preise, MwSt.-Gruppe
- Verträge: Vertragsnummer, Kunde, Beschreibung, Laufzeit, Status, Preise
- Aufträge: Auftragsnummer, Kunde, Positionen, Beträge, Status

In SAP zurückgeschriebene Daten:

- Arbeitszeit Einträge aus dem Ticket-System
- Ticket-Nummern und Beschreibungen
- Zugeordnete Mitarbeiter und Geschäftspartner
- Anrechenbare und sofern aktiviert nicht-abrechenbare Arbeitszeiten
- Arbeitstyp und Lieferart

3.7 E-Mail-Integrationsdaten (sofern aktiviert)

- E-Mail-Betreff
- E-Mail-Inhalt (zur Ticket-Erstellung)
- Absender/Empfänger-Adressen
- E-Mail-Anhänge

4. Modulspezifische Kategorien betroffener Personen

Zusätzlich zu den in Anhang B genannten Kategorien:

Kategorie	Beschreibung
Mitarbeiter des Auftraggebers	Alle Nutzer des Ticket-Systems (Administratoren, Support-Mitarbeiter, Projektleiter, Sachbearbeiter)
Kunden des Auftraggebers (indirekt)	Nur wenn in Tickets erwähnt/dokumentiert (z.B. Kundennamen in Ticket-Beschreibungen)
Geschäftspartner des	Nur wenn in Projekten oder Tickets referenziert



Auftraggebers (indirekt)	
Externe Ansprechpartner (indirekt)	Kontaktpersonen bei Kunden oder Partnern, die in Tickets erwähnt werden
E-Mail-Absender (indirekt)	Bei aktivierter M365-Integration: Absender eingehender E-Mails, die als Tickets erfasst werden

5. Modulspezifische Integrationen

5.1 SAP Business One Integration

- Art: Bidirektional (lesen und schreiben)
- Technologie: Synchronisationsskripte auf VM des Auftraggebers, BigQuery als Datenschicht
Verantwortlichkeit: VM und SAP-Zugangsdaten liegen beim Auftraggeber
- Datenhaltung: BigQuery-Daten sind direkte SAP-Synchronisation ohne separate

Backups

5.2 Microsoft 365 Integration

- Art: E-Mail-basierte Ticket-Erstellung
- Technologie: Microsoft Graph API, OAuth 2.0
- Verfügbarkeit: Für alle lizenzierten Benutzer
- Besonderheit: Benutzer erteilen individuelle OAuth-Zustimmung

6. Modulspezifisches Berechtigungssystem

HaiSoTec-Tickets verwendet ein rollenbasiertes Berechtigungssystem mit 21 granularen Berechtigungen in 6 Kategorien:

Kategorie	Berechtigungen
Projects	read, create, edit, edit.creator, archive
Tickets	read, create, edit, edit.creator, edit.assignee, archive, ghostwriter, sync



HaiSoTec GmbH

Orders	read, read.fromTickets
Business Partners	read, read.fromTickets, read.supplier
Finance	read
Contracts	read, read.fromTickets

7. Besondere Kategorien personenbezogener Daten

Es werden grundsätzlich KEINE besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet. Sollten solche Daten versehentlich vom Auftraggeber in Tickets eingegeben werden, ist der Auftraggeber für die Rechtmäßigkeit verantwortlich.

8. Löschungsverfahren (modulspezifisch)

Die Löschung personenbezogener Daten in HaiSoTec-Tickets erfolgt durch:

- Anonymisierung personenbezogener Daten in Tickets, Kommentaren und Projekten
Löschung von Ticket-Anhängen aus Cloud Storage
- Anonymisierung von Zeiterfassungseinträgen
- Löschung von OAuth-Tokens der Microsoft 365 Integration

Dieses Dokument ist Bestandteil des Auftragsverarbeitungsvertrags der HaiSoTec GmbH.



HaiSoTec GmbH

ANHANG A2: PRODUKTSPEZIFISCHER ANHANG HAIOTECH-TIME

Bestandteil des Auftragsverarbeitungsvertrags (AVV) der HaiSoTec GmbH

Dokument: ANHANG A2: PRODUKTSPEZIFISCHER ANHANG HAIOTECH-TIME_V1.0

Version: 1.0 Stand: 15.03.2026



HaiSoTec GmbH

Inhaltsverzeichnis

1. Modulbeschreibung.....	3
2. Modulspezifische Vorbereitungstätigkeiten.....	3
3. Modulspezifische Datenkategorien.....	4
4. Modulspezifische Kategorien betroffener Personen.....	5
5. Modulspezifische Integrationen.....	5
6. Besondere Hinweise zum Datenschutz.....	5
7. Lösungsverfahren (modulspezifisch).....	6



1. Modulbeschreibung

1.1 Bezeichnung

HaiSoTec-Time

1.2 Produktcharakter

HaiSoTec-Time ist ein cloudbasiertes Zeiterfassungs- und Anwesenheitsmanagementsystem zur digitalen Erfassung, Verwaltung und Auswertung von Arbeitszeiten, Abwesenheiten und Anwesenheiten von Mitarbeitern.

1.3 Bereitstellung

Software-as-a-Service (SaaS) auf der HaiSoTec-Plattform. Dedizierte Einzelinstanz (Single-Instance) je Endkunde.

2. Modulspezifische Vorbereitungstätigkeiten

Zusätzlich zu den in ANHANG B: ZENTRALE BESCHREIBUNG DER VERARBEITUNG beschriebenen plattformübergreifenden Vorbereitungstätigkeiten umfasst HaiSoTec-Time folgende modulspezifische Verarbeitungen:

Verarbeitungstätigkeit	Beschreibung
Arbeitszeiterfassung	Erfassung von Arbeitszeiten (Beginn, Ende, Pausen)
Abwesenheitsverwaltung	Verwaltung von Urlaub, Krankheit, Sonderurlaub und weiteren Abwesenheitsarten
Anwesenheitsübersicht	Darstellung von An-/Abwesenheiten in Übersichten und Kalendern
Arbeitszeitkonten	Führung von Gleitzeitkonten, Überstundenkonten
Genehmigungsprozesse	Workflows für Urlaubs- und Abwesenheitsanträge
Auswertungen und Reports	Erstellung von Zeitauswertungen, Monatsberichten,



3. Modulspezifische Datenkategorien

3.1 Arbeitszeitdaten

- Arbeitsbeginn und Arbeitsende (Zeitstempel)
- Pausenzeiten (Beginn, Ende, Dauer)
- Tägliche Arbeitszeit (Soll/Ist)
- Überstunden und Zeitguthaben
- Art der Zeitbuchung (regulär, Überstunden, Rufbereitschaft etc.)

