Vertrag über die Verarbeitung personenbezogener Daten

– nachfolgend „Vertrag“ genannt –

zwischen

(Firmenname)
(Adresse)

– nachfolgend **„Auftraggeber“** oder „Verantwortlicher“ –

und

Haiilo GmbH
Gasstraße 6a, 22761 Hamburg

– nachfolgend **„Auftragnehmer“** oder „Auftragsverarbeiter“ –

einzeln oder gemeinsam auch **„Partei“** und / oder „Parteien“

1. Rechtsgrundlage, Gegenstand, Dauer des Vertrages

1) Dieser Vereinbarung liegen die Bestimmungen der EU-Datenschutzgrundverordnung (DSGVO) zu Grunde.
2) Gegenstand dieses Vertrages ist die Erhebung und Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Verantwortlichen in dessen Auftrag und nach dessen Weisung im Zusammenhang mit den jeweiligen Bedingungen der Cloud-Dienste. Zweck der Auftragsverarbeitung ist die Bereitstellung und Betriebsführung der Software sowie deren Sicherstellung gemäß der Beschreibung im **Annex 1**. Art und Umfang der Verarbeitung, der personenbezogenen Daten sowie die Kategorien betroffener Personen ergeben sich ebenso aus **Annex 1**.
3) Die Dauer dieses Vertrages richtet sich nach der Dauer des Bestehens eines Verarbeitungszweckes gem. Abs. 2 dieser Ziffer, sofern sich aus den nachfolgenden Bestimmungen nicht ein anderes ergibt. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

2. Rechte und Pflichten des Verantwortlichen

1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenübermittlung an den Auftragnehmer sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich.
2) Der Auftragnehmer wird personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu der Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.
3) Der Auftragnehmer wird nur ausreichend qualifizierte und zuverlässige Kräfte mit der Datenverarbeitung betrauen. Insbesondere wird der Auftragnehmer die Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf die Wahrung des Datengeheimnisses (Verschwiegenheitspflicht) verpflichten und über die sich aus der Datenverarbeitung ergebenden Datenschutzpflichten sowie bestehende Weisungs- bzw. Zweckbindung belehren.
4) Der Auftragnehmer bestellt einen Datenschutzbeauftragten. Dieser ist unter dpo@haiilo.com erreichbar. Ein Wechsel des Datenschutzbeauftragten wir dem Auftraggeber unverzüglich mitgeteilt.
5) Die Parteien unterstützen sich gegenseitig, zeitnah und umfänglich bei der Prüfung möglicher Verstöße und der Abwehr von Ansprüchen betroffener Personen oder Dritter sowie der Abwehr von Sanktionen durch Aufsichtsbehörden. Der Auftragnehmer unterstützt den Auftraggeber insbesondere dabei, dessen Aufgaben nach den Art. 32 bis 36 DSGVO zu erfüllen sowie dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte betroffener Personen nachzukommen.
6) Der Auftragnehmer stellt dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist jederzeit alle verfügbaren Auskünfte und Nachweise bereit, die zur Beurteilung der Vertragsgemäßheit der Datenverarbeitung erforderlich sind. Der Auftraggeber überzeugt sich vor

der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der in diesen Vertrag vereinbarten Regelungen zum Schutz der personenbezogenen Daten, insbesondere von der Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert dieses Ergebnis. Hierfür kann er beispielsweise

a) Selbstauskünfte des Auftragnehmers einholen,
b) sich ein Testat eines Sachverständigen bzw. Zertifikate vorlegen lassen oder
c) nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

Bei Verdacht auf Verletzungen vertraglicher Verpflichtungen des Auftragnehmers bzw. der bei ihm zur Auftragsverarbeitung beschäftigten Personen oder sonstigen Verstößen gegen datenschutzrechtliche Bestimmungen wird der Auftragnehmer den Auftraggeber unverzüglich in Textform informieren.

3. Technische und organisatorische Maßnahmen

1) Der Auftraggeber und der Auftragnehmer werden geeignete technische und organisatorische Maßnahmen (TOM) zur Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, sodass ein den einschlägigen datenschutzrechtlichen Bestimmungen – insbesondere der DSGVO – angemessenes Schutzniveau gewährleistet werden kann.
2) Die von den Parteien zum Zwecke dieser Vereinbarung als geeignet befundenen TOM des Auftragnehmers sind in **Annex 2** aufgeführt und beschrieben.
3) TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternativ adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind abzustimmen und zu dokumentieren.

