VEREINBARUNG ZUR AUFTRAGS-VERARBEITUNG (AV-VEREINBARUNG)

zwischen

Kunde / Firma
Verantwortliche Person
Postanschrift

- im Folgenden: Auftraggeber

sowie

Idiligo B.V.
Kabelweg 57
NL-1014 Amsterdam

- im Folgenden: Auftragsverarbeiter

wird der folgende Vertrag geschlossen:

§ 1 Präambel

Die Vertragsparteien planen bzw. unterhalten bereits eine Geschäftsbeziehung. Die vorliegende Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem zugrunde liegenden Vertrag (im Folgenden: „Hauptvertrag“) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Die in dem vorgenannten Vertrag beschriebene Tätigkeit stellt eine Auftragsdatenverarbeitung dar. Daher ist es erforderlich, dass die Vertragsparteien eine Vereinbarung zur Auftragsdatenverarbeitung gem. Art. 28 EU-Datenschutzgrundverordnung (DSGVO) schließen.
Diese Vereinbarung findet auf alle Tätigkeiten, welche mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragsverarbeiters oder durch diesen Beauftragten personenbezogene Daten des Auftraggebers verarbeiten.

§ 2 Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Ziff. 7 DSGVO).

(2) Der Auftragsverarbeiter selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DSGVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DSGVO notwendigen Angaben zur Verfügung.

(3) Soweit der Auftragsverarbeiter unter Verstoß gegen diese Vereinbarung und gegen die DSGVO die Zwecke und Mittel der Verarbeitung selbst bestimmt, gilt der Auftragsverarbeiter in Bezug auf diese Verarbeitung als Verantwortlicher i.S.d. Art. 4 Ziff. 7 DSGVO.

§ 3 Definitionen

(1) „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

(2) „personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;

(3) „Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

(4) „Weisung“ ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragsverarbeiters mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers.

(5) „Unterauftragnehmer“ ist jeder weitere Auftragsverarbeiter des Auftragsverarbeiters i.S.d. Art. 28 Abs. 4 DSGVO

(6) „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

(7) „Drittland“ ist ein Land, das sich außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums befindet.

§ 4 Gegenstand und Dauer des Auftrags/der Verarbeitung

(1) Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag, auf welchen hier verwiesen wird.

(2) Soweit sich der Gegenstand nicht oder nicht vollständig aus dem Hauptvertrag ergibt, ist Gegenstand der Verarbeitung: Idiligo B.V. gewährt dem Auftraggeber eine nicht übertragbare, nicht exklusive Lizenz für den Gebrauch der Idiligo Applikation, gemäß den Bestimmungen der „Allgemeinen Geschäftsbedingungen, 3. Lizenz und Gebrauch“ von Idiligo B.V., im Detail

   a) Idiligo stellt den Zugang zur Idiligo Applikation zur Verfügung (Benutzer log-in über die Idiligo B.V. website)
   b) Die Idiligo Applikation ermöglicht dem Auftraggeber eigene Nutzer für seinen Idiligo Account anzulegen
   c) Der Auftraggeber kann eigenständig Skripte entwickeln und einsetzen. Mit diesen Skripten kann er z.B. auch auftraggeberspezifische Informationen dokumentieren.
   d) Auftraggeber erhält Zugang zu seinen dokumentierten Informationen.

(3) Die Dauer des Auftrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht etwas anderes ergibt.

(4) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

§ 5 Umfang, Art und Zweck der Verarbeitung sowie Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Soweit sich Umfang, Art und Zweck der Verarbeitung nicht bereits aus dem Hauptvertrag ergeben, gelten die folgenden Bestimmungen ergänzend.

(2) Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung

Art der Daten	**Kategorien betroffener Personen des Auftraggebers**
Personenstammdaten	Kunden
Kontaktdaten (E-Mail, Telefon)	Mitarbeiter
Kundendaten	Interessenten
Kommunikationsdaten (Audio-und Videostreaming, Screensharing)	Bewerber
Inhaltsdaten (Geteilte Dateien in Skripten, Textchat, Whiteboard-Inhalte)	Lieferanten
Aktivitätsprotokolle (Log-Files)	Abonnenten
Signaturdaten (Charaktereigenschaften der digitalen Signatur)	Auftragnehmer
Vertragsdaten (zugrundeliegende rechtliche Dokumente bei digitaler Signatur)	Handelsvertreter / Partner
Kalenderdaten (Datum, Dauer)	Selbstsständig tätige Mitarbeiter
	Gesprächspartner des Auftraggebers
Support-Ticket-Daten (Nachrichten und Chatverläufe zwischen Nutzern und dem Auftragnehmer im Rahmen von Support-Anfragen)	
Metadaten (Nutzungsstatistiken) • Aktivitätsprotokolle (Log-Files) • IP-Adresse • Cookies • API Traffic • Control/Signalisierung Traffic • Media Server Log-Files • Plattform Access Log-Files	

§ 6 Weisungsbefugnis

(1) Die Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers, es sei denn, es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3a DSGVO vor.