3.2 Abwesenheitsdaten

- Abwesenheitsart (Urlaub, Krankheit, Sonderurlaub, Fortbildung, Elternzeit etc.)
Abwesenheitszeitraum (Beginn, Ende)
- Genehmigungsstatus
- Verbleibender Urlaubsanspruch
- Krankmeldungen (nur Tatsache der Krankmeldung, keine Diagnosen)

3.3 Arbeitszeitkontendaten

- Gleitzeitkonto-Saldo
- Überstundenstand
- Jahresurlaubskonto
- Historische Kontoveränderungen

3.4 Genehmigungsdaten

- Antragsteller (Benutzer-ID, Name)
- Genehmiger/Vorgesetzter (Benutzer-ID, Name)
- Antragsdatum, Genehmigungsdatum
- Genehmigungsstatus (beantragt, genehmigt, abgelehnt)
- Kommentare zum Antrag

3.5 Auswertungsdaten

- Monatliche Arbeitszeitberichte
- Urlaubsübersichten
- Anwesenheitsstatistiken
- Abteilungsbezogene Zusammenfassungen



4. Modulspezifische Kategorien betroffener Personen

Zusätzlich zu den in Anhang B genannten Kategorien:

Kategorie	Beschreibung
Mitarbeiter des Auftraggebers	Alle Personen, deren Arbeitszeiten und Abwesenheiten im System erfasst werden
Vorgesetzte / Teamleiter	Personen mit Genehmigungs- und Einsichtsbefugnissen für Arbeitszeit- und Abwesenheitsanträge
HR-/Personalabteilung	Administratoren mit Zugriff auf Zeitauswertungen und Abwesenheitsübersichten
Externe Mitarbeiter (optional)	Sofern das Modul fuer die Zeiterfassung externer Mitarbeiter genutzt wird

5. Modulspezifische Integrationen

5.1 Verknüpfung mit HaiSoTec-Tickets (sofern beide Module aktiv und Verbindung zusätzlich aktiviert wurde)

- Zeitbuchungen können mit Tickets verknüpft werden
- Übertragung von Zeiteintragung in den Ticket Kontext

6. Besondere Hinweise zum Datenschutz

6.1 Sensibilität der Daten

Arbeitszeitdaten und insbesondere Abwesenheitszeiten (z.B. Krankmeldungen) erfordern eine erhöhte Sensibilität bei der Verarbeitung.

Der Auftragnehmer stellt sicher, dass:

- Zugriff auf Abwesenheitsdaten auf die dafür berechtigten Personen beschränkt ist Keine Verarbeitung von Diagnosen oder Gesundheitsdetails erfolgt
- Krankmeldungen nur als Tatsache (ja/nein, Zeitraum) erfasst werden



HaiSoTec GmbH

6.2 Keine besonderen Kategorien

Es werden grundsätzlich KEINE besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet. Insbesondere werden keine Gesundheitsdaten verarbeitet -- Krankmeldungen werden ausschließlich als organisatorische Abwesenheiten erfasst.

7. Lösungsverfahren (modulspezifisch)

Die Löschung personenbezogener Daten in HaiSoTec-Time erfolgt durch:

- Anonymisierung von Arbeitszeiteinträgen (Entfernung des Personenbezugs) Löschung von Abwesenheit Anträgen und Genehmigungsdaten
- Anonymisierung historischer Kontodaten
- Löschung von Mitarbeiterzuordnungen in Auswertungen

Dieses Dokument ist Bestandteil des Auftragsvertragsvertrags der HaiSoTec GmbH.



HaiSoTec GmbH

ANHANG A3: PRODUKTSPEZIFISCHER ANHANG HAISOTEC-PEOPLE

Bestandteil des Auftragsverarbeitungsvertrags (AVV) der HaiSoTec GmbH

ANHANG A3: PRODUKTSPEZIFISCHER ANHANG HAISOTEC-PEOPLE_V1.0

Version: 1.0 Stand: 15.03.2026



HaiSoTec GmbH

Inhaltsverzeichnis

1. Modulbeschreibung.....	3
2. Modulspezifische Vorbereitungstätigkeiten.....	3
3. Modulspezifische Datenkategorien.....	4
4. Modulspezifische Kategorien betroffener Personen.....	5
5. Besondere Hinweise zum Datenschutz.....	5
6. Modulspezifische Integrationen.....	6
7. Lösungsverfahren (modulspezifisch).....	6



1. Modulbeschreibung

1.1 Bezeichnung

HaiSoTec-People

1.2 Produktcharakter

HaiSoTec-People ist ein cloubasiertes Personal- und Organisationsmanagement System zur digitalen Verwaltung von Mitarbeiterstammdaten, Organisationsstrukturen, Dokumenten und personenbezogenen Prozessen.

1.3 Bereitstellung

Software-as-a-Service (SaaS) auf der HaiSoTec-Plattform. Dedizierte Einzelinstanz (Single-Instance) je Endkunde.

2. Modulspezifische Vorbereitungstätigkeiten

Zusätzlich zu den in ANHANG B: ZENTRALE BESCHREIBUNG DER VERARBEITUNG beschriebenen plattformübergreifenden Vorbereitungstätigkeiten umfasst HaiSoTec-People folgende modulspezifische Verarbeitungen:

Verarbeitungstätigkeit	Beschreibung
Mitarbeiter Stammdatenverwaltung	Erfassung und Pflege von Mitarbeiterdaten
Organisationsstruktur Verwaltung	Abbildung von Abteilungen, Teams, Hierarchien
Dokumentenverwaltung	Speicherung personenbezogener Dokumente
Onboarding/Offboarding	Verwaltung von Ein- und Austrittsprozessen
Qualifikation Verwaltung	Erfassung von Qualifikationen, Zertifikaten, Schulungen
Personal Übersichten	Darstellung von Mitarbeiterinformationen in Übersichten



3. Modulspezifische Datenkategorien

3.1 Mitarbeiterstammdaten

- Vor- und Nachname
- Geburtsdatum
- Geschlecht
- Privatadresse (optional)
- Geschäftliche Kontaktdaten (Telefon, E-Mail)
- Personalnummer
- Nationalität (optional)
- Familienstand (optional)

3.2 Beschäftigungsdaten

- Eintrittsdatum, ggf. Austrittsdatum
- Beschäftigungsart (Vollzeit, Teilzeit, Minijob, Werkstudent etc.)
- Arbeitszeitmodell (Wochenstunden, Gleitzeitrahmen)
- Probezeit-Enddatum
- Vertragsart (befristet/unbefristet)
- Abteilung/Team
- Position/Stellenbezeichnung
- Vorgesetzter
- Standort/Arbeitsort

3.3 Organisationsdaten

- Abteilungsbezeichnung
- Teamzugehörigkeit
- Hierarchiestufe
- Kostenstelle
- Unternehmensbereich

3.4 Dokumentendaten

- Personalakten-Dokumente (z.B. Arbeitsverträge, Zeugnisse, Bescheinigungen)
- Dateiname, Dateityp, Upload-Datum
- Dokumentenkategorie
- Zugeordneter Mitarbeiter

3.5 Qualifikationsdaten

- Qualifikation Bezeichnung
- Zertifikate und deren Gültigkeit
- Schulungsnachweise
- Ablaufdaten von Zertifizierungen



3.6 Prozessdaten (Onboarding/Offboarding)

- Checklisten und deren Status
- Aufgabenzuweisungen
- Fristen und Termine
- Verantwortliche Personen

4. Modulspezifische Kategorien betroffener Personen

Zusätzlich zu den in Anhang B genannten Kategorien:

Kategorie	Beschreibung
Mitarbeiter des Auftraggebers	Alle Personen, deren Personalstammdaten im System verwaltet werden
Ehemalige Mitarbeiter	Historische Datensätze (sofern nicht gelöscht/anonymisiert)
Vorgesetzte	Personen mit Einsichts- und Verwaltungsbefugnissen
HR-/Personalabteilung	Administratoren mit vollem Zugriff auf Personaldaten
Bewerber (optional)	Sofern das Modul fuer Bewerbermanagement genutzt wird

5. Besondere Hinweise zum Datenschutz

5.1 Erhöhte Sensibilität

HaiSoTec-People verarbeitet umfangreichere personenbezogene Daten als andere Module der Plattform. Der Auftragnehmer stellt sicher, dass:

- Der Zugriff auf Personaldaten streng nach dem Need-to-Know-Prinzip beschränkt ist
- Personalakten-Dokumente verschlüsselt gespeichert werden (AES-256)
- Zugriffe auf sensible Personaldaten protokolliert werden

5.2 Keine besonderen Kategorien

Es werden grundsätzlich KEINE besonderen Kategorien personenbezogener Daten gemäß Art. 9



HaiSoTec GmbH

DSGVO verarbeitet. Insbesondere:

- Keine Verarbeitung von Gesundheitsdaten
- Keine Verarbeitung von Gehaltsdaten oder Bankverbindungen
- Keine Verarbeitung von Gewerkschafts Zugehörigkeiten

Sollten solche Daten vom Auftraggeber in Dokumente eingepflegt werden, ist der Auftraggeber für die Rechtmäßigkeit verantwortlich.