4. Rückgabe und Löschung

Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Dies betrifft auch etwaiges Test- und Ausschussmaterial. Die Parteien werden sich nach dem Herausgabeverlangen auf weitere Modalitäten der Rückgabe (z.B. Format, Frist) einigen.

5. Unterauftragsverarbeiter

1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in **Annex 3** genannten Unterauftragsverarbeiter durchgeführt. Der Auftragnehmer ist im Rahmen dieses Vertrages zur Begründung von weiteren Unterauftragsverhältnissen zur Leistungserbringung befugt.
2) Der Auftragnehmer wählt Unterauftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit aus. Der Auftragnehmer ist verpflichtet, die Unterauftragsverarbeiter entsprechend dieser Vereinbarung zu verpflichten. Er stellt insbesondere sicher, dass der Verantwortliche seine Rechte aus dieser Vereinbarung auch direkt gegenüber den Unterauftragsverarbeiter wahrnehmen kann, die Unterauftragsverarbeiter hinreichende Garantien dafür bieten, dass sie denselben Datenschutzpflichten unterliegen wie der Auftragnehmer und die TOM der Unterauftragsverarbeiter so durchgeführt werden, dass sie den Anforderungen dieser Vereinbarung entsprechen. Der Auftragsverarbeiter hat dem Verantwortlichen auf dessen schriftliche Aufforderung Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erteilen; dies umfasst erforderlichenfalls auch die Einsicht in die relevanten Vertragsunterlagen.

3) Der Auftragnehmer informiert den Verantwortlichen per E-Mail über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen binnen 14 Tagen wegen eines wichtigen Grundes Einspruch zu erheben. Dem Auftragnehmer steht ein außerordentliches Kündigungsrecht gem. Ziffer 2 Abs. 3 zu, wenn der Verantwortliche der Einbindung des Unterauftragsverarbeiters ohne wichtigen Grund widerspricht.

4) Als Unterauftragsverarbeiter gelten auch Auftragsverarbeiter des Unterauftragsverarbeiters. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Aufträge zu verstehen, die der Auftragsverarbeiter Dritten zur Unterstützung bei der Auftragsdurchführung erteilt und die keine Verarbeitungsleistungen von Daten des Verantwortlichen beinhalten. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind insbesondere Nebenleistungen zu verstehen, die der Anbieter z.B. als Telekommunikationsleistung, Post-/Transportdienstleistung, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahme zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

5) Die Übermittlung personenbezogener Daten in Länder außerhalb des EWR darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. durch die Übernahme von Standardvertragsklauseln, die von der Europäischen Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 in ihrer Fassung vom 4. Juni 2021 angenommen wurden).

6. Haftung

1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadenersatz verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten, soweit Pflichten aus diesem Vertrag verletzt wurden.

2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

7. Sonstiges

1) Diese Vereinbarung zur Auftragsverarbeitung löst sämtliche vorangegangenen Regelungen zur Auftragsverarbeitung.

2) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll eine wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung bzw. dem von den Parteien Gewollten am nächsten kommt.

3) Es gilt deutsches Recht einschließlich EU-Rechts wie der DSGVO. Der Gerichtsstand ist Hamburg, Deutschland.

4) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung.

ANNEXE

Nachstehende Annexe sind feste Bestandteile dieser Vereinbarung:

Annex 1: Einzelheiten der Datenverarbeitung

Annex 2: Technische und organisatorische Sicherheitsmaßnahmen

Annex 3: Genehmigte Unterauftragsverarbeiter

Für den Verantwortlichen	**Für den Auftragsverarbeiter**
Ort, Datum	Ort, Datum
Unterschrift	Unterschrift
Name	Name
Funktion	Funktion

Annex 1

Einzelheiten der Datenverarbeitung

1. **Beschreibung der Verarbeitungstätigkeit**
   Im Wesentlichen handelt es sich um folgende Aufgaben durch den Auftragnehmer:

- Bereitstellung der Software, die ihren Nutzern die Zusammenarbeit und Kommunikation ermöglicht und verschiedene Funktionen bietet.
- Hosting von Daten des Auftraggebers auf einer IT-Infrastruktur, die vom Auftragnehmer und seinen Erfüllungsgehilfen bereitgestellt wird.