5.3 Aufbewahrung und Löschung

Aufgrund arbeitsrechtlicher Aufbewahrungsfristen kann es erforderlich sein, bestimmte Personalunterlagen auch nach Beendigung des Beschäftigungsverhältnisses aufzubewahren. Die Verantwortung für die Einhaltung der Aufbewahrungsfristen und die rechtzeitige Löschung liegt beim Auftraggeber.

6. Modulspezifische Integrationen

6.1 Verknüpfung mit HaiSoTec-Time (sofern beide Module aktiv)

- Übernahme von Mitarbeiterstammdaten in die Zeiterfassung
- Abgleich von Abteilungs- und Team Zuordnungen

6.2 Verknüpfung mit HaiSoTec-Tickets (sofern beide Module aktiv, sofern Verbindung aktiviert wurde)

- Zuordnung von Bearbeitern zu Tickets auf Basis der Organisationsstruktur

7. Lösungsverfahren (modulspezifisch)

Die Löschung personenbezogener Daten in HaiSoTec-People erfolgt durch:

- Anonymisierung oder Löschung von Mitarbeiterstammdaten
- Löschung von Personalakten-Dokumenten aus Cloud Storage
- Anonymisierung von Organisations Zuordnungen
- Löschung von Qualifikations- und Zertifikatsdaten
- Anonymisierung von Onboarding/Offboarding-Prozessdaten

Dieses Dokument ist Bestandteil des Auftragsverarbeitungsvertrags der HaiSoTec GmbH.



HaiSoTec GmbH

ANHANG A4: PRODUKTSPEZIFISCHER ANHANG HAISOTEC-VORGANO

Bestandteil des Auftragsverarbeitungsvertrags (AVV) der HaiSoTec GmbH

ANHANG A4: PRODUKTSPEZIFISCHER ANHANG HAISOTEC-VORGANO_V1.0

Version: 1.0 Stand: 15.03.2026



Inhaltsverzeichnis

1. Modulbeschreibung.....	3
2. Modulspezifische Vorbereitungstätigkeiten.....	3
3. Modulspezifische Datenkategorien.....	4
4. Modulspezifische Kategorien betroffener Personen.....	5
5. Besondere Hinweise zum Datenschutz.....	5
6. Modulspezifische Integrationen.....	6
7. Lösungsverfahren (modulspezifisch).....	6



1. Modulbeschreibung

1.1 Bezeichnung

HaiSoTec-Vorgano

1.2 Produktcharakter

HaiSoTec-Vorgano ist eine cloudbasierte Softwarelösung zur strukturierten Verwaltung von Kundenaufträgen, Geschäftspartnern, Artikeln und Leistungen, Aufgaben und betrieblichen Vorgängen sowie Lagerbeständen und Materialien. Das System richtet sich insbesondere an kleine und mittelständische Unternehmen, Handwerksbetriebe, Dienstleistungsunternehmen und produktionsnahe Betriebe.

1.3 Bereitstellung

Software-as-a-Service (SaaS) auf der HaiSoTec-Plattform. Dedizierte Einzelinstanz (Single-Instance) je Endkunde.

1.4 Technische Plattform

HaiSoTec-Vorgano basiert auf derselben technischen Plattform wie HaiSoTec-Tickets und nutzt die gleiche Systemarchitektur. Unterschiede ergeben sich ausschließlich aus dem funktionalen Schwerpunkt (Auftrags- und Betriebsprozesse) sowie dem aktuellen Integrations Umfang.

2. Modulspezifische Vorbereitungstätigkeiten

Zusätzlich zu den in ANHANG B: ZENTRALE BESCHREIBUNG DER VERARBEITUNG beschriebenen plattformübergreifenden Vorbereitungstätigkeiten umfasst HaiSoTec-Vorgano folgende modulspezifische Verarbeitungen:

Verarbeitungstätigkeit	Beschreibung
Geschäftspartnerverwaltung	Erfassung und Verwaltung von Kunden, Lieferanten und Leads
Auftragsverwaltung	Anlage, Bearbeitung und Nachverfolgung von Kundenaufträgen
Aufgaben- und Vorgangsverwaltung	Erstellung und Verwaltung von Aufgaben und betrieblichen Vorgängen



Artikel- und Leistungsverwaltung	Verwaltung von Artikeln, Dienstleistungen und Infrastruktur Artikeln
Lagerverwaltung	Verwaltung von Lagerorten, Beständen und Materialbewegungen
Dokumentation	Historisierung von Änderungen und nachvollziehbare Vorgang Historien

3. Modulspezifische Datenkategorien

3.1 Geschäftspartnerdaten

- Firmenname/Name
- Anschrift (Straße, PLZ, Ort, Land)
- Kontaktdaten (Telefon, E-Mail, Fax)
- Kundennummer/Lieferantennummer
- Ansprechpartner (Name, Position, Kontaktdaten)
- Kundenkategorie (Kunde, Lieferant, Lead/Interessent)
- Zusatzinformationen (Branche, Zahlungsbedingungen)

3.2 Auftragsdaten

- Auftragsnummer (system generiert)
- Auftragsbezeichnung und -beschreibung
- Auftragsstatus
- Zugeordneter Geschäftspartner (Kunde)
- Auftragspositionen (Artikel, Leistungen, Mengen)
- Termine und Fristen
- Zuständige Bearbeiter

3.3 Aufgaben- und Vorgangsdaten

- Aufgabenbezeichnung und -beschreibung
- Aufgaben Status und Priorität
- Zugewiesene Verantwortliche (Benutzer-ID, Name)
- Verknüpfung mit Aufträgen (optional)
- Termine, Fristen, Fälligkeitsdaten

3.4 Artikel- und Leistungsdaten

- Artikelnummer, Artikelbezeichnung
- Artikelkategorie (Ware, Dienstleistung, Infrastruktur/Hardware/Lizenz)
- Preise, Mengeneinheiten
- Lagerzuordnung

3.5 Lagerdaten



- Lagerort Bezeichnung
- Bestandsmengen pro Artikel
- Materialbewegungen (Eingang, Ausgang, Umlagerung)
- Zeitstempel der Bewegungen

3.6 E-Mail-Integrationsdaten (sofern aktiviert)

- E-Mail-Betreff
- E-Mail-Inhalt (zur Aufgaben-Erstellung)
- Absender/Empfänger-Adressen
- E-Mail-Anhänge

4. Modulspezifische Kategorien betroffener Personen

Zusätzlich zu den in Anhang B genannten Kategorien:

Kategorie	Beschreibung
Mitarbeiter des Auftraggebers	Nutzer des Systems (Administratoren, Sachbearbeiter, Lagerverwalter)
Kunden des Auftraggebers	Geschäftspartner, deren Stammdaten verwaltet werden
Lieferanten des Auftraggebers	Lieferanten, deren Stammdaten verwaltet werden
Ansprechpartner	Kontaktpersonen bei Kunden und Lieferanten
Leads/Interessenten	Potenzielle Kunden im Vertriebsprozess

5. Besondere Hinweise zum Datenschutz

5.1 Geschäftspartnerdaten

HaiSoTec-Vorgano verarbeitet umfangreiche Geschäftspartnerdaten. Der Auftragnehmer stellt sicher, dass:

- Der Zugriff auf Geschäftspartnerdaten rollenbasiert beschränkt ist



- Nur geschäftlich notwendige Kontaktdaten verarbeitet werden
- Keine privaten personenbezogenen Daten der Ansprechpartner erhoben werden

5.2 Keine besonderen Kategorien

Es werden grundsätzlich KEINE besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet.