2. **Betroffenenkategorien, Datenarten, Zugriffsformen**

   a. Kategorien betroffener Personen:
   Grundsätzlich dient die Software der Kommunikation unter Mitarbeitern. Soweit durch den Kunden (Verantwortlicher) beabsichtigt ist, personenbezogene Daten weiterer Kategorien in der Software zu verarbeiten, wäre dies nachfolgend durch den Verantwortlichen kenntlich zu machen:

   _____

   b. Betroffene personenbezogene Daten
   Es werden folgende Kategorien personenbezogener Daten verarbeitet:

   - Nachname/Vorname
   - Profildaten (z.B. Telefon, E-Mail)
   - Nutzerinhalte und -interaktionen
   - IP-Adresse
   - Metadaten

   Soweit der Verantwortliche weitere Datenarten in der Software verwenden möchte, wäre dies nachfolgend durch den Verantwortlichen kenntlich zu machen:

   _____

   c. Sensible Daten / Besondere Kategorien von Daten i.S.v. Art. 9 DSGVO:
   Zur Nutzung der Software werden keine sensiblen Daten benötigt. Soweit der Verantwortliche sensible Daten in der Software verarbeiten möchte, so ist dies durch den Verantwortlichen zu ergänzen:

   _____

Haiilo

Annex 2

Technische und organisatorische Sicherheitsmaßnahmen

Dieser Annex konkretisiert die im Vertrag zur Auftragsverarbeitung getroffenen technischen und organisatorischen Maßnahmen.

1. Organisation der Informationssicherheit

Haiilo hat eine Abteilung für Informationssicherheit eingerichtet, die von der Unternehmensleitung unterstützt wird, um sicherzustellen, dass unsere Mitarbeiter über die erforderlichen Fähigkeiten und Kenntnisse im Bereich der Informationssicherheit verfügen.

Die Maßnahmen umfassen:

a) Haiilo beschäftigt Mitarbeiter, die sich in Vollzeit der Informationssicherheit widmen.
b) Haiilo verfügt über einen Sicherheitslenkungsausschuss, der sich aus verschiedenen Abteilungen zusammensetzt, um die Belange der Informationssicherheit in verschiedenen Bereichen der Organisation zu behandeln.
c) Das Informationssicherheitspersonal ist direkt der Geschäftsleitung unterstellt.
d) Bei Haiilo gelten eine Reihe umfassender Sicherheitsrichtlinien, die von der Geschäftsleitung genehmigt und innerhalb des Unternehmens kommuniziert werden.
e) Alle Mitarbeiter haben Vertraulichkeitsvereinbarungen unterzeichnet, die rechtlich geprüft wurden und für die Zeit des Arbeitsverhältnisses und darüber hinaus gelten.
f) Die Nichteinhaltung der Informationssicherheitsrichtlinien durch das bei Haiilo beschäftigte Personal kann zu Disziplinarmaßnahmen führen und Sanktionen nach sich ziehen bis hin zur außerordentlichen Kündigung des Arbeitsverhältnisses
g) Alle Mitarbeiter erhalten routinemäßige Schulungen zur Informationssicherheit über verschiedene Medien wie Videos, interaktive Schulungen, Poster und Ankündigungen. Sie müssen während des Einführungsprozesses und anschließend vierteljährlich ein Informationssicherheitstest absolvieren und bestehen. Darüber hinaus wird das gesamte Personal bei der Einarbeitung in den Datenschutz geschult. Mitarbeiter in spezialisierten technischen Funktionen nehmen darüber hinaus an rollenspezifischen Sicherheitsschulungen teil, die auf ihre Aufgaben zugeschnitten sind.
h) Das Managementsystem für die Informationssicherheit unterliegt einer ständigen Überprüfung und Verbesserung.

2. Managementsystem für Informationssicherheit

Haiilo hat ein Informationssicherheitsmanagementsystem (ISMS) eingeführt, um die Risiken im Zusammenhang mit der Sicherheit von Kunden- und Personaldaten zu bewerten, die Bewertung und Minderung dieser Risiken zu überwachen und die Maßnahmen zur Informationssicherheit ständig zu verbessern.

Die Maßnahmen umfassen:

a) Haiilo hat ein ISMS eingeführt, um Sicherheitsfragen professionell zu behandeln. Sowohl Haiilo als auch sein ISMS werden regelmäßig von einem unabhängigen externen Prüfer überprüft und sind nach der Norm ISO/IEC 27001:2022 sowie SOC 2 Typ II oder einer späteren Version zertifiziert.
b) ISO/IEC 27001:2022 und SOC 2 sind globale Standards, die Kriterien für die Einrichtung, Ausführung, Aufrechterhaltung und Verbesserung eines ISMS beschreiben und die Bewertung und Minderung von Informationssicherheitsrisiken umfasst. Eine Kopie unseres ISO27001-Zertifikats und SOC 2 Berichts kann auf Anfrage via trust.haiilo.com zur Verfügung gestellt werden.

3. Physischer Zugang

Der Zugriff auf die Datenverarbeitungssysteme von Haiilo erfolgt ausschließlich durch autorisierte und authentifizierte Nutzer.

Die Maßnahmen umfassen:

a) Haiilo betreibt seine Produkte über eine ISO-Familie, die ISO27001-zertifizierte und SOC2-akkreditierte Drittanbieter für Cloud-Hosting umfasst. Die Rechenzentren verfügen über klar definierte und geschützte physische Sicherheitsgrenzen, robuste Zugangskontrollrichtlinien, kontrollierte Liefer- und Ladezonen, Überwachungssysteme und Sicherheitspersonal rund um die Uhr. Nur befugtes Personal hat Zugang zu den Räumlichkeiten dieser Rechenzentren.
b) Strom- und Telekommunikationskabel, die Personaldaten transportieren oder Informationsdienste in den Rechenzentren unterstützen, sind gegen Abhören, Störungen und Beschädigungen geschützt.
c) Die Rechenzentren haben physische Schutzmaßnahmen gegen Naturkatastrophen, böswillige Angriffe und Unfälle getroffen.
d) Die Rechenzentren verfügen über einen Notfallplan für Stromausfälle, der sicherstellt, dass die Rechenzentren auch bei einem Stromausfall nahtlos weiterarbeiten.
Lesen Sie hier mehr über die Daten und die Sicherheit der Rechenzentren.
e) Haiilo verwendet Schlüsselanhänger und Sicherheitsschlösser für den Zugang zu den Büroräumen, alle Haiilo Büros sind mit Kameras an den Eingangstüren des Gebäudes ausgestattet.

4. Zugang zum System

Der Zugang zu personenbezogenen Daten und den internen Systemen von Haiilo wird streng kontrolliert und in Übereinstimmung mit einschlägigen Industriestandards geschützt.

Die Maßnahmen umfassen:

a) Der Zugang zu den internen Systemen von Haiilo ist auf das Personal von Haiilo beschränkt, wobei der Zugang streng nach dem "least privilege"-Grundsatz erfolgt und auf das Maß beschränkt ist, das für die Ausführung und Erfüllung ihrer Aufgaben erforderlich ist.
b) Jeder Nutzerzugang zu allen Systemen des Unternehmens, die mit Haiilo in Verbindung stehen, ist mit einer eindeutigen Kennung (UserID) verknüpft, um die Rückverfolgbarkeit von Aktionen jederzeit zu gewährleisten.
c) Haiilo verwendet, wann immer möglich, Single-Sign-On (SSO)
d) Haiilo setzt eine Passwortrichtlinie um, die die unbefugte Weitergabe von Passwörtern verbietet und im Falle einer Kompromittierung eine Passwortänderung vorschreibt. Alle Passwörter müssen bestimmte Mindestanforderungen erfüllen und werden in verschlüsselter Form in einem Passwortmanagementsystem (1Password) gespeichert. Außerdem verfügt jedes Endgerät über einen passwortgeschützten Bildschirmschoner, der nach 5 Minuten Inaktivität aktiviert wird.
e) Haiilo erzwingt eine Multi-Faktor-Authentifizierung über den Identity Provider (IdP) für den Zugriff auf alle Systeme innerhalb von Haiilo.
f) Haiilo verfügt über ein umfassendes Verfahren zur Deaktivierung von Benutzerkonten und zum Entzug des Zugriffs bei Ausscheiden eines Mitglieds aus dem Unternehmen oder zur Anpassung der Zugriffsrechte, wenn sich seine Rolle ändert.
g) Haiilo setzt geeignete Firewall-Technologien in Übereinstimmung mit den Industriestandards ein, um die verschiedenen Anwendungen, Server und virtuellen Maschinen in den Rechenzentren vor webbasierten Angriffen zu schützen.
h) Haiilo bietet eine breite Palette von Authentifizierungsfunktionen, einschließlich der Möglichkeit für Kunden, ihre eigenen Passwortrichtlinien festzulegen und Unterstützung für SAML 2.0 und OpenID. Kunden haben die Möglichkeit, verschiedene Benutzerverzeichnisse wie Active Directory, LDAP und LDAPS zu verbinden. Auf

Kundenwunsch können Benutzerverzeichnisse auch über Google Workspace oder Microsoft Graph angebunden werden.