5.3 Microsoft 365 Integration (geplant/optional)

Die Microsoft 365 Integration für HaiSoTec-Vorgano befindet sich in Planung und ist zum Zeitpunkt dieser Version noch nicht aktiv. Bei zukünftiger Aktivierung gelten folgende vorgesehene Parameter:

- Art: E-Mail-basierte Aufgaben-Erstellung
- Technologie: Microsoft Graph API, OAuth 2.0
- Verfügbarkeit: Für alle lizenzierten Benutzer
- Besonderheit: Benutzer erteilen individuelle OAuth-Zustimmung

Die Nutzung der Microsoft 365 Integration erfordert eine gesonderte Aktivierung und kann zusätzliche Vereinbarungen oder Ergänzungen dieses Anhangs erfordern.

6. Modulspezifische Integrationen

6.1 Aktueller Stand

Zum Zeitpunkt dieser Version bestehen keine aktiven direkten Integrationen mit externen Systemen. Die Microsoft 365 Integration ist als zukünftige Erweiterung geplant (siehe §5.3).

6.2 Zukünftige Integrationen

Integrationen können zukünftig im Rahmen der Produktentwicklung ergänzt werden. Die Nutzung zukünftiger Integrationen kann zusätzliche Vereinbarungen oder Ergänzungen dieses Anhangs erfordern.

6.3 Verknüpfung mit anderen Modulen (sofern aktiv)

HaiSoTec-Tickets: Erstellung von Aufgaben/Vorgängen aus Tickets und umgekehrt

HaiSoTec-Time: Zeitbuchungen auf Aufträge und Aufgaben

HaiSoTec-People: Personen-Management

7. Lösungsverfahren (modulspezifisch)

Die Löschung personenbezogener Daten in HaiSoTec-Vorgano erfolgt durch:



HaiSoTec GmbH

- Anonymisierung von Geschäftspartnerdaten (Ersetzung durch "Gelöschter Partner") Anonymisierung von Ansprechpartner-Daten
- Anonymisierung von Benutzerzuordnungen in Aufträgen und Aufgaben
- Löschung von Kontaktdaten und Adressen
- Löschung von OAuth-Tokens der Microsoft 365 Integration (sofern zukünftig aktiviert)

Dieses Dokument ist Bestandteil des Auftragsverarbeitungsvertrags der HaiSoTec GmbH.



HaiSoTec GmbH

ANHANG B: ZENTRALE BESCHREIBUNG DER VERARBEITUNG

Bestandteil des Auftragsverarbeitungsvertrags (AVV) der HaiSoTec GmbH

Dokument: ANHANG B: ZENTRALE BESCHREIBUNG DER VERARBEITUNG_V1.0

Version: 1.0 Stand: 15.03.2026



Inhaltsverzeichnis

1. Gegenstand der Verarbeitung.....	3
2. Dauer der Verarbeitung.....	3
3. Art und Zweck der Verarbeitung.....	3
4. Plattformübergreifende Datenkategorien.....	4
5. Plattformübergreifende Kategorien betroffener Personen.....	5
6. Besondere Kategorien personenbezogener Daten.....	5
7. Rechtsgrundlagen der Verarbeitung.....	5



Dieser Anhang beschreibt die plattformübergreifenden Vorbereitungstätigkeiten, die für alle Module der HaiSoTec-Plattform gleichermaßen gelten. Modulspezifische Besonderheiten sind in den jeweiligen produktspezifischen Anhängen (Anhänge A1-A4) geregelt.

1. Gegenstand der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber cloudbasierte Softwarelösungen der HaiSoTec-Plattform zur Verfügung. Die folgenden Vorbereitungstätigkeiten gelten für alle Module gleichermaßen:

- Benutzerverwaltung: Verwaltung von Benutzerkonten, Authentifizierung, Berechtigungen Datei-Verwaltung: Upload und Speicherung von Anhängen und Dokumenten
- System-Logging: Änderungshistorie (Wer hat was wann geändert); Google Cloud Audit Logs auf Infrastrukturebene

Die modulspezifischen Verarbeitungstätigkeiten sind in den Anhängen A1-A4 beschrieben.

2. Dauer der Verarbeitung

Beginn: Mit Vertragsunterzeichnung und Aktivierung des jeweiligen Moduls

Ende: Mit Beendigung des Lizenzvertrags zuzüglich maximal 30 Tage für die

Datenrückgabe bzw. den Datenexport und maximal 60 Tage für die endgültige Löschung einschließlich Backups

Laufzeit: Entspricht der Laufzeit des Lizenzvertrags zwischen den Parteien

3. Art und Zweck der Verarbeitung

3.1 Art der Verarbeitung (plattformübergreifend)

- Erfassung: Erhebung von Benutzerdaten bei Registrierung
- Speicherung: Persistierung in Cloud-Datenbank (Firestore) und Cloud Storage Organisation: Strukturierung nach Mandanten und modulspezifischen Strukturen Veränderung: Updates von Benutzerprofilen und modulspezifischen Daten
- Abfrage: Bereitstellung von Daten im System für autorisierte Nutzer
- Verwendung: Darstellung in Benutzeroberfläche, Reports, Exports



- Übermittlung: Interne Weitergabe innerhalb des Systems (rollenbasiert)
- Löschung: Anonymisierung oder vollständige Löschung auf Weisung

3.2 Zweck der Verarbeitung (plattformübergreifend)

Die Verarbeitung erfolgt ausschließlich zum Zweck der:

- Bereitstellung der Systemfunktionalität der genutzten Module
- Authentifizierung und Autorisierung: Sichere Anmeldung und Zugriffskontrolle Dokumentation: Nachvollziehbarkeit von Arbeitsabläufen und Entscheidungen Systemsicherheit: Logging und Monitoring zur Gewährleistung der IT-Sicherheit

4. Plattformübergreifende Datenkategorien

Die folgenden Datenkategorien werden von allen Modulen der HaiSoTec-Plattform

verarbeitet: 4.1 Bestandsdaten (alle Module)

- Vor- und Nachname
- E-Mail-Adresse
- Telefonnummer (optional)
- Abteilung/Position (optional)
- Benutzer-ID (systemgeneriert)

Hinweis: Nur betrieblich notwendige Geschäftsdaten, keine Gehaltsdaten oder Bankverbindungen.

4.2 Authentifizierungsdaten (alle Module)

- Passwort-Hash (verschlüsselt, nicht im Klartext)
- Sitzung Tokens
- OAuth-Tokens für Microsoft 365 (verschlüsselt, sofern Benutzer Verbindung herstellt)

4.3 Metadaten (alle Module)

- Zeitstempel (Erstellung, Änderung)
- IP-Adresse (nur in Google Cloud Audit Logs auf Infrastrukturebene)
- User-Agent / Browser-Informationen (nur in Google Cloud Audit Logs auf Infrastrukturebene) Änderungshistorie (Wer hat was wann geändert)

4.4 Modulspezifische Datenkategorien

Die modulspezifischen Datenkategorien (z.B. Ticket-Daten, Zeiterfassungsdaten,



Personaldaten, Auftragsdaten) sind in den jeweiligen Anhängen A1-A4 beschrieben.