5. Datenzugang

Berechtigte Personen, die auf Datenverarbeitungssysteme zugreifen, erhalten nur Zugang zu bestimmten personenbezogenen Daten, zu denen sie berechtigt sind.

Die Maßnahmen umfassen:

a) Haiilo schränkt den Zugang des Personals zu Daten und Systemen nach dem Prinzip "need-to-know" ein.
b) Haiilo führt ein formelles Verfahren zur Überprüfung des Hintergrunds während des Screening-Aufrufs für alle erforderlichen Dokumente durch. Für angehende C-Level-, VP-Level- und Informationssicherheitspersonal wird ein Führungszeugnis verlangt.
c) Die Einführungsschulung umfasst Zugriffsrechte und allgemeine Grundsätze zur Definition und Verwendung personenbezogener Daten.
d) Haiilo setzt die Pseudonymisierung/Anonymisierung von Daten ein, wo dies angemessen und praktikabel ist, um die Wahrscheinlichkeit eines unangemessenen Zugriffs auf personenbezogene Daten zu verringern.
e) Die für Haiilo Produkte verwendete Produktionsumgebung ist von der Entwicklungs- und Testumgebung getrennt. Die Testumgebung verwendet anonymisierte Produktionsdaten, um sicherzustellen, dass keine Kundendaten in den Testdaten enthalten sind.
f) Alle Endnutzergeräte bei Haiilo werden durch Anti-Malware-Software (MalwareBytes) geschützt und sind in ein Mobile Devices Management System (MDM) eingebunden, in dem eine Reihe von Richtlinien durchgesetzt wird. Darüber hinaus werden alle Endnutzergeräte von einer Endpoint Detection and Response Software (Nebula) überwacht.
g) Das Netzwerk in den Haiilo Büros ist durch eine Firewall geschützt, um die Sicherheitsmaßnahmen zu verbessern.

6. Datenübertragung

Sicherstellen, dass Unbefugte während der Übertragung nicht auf Kundendaten zugreifen, sie kopieren, verändern oder löschen können.

Die Maßnahmen umfassen:

a) Der Kundenzugang zu Haiilo-Produkten ist durch TLS1.2 oder höher geschützt.
b) Haiilo verwendet starke Verschlüsselungsmethoden für alle anderen Übertragungen von Kundendaten an externe Netzwerke.

7. Entwicklungsprozess

Haiilo ergreift sowohl administrative als auch technische Maßnahmen, um eine sichere Codeentwicklung zu gewährleisten.

Die Maßnahmen umfassen:

a) Haiilo verfolgt bei der Softwareentwicklung einen Defense-in-Depth-Ansatz und verwendet einen Secure Development Lifecycle (SDLC), der eine breite Palette von Sicherheitstests, Fehlerberichten und Managementverfahren umfasst.
b) Haiilo bietet seinen Softwareentwicklern, Ingenieuren und Qualitätssicherern Schulungen an, die bewährte Entwicklungspraktiken und neue Sicherheitsbedrohungen im Zusammenhang mit der Anwendungssicherheit und der sicheren Codierung umfassen.

c) Die Sicherheitsprüfung umfasst die Durchführung von Peer-Code-Reviews, die Durchführung von Einheitstests, Integrationstests, API-Tests, End-to-End-Tests (E2E) und funktionalen Tests.
d) Alle Änderungen am Code erfolgen über einen geregelten und genehmigten Freigabemechanismus, der im Rahmen eines strukturierten Änderungskontrollprogramms arbeitet. Dieses Programm verfolgt, dokumentiert und genehmigt Änderungswünsche, bevor sie umgesetzt werden.
e) Haiilo führt Penetrationstests durch Dritte auf den verschiedenen Plattformen durch und bewertet sie im Hinblick auf neue Bedrohungen der Anwendungssicherheit. Erkannte Schwachstellen werden umgehend behoben, um die robuste Sicherheitslage der Plattform aufrechtzuerhalten.
f) Alle Verschlüsselungs- und anderen kryptographischen Funktionen, die in Haiilo-Produkten verwendet werden, entsprechen den Industriestandards gemäß BSI, NIST und ISO/IEC.