5. Plattformübergreifende Kategorien betroffener Personen

5.1 Mitarbeiter des Auftraggebers

- Hauptgruppe: Alle Nutzer der HaiSoTec-Plattform im Auftrag des Auftraggebers
- Typische Rollen: Administratoren, Sachbearbeiter, Projektleiter, Teamleiter

5.2 Weitere betroffene Personen

- Weitere Kategorien betroffener Personen ergeben sich aus den modulspezifischen Anhängen (z.B. Kunden, Lieferanten, Geschäftspartner, Ansprechpartner).

6. Besondere Kategorien personenbezogener Daten

Es werden grundsätzlich KEINE besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO auf der HaiSoTec-Plattform verarbeitet.

Dazu gehören insbesondere NICHT:

- Gesundheitsdaten
- Genetische Daten
- Biometrische Daten
- Daten über rassische/ethnische Herkunft
- Politische Meinungen
- Religiöse/weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Sexualleben/sexuelle Orientierung

Sollten solche Daten versehentlich vom Auftraggeber in ein Modul eingegeben werden, ist der Auftraggeber für die Rechtmäßigkeit verantwortlich.

7. Rechtsgrundlagen der Verarbeitung

Alle Verarbeitungen erfolgen auf Grundlage von:

- Art. 6 Abs. 1 lit. b DSGVO: Vertragserfüllung (Bereitstellung der Plattform)
- Art. 6 Abs. 1 lit. f DSGVO: Berechtigtes Interesse (Systemsicherheit, Logging)
- Art. 28 DSGVO: Auftragsverarbeitung



HaiSoTec GmbH

Dieses Dokument ist Bestandteil des Auftragsverarbeitungsvertrags der HaiSoTec GmbH.



HaiSoTec GmbH

ANHANG C: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

Bestandteil des Auftragsverarbeitungsvertrags (AVV) der HaiSoTec GmbH

Dokument: ANHANG_C_TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN_TOM_V1.0

Version: 1.0 Stand: 15.03.2026



Inhaltsverzeichnis

Geltungsbereich.....	3
1. ZUTRITTSKONTROLLE.....	3
2. ZUGANGSKONTROLLE.....	4
3. ZUGRIFFSKONTROLLE.....	5
4. WEITERGABEKONTROLLE.....	6
5. EINGABEKONTROLLE.....	8
6. AUFTRAGSKONTROLLE.....	9
7. VERFÜGBARKEITSKONTROLLE.....	10
8. TRENNUNGSKONTROLLE.....	12
9. DATENSCHUTZ-MANAGEMENT.....	13
10. AKTUALISIERUNG UND WARTUNG.....	14
11. ZUSAMMENFASSUNG DER SICHERHEITSMASSNAHMEN.....	15



Geltungsbereich

Diese technischen und organisatorischen Maßnahmen gelten einheitlich für alle Module der HaiSoTec Plattform:

- HaiSoTec-Tickets
- HaiSoTec-Time
- HaiSoTec-People
- HaiSoTec-Vorgano
- sowie alle zukünftigen Module der HaiSoTec-Plattform

Begründung: Alle Module der HaiSoTec-Plattform basieren auf derselben technischen Architektur, nutzen dieselbe Cloud-Infrastruktur (Google Cloud Platform / Firebase) und unterliegen denselben Sicherheitsstandards und Betriebsprozessen. Eine separate TOM je Modul ist daher nicht erforderlich.

Modulspezifische Besonderheiten (z.B. erhöhte Zugriffskontrollen für Personaldaten in HaiSoTec-People) werden in den Abschnitten dieser TOM gesondert gekennzeichnet.

1. ZUTRITTSKONTROLLE

Ziel: Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

1.1 Physische Sicherheit (Google Cloud Rechenzentren)

Infrastruktur:

- Geografisch verteilte Rechenzentren in der EU (Frankfurt, Belgien)
- Physisch sichere Rechenzentrumsgebäude
- Redundante Systeme zur Eliminierung von Single Points of Failure

Zutrittssicherung:

- 24/7 Sicherheitspersonal vor Ort
- Elektronische Zutrittskontrollsysteme mit Kartenleser
- Mehrstufiges Authentifizierungsverfahren
- Biometrische Zugangskontrollen an kritischen Bereichen
- Videoüberwachung (CCTV) innen und außen
- Protokollierung aller Zutrittsversuche
- Besucherverwaltung mit Begleitpflicht



- ISO 27001 (Information Security Management)
- ISO 27017 (Cloud Security)
- SOC 2 Type II (Security, Availability, Confidentiality)
- BSI C5 (Cloud Computing Compliance Criteria Catalogue)

Stromversorgung:

- Redundante Stromversorgungssysteme
- Unterbrechungsfreie Stromversorgung (USV) mit Batterien
- Notstromgeneratoren für mehrtägigen Betrieb
- Automatische Umschaltung bei Stromausfall

Geltung: Alle Module -- identische Infrastruktur.

2. ZUGANGSKONTROLLE

Ziel: Zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

2.1 Authentifizierung (Firebase Authentication)

Grundlegende Authentifizierung (alle Module):

- E-Mail/Passwort-basierte Anmeldung
- Passwortanforderungen: Mindestlänge, Komplexität
- Passwort-Hashing mit bcrypt (Industry Standard)
- Automatische Sitzungsverwaltung
- Automatischer Logout nach Inaktivität (konfigurierbar)

Sitzungsverwaltung (alle Module):

- Sichere Session-Tokens (Firebase ID Tokens)
- Token-Ablauf nach konfigurierbarer Zeit (Standard: 1 Stunde)
- Automatische Token-Erneuerung bei Aktivität
- Secure Cookie-Flags (HttpOnly, Secure, SameSite)

2.2 Single Sign-On (SSO)

Microsoft 365 Integration (sofern aktiviert -- primär HaiSoTec-Tickets):

- OAuth 2.0 Protokoll
- Verfügbar für alle lizenzierten Benutzer
- Benutzer stellt Verbindung zu persönlichem Microsoft 365-Konto her
- Keine Speicherung von Passwörtern
- Verschlüsselte Token-Speicherung (AES-256)

2.3 Zugriffsprotokolle



Google Cloud Audit Logs (alle Module):

- Google Cloud Platform erstellt automatisch Audit-Logs für alle Firebase-Services
Erfassung von Authentifizierungsereignissen und Datenzugriffen auf
Infrastrukturebene Zugriff über die Google Cloud Console
- Aufbewahrung gemäß Google Cloud Logging-Richtlinien

3. ZUGRIFFSKONTROLLE

Ziel: Zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

3.1 Rollenbasierte Zugriffskontrolle (RBAC)

Berechtigungssystem (plattformübergreifend): Alle Module der HaiSoTec-Plattform nutzen ein einheitliches, rollenbasiertes Berechtigungssystem. Der konkrete Umfang der verfügbaren Berechtigungen variiert je nach Modul:

HaiSoTec-Tickets	Projects, Tickets, Orders, Business Partners, Finance, Contracts	21 granulare Berechtigungen in 6 Kategorien
HaiSoTec-Time	Zeiterfassung, Abwesenheiten, Auswertungen, Genehmigungen	Zugriff auf Zeitdaten, Abwesenheitsmanagement, Berichtswesen
HaiSoTec-People	Mitarbeiterdaten, Dokumente, Organisation, Qualifikationen	Zugriff auf Personalstammdaten, Dokumentenverwaltung, Organisationsstrukturen
HaiSoTec-Vorgano	Aufträge, Aufgaben, Geschäftspartner, Artikel, Lager	Zugriff auf Auftrags- und Vorgangsdaten, Partnerverwaltung

Berechtigungskonzepte (alle Module):

- Admin-Rolle: Vollzugriff auf alle Funktionen des jeweiligen Moduls
- Benutzerdefinierte Rollen: Individuelle Berechtigungskombinationen
- Read-Only-Zugriff: Nur Lesezugriff ohne Änderungserechtigung
- Need-to-Know-Prinzip: Zugriff nur auf die für die jeweilige Aufgabe erforderlichen Daten

Modulspezifische Besonderheit -- HaiSoTec-People: Aufgrund der erhöhten Sensibilität von



Personaldaten gelten für HaiSoTec-People zusätzliche Zugriffsbeschränkungen:

- Personalakten-Dokumente sind nur für berechtigte HR-Rollen zugänglich
- Zugriffe auf sensible Personaldaten werden gesondert protokolliert
- Keine automatische Sichtbarkeit von Personalstammdaten für andere Benutzer

3.2 Firestore Security Rules

Datenbankebene (alle Module):

- Serverseitige Zugriffskontrolle direkt in der Datenbank
- Automatische Validierung jeder Lese-/Schreibanfrage
- Kein Zugriff ohne gültige Authentifizierung
- Berechtigungsprüfung auf Dokumentenebene
- Unterbindung von direkten Datenbank-Zugriffen

Mandantentrennung (alle Module):

- Logische Trennung der Daten nach Organisationen
- Kein Zugriff auf Daten anderer Kunden
- Isolation durch Firestore Collections und Security Rules

3.3 API-Zugriffskontrolle

Cloud Functions (alle Module):

- Authentifizierungsprüfung bei jedem API-Call
- Berechtigungsprüfung auf Funktionsebene
- Rate Limiting zur Verhinderung von Missbrauch
- CORS-Konfiguration für Web-Security

4. WEITERGABEKONTROLLE

Ziel: Zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

4.1 Verschlüsselung in Übertragung (alle Module)

HTTPS/TLS Verschlüsselung:

- Mindestversion: TLS 1.2
- Empfohlene Version: TLS 1.3
- Cipher Suites: Nur moderne, sichere Verschlüsselungsalgorithmen
- Perfect Forward Secrecy (PFS): RSA und ECDSA Diffie-Hellman Schlüsselaustausch
- HTTPS-Erzwingung: Automatische Umleitung von HTTP zu HTTPS



- HSTS-Header: HTTP Strict Transport Security

Zertifikatsverwaltung:

- Automatische SSL/TLS-Zertifikate durch Firebase Hosting
- Automatische Erneuerung vor Ablauf
- Let's Encrypt oder Google-managed Zertifikate

4.2 Verschlüsselung im Ruhezustand (alle Module)

Datenbank (Firestore):

- Verschlüsselung: AES-256
- Schlüsselverwaltung: Google-managed encryption keys
- Automatisch: Keine Konfiguration erforderlich
- Transparenz: Verschlüsselung ohne Leistungseinbußen

Cloud Storage (Dateien):

- Verschlüsselung: AES-256
- Automatisch: Alle hochgeladenen Dateien verschlüsselt
- Schlüsselrotation: Automatische Rotation durch Google

Anwendungsebene (zusätzlich):

- OAuth-Tokens: AES-256-CBC Verschlüsselung vor Speicherung
- Verschlüsselungsschlüssel: In Firebase Environment Variables (nicht im Code)
- Initialization Vector (IV): Einzigartig pro Token

4.3 Netzwerksicherheit (alle Module)

Google Cloud Netzwerk:

- Private Hochgeschwindigkeitsverbindungen zwischen Rechenzentren
- Automatische DDoS-Abwehr (Distributed Denial of Service)
- Intrusion Detection Systems (IDS)
- Firewall-Regeln auf Netzwerkebene

Application-Level:

- Content Security Policy (CSP) Headers
- X-Frame-Options (Clickjacking-Schutz)
- X-Content-Type-Options (MIME-Sniffing-Schutz)
- Referrer-Policy



5. EINGABEKONTROLLE

Ziel: Zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

5.1 Audit-Logging

Google Cloud Audit Logs (alle Module):

- Google Cloud Platform erstellt automatisch Audit-Logs für alle Firebase-Services
- Erfassung von Authentifizierungsereignissen und Datenzugriffen
- Zugriff über Google Cloud Console
- Aufbewahrung gemäß Google Cloud Logging-Richtlinien

Datenänderungs-Protokollierung (alle Module):

- History-Collections für alle wesentlichen Geschäftsobjekte:

Modul	Protokollierte Objekte
HaiSoTec-Tickets	Tickets, Kommentare, Projekte, Zeiteinträge
HaiSoTec-Time	Arbeitszeitbuchungen, Abwesenheitsanträge, Genehmigungen
HaiSoTec-People	Mitarbeiterstammdaten, Dokumenten-Uploads, Organisationsänderungen
HaiSoTec-Vorgano	Aufträge, Aufgaben, Geschäftspartner, Bestandsbewegungen

Für alle Objekte gilt:

- Wer hat was wann geändert
- Alte und neue Werte
- Änderungsgrund (optional)
- Unveränderbar (read-only)

Versionierung (alle Module):

- Automatische Versionierung von Dokumenten
- Nachvollziehbarkeit aller Änderungen
- Wiederherstellung früherer Versionen möglich (Admin)



5.2 Unveränderbarkeit von Logs (alle Module)

Firestore Rules:

- History-Einträge können nicht gelöscht oder geändert werden
- Nur Lesezugriff für autorisierte Nutzer
- Nur System kann History-Einträge erstellen

5.3 Metadaten (alle Module)

Automatische Metadaten:

- createdAt: Timestamp der Erstellung
- createdBy: User-ID des Erstellers
- updatedAt: Timestamp der letzten Änderung
- updatedBy: User-ID des letzten Bearbeiters
- Bei Löschung: deletedAt, deletedBy

6. AUFTRAGSKONTROLLE

Ziel: Zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

6.1 Vertragliche Regelung (alle Module)

- Dieser Vertrag: Definiert die Weisungen
- Anhänge A1-A4: Modulspezifische Verarbeitungsbeschreibungen
- Anhang B: Zentrale Verarbeitungsbeschreibung
- Lizenzvertrag/Partnervertrag: Zugrundeliegende Vereinbarung

6.2 Technische Umsetzung (alle Module)

Konfigurierbarkeit durch Auftraggeber: Der Auftraggeber konfiguriert die Module selbst über die bereitgestellte Benutzeroberfläche:

Modul	Konfigurationsmöglichkeiten
HaiSoTec-Tickets	Benutzerkonten, Berechtigungen, Ticketstatus, Kategorien, Prioritäten, Projekte, Vorlagen
HaiSoTec-Time	Benutzerkonten, Arbeitszeitmodelle, Abwesenheitsarten, Genehmigungsworkflows



HaiSoTec-People	Benutzerkonten, Organisationsstrukturen, Dokumentenkategorien, Qualifikationstypen
HaiSoTec-Vorgano	Benutzerkonten, Auftragsstatus, Artikelkategorien, Lagerorte, Geschäftspartnertypen

Der Auftragnehmer unterstützt bei der initialen Einrichtung im Rahmen des Onboarding-Prozesses, übernimmt jedoch keine laufende Konfiguration für den Auftraggeber.

Keine Eigen-Verarbeitung (alle Module):

- Daten werden nur für Systemzwecke verwendet
- Keine Analyse für eigene Zwecke
- Keine Weitergabe an Dritte (außer Sub-Prozessoren)
- Keine Verwendung für Marketing

6.3 Unterauftragsverarbeiter

Dokumentierte Sub-Prozessoren (für alle Module):

- Liste in Anhang D
- Google Cloud Platform (Infrastruktur -- alle Module)
- Microsoft (E-Mail-Integration -- primär HaiSoTec-Tickets)

Vertragliche Absicherung:

- Google Cloud DPA
- Microsoft DPA
- EU-Standardvertragsklauseln

7. VERFÜGBARKEITSKONTROLLE

Ziel: Zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

7.1 Backup-Strategie (alle Module)

Automatische Backups (Firestore):

- Häufigkeit: Täglich automatisch
- Aufbewahrung: 30 Tage
- Umfang: Vollständige Firestore-Datenbank -- umfasst Daten aller Module (Tickets,



Zeiteinträge, Personaldaten, Aufträge, Kommentare, Benutzerprofile, Projekte, Geschäftspartner etc.) Standort: EU-Rechenzentren (getrennt vom Produktivsystem)

- Verschlüsselung: AES-256

Point-in-Time Recovery (Firestore):

- Wiederherstellung auf beliebigen Zeitpunkt innerhalb 7 Tage
- Granulare Wiederherstellung einzelner Dokumente möglich

BigQuery-Daten (SAP-Integration, sofern aktiviert):

- Keine separaten Backups: BigQuery dient als direkte Synchronisation mit dem SAP-System Datenhaltung: SAP-Stammdaten werden in Echtzeit vom SAP-System gespiegelt
- Verantwortlichkeit: Datensicherung erfolgt durch das SAP-System des Auftraggebers Zugriff: Nur lesender Zugriff (Read-Only) auf SAP-Daten

7.2 Hochverfügbarkeit (alle Module)

Firestore:

- Multi-Region Replication: Automatische Replikation über mehrere Rechenzentren Verfügbarkeit: Gemäß Firestore Service Level Agreement (Multi-Region)
- Automatisches Failover: Bei Ausfall eines Rechenzentrums

Firebase Hosting:

- Global CDN: Content Delivery Network weltweit
- Verfügbarkeit: Gemäß Firebase Hosting Service Level Agreement
- Automatische Skalierung: Bei Lastspitzen

Cloud Functions:

- Verfügbarkeit: Gemäß Cloud Functions Service Level Agreement
- Automatische Skalierung: Nach Bedarf
- Redundanz: Über mehrere Zonen

7.3 Disaster Recovery (alle Module)

Business Continuity Plan:

- Dokumentierte Wiederherstellungsprozesse
- Recovery Time Objective (RTO): < 4 Stunden
- Recovery Point Objective (RPO): < 1 Tag



- Regelmäßige Wiederherstellung Tests

Notfallkontakt:

- 24/7 Google Cloud Support
- Eskalationsprozesse definiert
- Kontaktinformationen dokumentiert

8. TRENNUNGSKONTROLLE

Ziel: Zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

8.1 Mandantentrennung (alle Module)

Firestore Collections:

- Separate Collections pro Kunde (Mandant)
- Keine Überschneidung von Daten
- Isolation durch Security Rules

User-Isolation:

- User gehören zu genau einem Kunden
- Kein Zugriff auf Daten anderer Kunden
- Validierung auf Anwendungs- und Datenbankebene

8.2 Zweckbindung (alle Module)

Datenkategorisierung:

- Klare Trennung von Produktivdaten und Logging-Daten
- Unterschiedliche Aufbewahrungsfristen
- Separate Speicherorte

Modulübergreifende Trennung:

- Daten der verschiedenen Module sind logisch getrennt
- Verknüpfungen zwischen Modulen erfolgen nur über definierte Schnittstellen
- Kein unkontrollierter Datenaustausch zwischen Modulen

Zugriffstrennung:

- Getrennte Berechtigungen für unterschiedliche Datenarten und Module
- Finance-Daten nur mit spezifischer Berechtigung sichtbar
- Personaldaten (HaiSoTec-People) nur für berechtigte HR-Rollen zugänglich
- Anonymisierte Analytics getrennt von personenbezogenen Daten



8.3 Umgebungstrennung (alle Module)

Entwicklung vs. Produktion:

- Separate Firebase-Projekte
- Keine Produktivdaten in Entwicklung
- Test-Daten sind synthetisch/anonymisiert

9. DATENSCHUTZ-MANAGEMENT

9.1 Verantwortlichkeiten (plattformübergreifend)

Datenschutz-Ansprechpartner:

- Name: Moritz Mueller (Geschäftsführer)
- E-Mail: info@haisotec.de
- Telefon: +49 7474 3199680
- Eskalationswege: Direkt an Geschäftsführung

Hinweis zur Datenschutzbeauftragten-Pflicht: Der Auftragnehmer hat keinen Datenschutzbeauftragten bestellt, da die gesetzliche Bestellpflicht gemäß Art. 37 Abs. 1 lit. b und c DSGVO nicht vorliegt (weniger als 20 Mitarbeiter mit regelmäßiger Verarbeitung personenbezogener Daten und keine Kerntätigkeit in systematischer Überwachung).

Mitarbeiter-Schulung:

- Regelmäßige Datenschutz-Schulungen
- Verpflichtung auf Vertraulichkeit
- Awareness-Maßnahmen

9.2 Incident Response (alle Module)

Prozess bei Datenschutzverletzungen:

- Erkennung: Monitoring und Alerting
- Bewertung: Schweregrad-Einschätzung (inkl. Identifikation betroffener Module)
- Eindämmung: Sofortmaßnahmen
- Meldung: An Auftraggeber innerhalb 24h
- Dokumentation: Vollständige Vorfälle Dokumentation (inkl. betroffener Module und Datenkategorien) Nachbereitung: Lessons Learned, Verbesserungen

Benachrichtigung:

- E-Mail an Auftraggeber-Kontakt
- Telefonischer Kontakt bei kritischen Vorfällen



- Schriftlicher Bericht innerhalb 48h

9.3 Datenschutz by Design & Default (alle Module)

Privacy by Design:

- Datenschutz von Anfang an berücksichtigt
- Datensparsamkeit als Grundprinzip
- Pseudonymisierung wo möglich

Privacy by Default:

- Restriktivste Einstellungen als Standard
- Benutzer müssen aktiv Verbindung zu Microsoft 365 herstellen (OAuth-Zustimmung) Keine unnötige Datenerhebung
- Neue Module folgen denselben Datenschutzprinzipien

10. AKTUALISIERUNG UND WARTUNG

10.1 Software-Updates (alle Module)

Automatische Updates:

- Sicherheitspatches automatisch eingespielt
- Keine Ausfallzeiten bei Updates
- Versionierung für Rollback-Möglichkeit

Change Management:

- Dokumentation aller Änderungen
- Risikobewertung vor kritischen Updates
- Kommunikation an Kunden bei größeren Änderungen

10.2 Zertifizierungen

Regelmäßige Audits:

- Jährliche Überprüfung der TOMs
- Externe Audits durch Google für Rechenzentren
- Anpassung an aktuelle Standards