8. Verfügbarkeit

Personenbezogene Daten werden vor Zerstörung oder Verlust geschützt, und es gibt Maßnahmen, die einen rechtzeitigen Zugang, die Wiederherstellung oder die Verfügbarkeit von Kundendaten im Falle eines Zwischenfalls gewährleisten.

Die Maßnahmen umfassen:

a) Haiilo implementiert Redundanzmaßnahmen, um die Verfügbarkeit und Ausfallsicherheit der Cloud-Infrastruktur zu erhöhen. Die Cloud nutzt redundante Komponenten wie Load Balancer und virtuelle Maschineninstanzen, um eine hohe Verfügbarkeit zu gewährleisten.
b) Rechenzentren verfügen über Wiederherstellungspläne für Stromausfälle, und es sind Generatoren vor Ort vorhanden, um sicherzustellen, dass das Rechenzentrum vor Stromausfällen geschützt ist.
c) Die Rechenzentren werden rund um die Uhr auf Strom-, Netzwerk-, Umwelt- und technische Probleme überwacht.
d) Haiilo erstellt täglich verschlüsselte Sicherungskopien der Kundendaten, welche an einem Ort mit anderen Verfügbarkeitszonen als das primäre Rechenzentrum gespeichert sind. Haiilo hat Maßnahmen zur sofortigen Erkennung von Sicherungsfehlern ergriffen und führt regelmäßig Wiederherstellungstests durch, um die Wirksamkeit und Vollständigkeit der Sicherungskopien sicherzustellen.
e) Haiilo hält sich an einen Business Continuity Plan und einen Disaster Recovery Plan, die regelmäßig überprüft und aktualisiert werden.
f) Haiilo testet regelmäßig die Komponenten des Business Continuity Plans und des Disaster Recovery Plans, die Überprüfung/Übung soll den Prozess verbessern.

9. Datentrennung

Daten, die zu einem Kunden gehören, werden konsequent von den Daten anderer Kunden durch logische oder physische Trennung getrennt gehalten.

Die Maßnahmen umfassen:

a) Haiilo gestaltet seine Systeme so, dass eine logische oder physische Trennung der von verschiedenen Kunden stammenden Kundendaten gewährleistet ist.
b) In jeder Phase der Verarbeitung können die von verschiedenen Kunden erhaltenen Daten unterschieden werden, so dass eine konsequente physische oder logische Trennung der Daten gewährleistet ist.

10. Management von Zwischenfällen

Im Falle einer Sicherheitsverletzung, die Kundendaten betrifft, werden Anstrengungen unternommen, um die Auswirkungen der Verletzung zu minimieren, und der Kunde wird im Einklang mit rechtlichen Anforderungen umgehend benachrichtigt.

Die Maßnahmen umfassen:

a) Haiilo hat eine Richtlinie für den Umgang mit Vorfällen und einen Prozess für das Schwachstellenmanagement implementiert, in dem Rollen und Verantwortlichkeiten sowie Verfahren für die Bewertung und Einstufung von Informationssicherheitsvorfällen festgelegt sind.
b) Haiilo hat Überwachungs- und Protokollierungssysteme in der Cloud-Infrastruktur konfiguriert, um Aufzeichnungen über System- und Anwendungsereignisse zu erstellen.
c) Haiilo unterhält eine synchronisierte Uhr auf allen Systemen, um Untersuchungen im Falle eines Vorfalls zu erleichtern.
d) Im Falle einer Verletzung des Schutzes personenbezogener Daten, die nach geltendem Recht eine Benachrichtigung erfordert, wird Haiilo den Kunden unverzüglich benachrichtigen. Darüber hinaus wird Haiilo auch die zuständige Aufsichtsbehörde ohne unangemessene Verzögerung und innerhalb der gesetzlichen Frist benachrichtigen. Die Benachrichtigung sowohl des Kunden als auch der Behörden wird, soweit nach geltendem Recht erforderlich, eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten und der möglichen Folgen enthalten. Haiilo ergreift angemessene und notwendige Maßnahmen, um die Auswirkungen der Verletzung des Schutzes personenbezogener Daten abzumildern.