Nachweise:

- ISO 27001, ISO 27017, ISO 27018 Zertifikate
- SOC 2 Type II Reports
- BSI C5 Attestation



11. ZUSAMMENFASSUNG DER SICHERHEITSMASSNAHMEN

Kategorie	Massnahme	Technologie/ Standard	Gilt für
Zutrittskontrolle	Physische Sicherheit	Google Cloud Rechenzentren, ISO 27001	Alle Module
Zugangskontrolle	Authentifizierung	Firebase Auth (E-Mail/Passwort), bcrypt	Alle Module
Zugriffskontrolle	Autorisierung	RBAC (modulspezifische Permissions), Firestore Rules	Alle Module
Weitergabekontrolle	Verschlüsselung Transit	TLS 1.2+, HTTPS	Alle Module
Weitergabekontrolle	Verschlüsselung Rest	AES-256 (Firestore, Storage)	Alle Module
Eingabekontrolle	Logging	Google Cloud Audit Logs (Infrastruktur), History Collections (Anwendung)	Alle Module
Auftragskontrolle	Vertragliche Basis	Dieser AVV, DPAs mit Sub-Prozessoren	Alle Module
Verfügbarkeitskontrolle	Backups	Täglich für Firestore (30 Tage), BigQuery ist SAP-Sync	Alle Module
Verfügbarkeitskontrolle	Hochverfügbarkeit	Multi-Region Replication, automatisches Failover	Alle Module
Trennungskontrolle	Mandantentrennung	Firestore Collections, Security Rules	Alle Module



HaiSoTec GmbH

Dieses Dokument ist Bestandteil des Auftragsverarbeitungsvertrags der HaiSoTec GmbH.



HaiSoTec GmbH

ANHANG D: GENEHMIGTE UNTERAUFTRAGSVERARBEITER

Bestandteil des Auftragsverarbeitungsvertrags (AVV) der HaiSoTec GmbH

Dokument: ANHANG_D_GENEHMIGTE UNTERAUFTRAGSVERARBEITER_V1.0

Version: 1.0 Stand: 15.03.2026



HaiSoTec GmbH

Inhaltsverzeichnis

1. Google LLC (Google Cloud Platform).....	3
2. Microsoft Corporation.....	4
3. Hinzufügung weiterer Unterauftragsverarbeiter.....	5
4. Übersicht -- Genehmigte Sub-Prozessoren.....	5



Dieser Anhang gilt für alle Module der HaiSoTec-Plattform, da sämtliche Module auf derselben technischen Infrastruktur betrieben werden.

1. Google LLC (Google Cloud Platform)

Parameter	Details
Firmenname	Google LLC
Anschrift	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
Verarbeitungsstandort	EU/EWR (Primär: Frankfurt, Deutschland; Sekundär: Belgien)
Leistung/Zweck	Cloud-Infrastruktur, Hosting, Datenbank (Firestore), Authentifizierung (Firebase Auth), Cloud Functions, Cloud Storage, BigQuery
Betroffene Module	Alle Module der HaiSoTec-Plattform
Art der verarbeiteten Daten	Alle im System verarbeiteten personenbezogenen Daten (siehe Anhang B und Anhänge A1-A4)
Datenverarbeitung	Ausschließlich in der EU/EWR, keine Übermittlung in Drittländer
Zertifizierungen	ISO 27001, ISO 27017, ISO 27018, SOC 2 Type II, BSI C5
Vertrag	Google Cloud Data Processing Addendum: https://cloud.google.com/terms/data-processing-addendum
Sub-Prozessor-Liste	https://cloud.google.com/terms/subprocessors
Rechtliche Absicherung	EU-Standardvertragsklauseln (SCCs) als zusätzliche Absicherung enthalten, obwohl keine Drittland Übermittlung erfolgt

Vorbereitungstätigkeiten im Detail:

- Bereitstellung der Cloud-Infrastruktur für alle Module
- Hosting der Webanwendung (Firebase Hosting)



- Datenbank-Services (Cloud Firestore)
- Authentifizierungs-Services (Firebase Authentication)
- Serverless Computing (Cloud Functions)
- Dateispeicherung (Cloud Storage)
- BigQuery-Anbindung für SAP-Daten (sofern SAP-Integration aktiviert)

2. Microsoft Corporation

Parameter	Details
Firmenname	Microsoft Corporation
Anschrift	One Microsoft Way, Redmond, WA 98052, USA
Verarbeitungsstandort	EU/EWR (Microsoft 365 EU Data Boundary)
Leistung/Zweck	E-Mail-Integration über Microsoft 365 / Graph API fuer Ticket-Erstellung aus E-Mails
Betroffene Module	HaiSoTec-Tickets (primär), weitere Module sofern M365-Integration freigeschaltet
Verfügbarkeit	Für alle lizenzierten Benutzer verfügbar
Art der verarbeiteten Daten	E-Mail-Betreff, E-Mail-Inhalt, Absender/Empfänger, E-Mail-Anhänge; OAuth-Zugriffstokens (verschlüsselt)
Datenverarbeitung	Ausschließlich in der EU/EWR (Microsoft 365 EU Data Boundary), keine Übermittlung in Drittländer
Zertifizierungen	ISO 27001, ISO 27017, ISO 27018, SOC 2
Vertrag	Microsoft Products and Services DPA: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
Rechtliche Absicherung	EU-Standardvertragsklauseln (SCCs) als zusätzliche Absicherung enthalten, obwohl keine Drittland Übermittlung erfolgt

Besonderheiten

- Diese Integration ist für alle lizenzierten Benutzer verfügbar
- Nutzer können die Verbindung zu ihrem Microsoft 365-Konto erstellen



Nutzer erteilen individuelle OAuth-Zustimmung für den Zugriff auf ihr Postfach Nutzer können die Verbindung jederzeit trennen

- Tokens werden verschlüsselt gespeichert (AES-256)

Vorbereitungstätigkeiten im Detail:

- Zugriff auf Postfach des Endnutzers (nur lesend, nach OAuth-Zustimmung) Abruf von E-Mails zur Ticket-Erstellung
- Keine Speicherung vollständiger E-Mails
- Nur Extraktion relevanter Informationen für Tickets

3. Hinzufügung weiterer Unterauftragsverarbeiter

Benachrichtigungsverfahren:

- Auftragnehmer informiert Auftraggeber mindestens 30 Tage im Voraus per E-Mail Mitteilung enthält: Name, Standort, Leistung, Garantien des neuen Sub-Prozessors, betroffene Module Auftraggeber hat 30 Tage Widerspruchsrecht
- Bei berechtigtem Widerspruch: Verzicht auf Sub-Prozessor oder Kündigungsrecht

Kriterien für neue Sub-Prozessoren:

- Gleichwertiges Datenschutzniveau wie dieser Vertrag
- Zertifizierungen (ISO 27001 oder gleichwertig)
- Schriftlicher Vertrag mit Datenschutzklauseln
- Datenverarbeitung ausschließlich innerhalb der EU/des EWR
- EU-Standardvertragsklauseln (SCCs) als zusätzliche Absicherung

4. Übersicht -- Genehmigte Sub-Prozessoren

Nr.	Unternehmen	Leistung	Standort	Betroffene Module	Status
1	Google LLC	Cloud-Infrastruktur	EU (DE, BE)	Alle Module	Aktiv
2	Microsoft Corporation	E-Mail-Integration	EU	Tickets (primär)	Aktiv

Dieses Dokument ist Bestandteil des Auftragsverarbeitungsvertrags der HaiSoTec GmbH.