11. Einhaltung der Vorschriften

Haiilo führt Überprüfungen durch Dritte durch, um die Wirksamkeit sowohl der technischen als auch der administrativen Kontrollen innerhalb des ISMS zu bewerten, und vergleicht sie mit branchenüblichen Sicherheitsrahmen.

Die Maßnahmen umfassen:

a) Haiilo unterzieht sich regelmäßig internen und externen Sicherheitsaudits
b) Haiilo unterhält eine dokumentierte Richtlinie zur Überwachung der Sicherheit von Lieferanten. Die Richtlinie umfasst Kriterien für die Bewertung und Zulassung von Lieferanten sowie Maßnahmen zur Überwachung und Bewertung der Leistung der Lieferanten.
c) Haiilo führt regelmäßig Schwachstellenscans von Anwendungen und jährliche externe Penetrationstests für die verschiedenen Produkte von Haiilo durch, die von seriösen Drittanbietern durchgeführt werden. Weitere Einzelheiten können auf Anfrage mitgeteilt werden.

Annex 3

Angaben zu Unterauftragsverarbeitern

Die folgenden Unterauftragsverarbeiter dürfen im Rahmen dieser Vereinbarungen eingesetzt werden:

Unterauftragsverarbeiter 1	**Google Cloud EMEA Limited**, 70 Sir John Rogerson's Quay, Dublin 2, Irland
Datenschutzkontakt	https://support.google.com/policies/answer/9581826
Leistungen	Hosting Provider
Speicherort	EU
Rechtsgrundlage	Auftragsverarbeitungsvertrag ("DPA"), EU-US Data Privacy Framework zertifiziert, EU Standardvertragsklauseln ("SCC")

Unterauftragsverarbeiter 2	**T-Systems International GmbH**, Hahnstraße 43d, 60528 Frankfurt
Datenschutzkontakt	datenschutz@telekom.de
Leistungen	Sovereign Cloud externes Key Management
Speicherort	Deutschland
Rechtsgrundlage	DPA

Unterauftragsverarbeiter 3	**Telekom Deutschland GmbH**, Landgrabenweg 151, 53227 Bonn
Datenschutzkontakt	datenschutz@telekom.de
Leistungen	E-Mail Versand (z.B. Benachrichtigungen oder Passwort zurücksetzen)
Speicherort	EU
Rechtsgrundlage	DPA

Unterauftragsverarbeiter 4	**Zendesk Inc.**, 109 Market Street, San Francisco CA 94103, USA
Datenschutzkontakt	privacy@zendesk.com
Leistungen	SaaS Servicedesk Ticket System
Speicherort	Europäischer Wirtschaftsraum
Rechtsgrundlage	DPA, EU-US Data Privacy Framework zertifiziert, SCC

Unterauftragsverarbeiter 5	**Andere Haiilo Gesellschaften**
Datenschutzkontakt	dpo@haiilo.com
Leistungen	Kundensupport

Leistungen	Deutschland, UK, USA, Finnland (abhängig von der jeweiligen Gesellschaft)
Rechtsgrundlage	DPA, SCC

(Unterauftragsverarbeiter 6)	**Gainsight Inc.**, 350 Bay Street, Suite 100, San Francisco, CA 94133, USA
Datenschutzkontakt	privacy@gainsight.com
Leistungen	Plattform mit Lehrinhalten zur Nutzung der Software (Teil der Haiilo Academy; **Nutzung optional**)
Speicherort	USA
Rechtsgrundlage	DPA, EU-US Data Privacy Framework zertifiziert, SCC

Zusätzlich für Kunden des Produkts **Haiilo Align – Employee Communications:**

Unterauftragsverarbeiter 6	**ImageKit Inc.**, Christiana Corporate Business Center, 200 Continental Drive, Suite 401, Newark, DE 19713, USA
Datenschutzkontakt	support@imagekit.io
Leistungen	Content Delivery Network (optimierte Medienbereitstellung)
Speicherort	Deutschland
Rechtsgrundlage	DPA, EU-US Data Privacy Framework zertifiziert, SCC

Unterauftragsverarbeiter 7	**Twilio Inc.**, 375 Beale Street Suite 300 San Francisco, CA 94105, USA
Datenschutzkontakt	privacy@twilio.com
Leistungen	E-Mail Versand (Newsletter)
Speicherort	USA
Rechtsgrundlage	DPA, EU-US Data Privacy Framework zertifiziert, SCC