Soweit es der Auftraggeber für erforderlich hält, können weisungsberechtigte Personen benannt werden. Diese wird der Auftraggeber dem Auftragsverarbeiter schriftlich oder in Textform mitteilen. Für den Fall, dass sich diese weisungsberechtigten Personen bei dem Auftraggeber ändern, wird dies dem Auftragsverarbeiter unter Benennung der jeweils neuen Person/-en schriftlich oder in Textform mitgeteilt.

(2) Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragsverarbeiter bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.

(3) Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(4) Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragsverarbeiter darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(5) Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragsverarbeiter tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten.

(6) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer vom Auftragsverarbeiter als wesentlich angesehenen Änderung des Auftrags steht dem Auftragsverarbeiter ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragsverarbeiters auf der Änderung, so ist diese Änderung als wichtiger Grund anzusehen und erlaubt eine fristlose Kündigung des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragsverarbeiter ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragsverarbeiters auf der Änderung, so ist diese Änderung als wichtiger Grund anzusehen und erlaubt eine fristlose Kündigung des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages.

§ 7 Leistungsort / Übermittlung in Drittland

Der Auftragsverarbeiter wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen. Etwaige Unterauftragnehmer werden die sie betreffenden Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen. Erfolgt eine Leistungserbringung durch den Auftragsverarbeiter oder einen Unterauftragnehmer in einem Drittland, garantiert der Auftragsverarbeiter die Einhaltung der diesbezüglichen Vorgaben der DSGVO und weist dies auf Verlangen des Auftraggebers nach.

(1) Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten ins Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragsverarbeiter für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§ 8 Wahrung des Datengeheimnisses/Vertraulichkeit und Geschäftsgeheimnisse

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(2) Der Auftragsverarbeiter ist zudem verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

(3) Weiterhin sind alle Personen des Auftragsverarbeiters bzgl. der Pflichten zur Wahrung von Geschäftsgeheimnissen des Auftraggebers zu verpflichten und müssen auf §4 GeschGehG hingewiesen werden.

§ 9 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten des Auftraggebers treffen, die den Anforderungen der DSGVO (Art. 28 Abs. 3 lit. c, 32 DSGVO) genügen.

(2) Der Auftragsverarbeiter hat solche technischen und organisatorischen Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

(3) Der Auftragsverarbeiter gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(4) Für die Einhaltung der vereinbarten Schutzmaßnahmen gilt nachfolgendes als vereinbart

- Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit wird auf die genehmigten Verhaltensregeln nach Art. 40 DSGVO verwiesen, denen sich der Auftragsverarbeiter am 25.09.2020 unterworfen hat und deren Einhaltung am 6.10.2020 geprüft und bestätigt wurde.

(5) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(6) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung und Freigabe zu übergeben.

(7) Eine Darstellung der vereinbarten technischen und organisatorischen Maßnahmen erfolgt in Anlage 1 zu dieser Vereinbarung.

§ 10 Unterauftragsverhältnisse, weitere Auftragsverarbeiter (Unterauftragnehmer)

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Leistung aus dem Hauptvertrag beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.
Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber ermächtigt den Auftragsverarbeiter weitere Auftragsverarbeiter (Unterauftragsnehmer) gemäß den Absätzen in § 10 dieser Vereinbarung in Anspruch zu nehmen. Diese Ermächtigung stellt eine allgemeine schriftliche Genehmigung i.S.d. Art. 28 Abs. 2 DSGVO dar.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform), sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(6) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Anlage 3 aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragsverarbeiter tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.

(7) Der Auftraggeber darf einen Widerspruch gegen die Einschaltung eines Unterauftragnehmers nur aus wichtigem Grund erheben.

§ 11 Berichtigung, Löschung und Sperrung von Daten

(1) Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragsverarbeiter die vertragsgegenständlichen Daten nur nach den Weisungen des Auftraggebers.

(2) Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks Berichtigung, Löschung oder Sperrung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

§ 12 Unterstützung durch den Auftragsverarbeiter bei Pflichten nach Art. 12 – 23, 33-36 DSGVO

(1) Der Auftragsverarbeiter unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche der betroffenen Personen gem. Art. 12- 23 DSGVO (Informationspflichten, Betroffenenrechte, Recht auf vergessenwerden, Recht auf Datenportabilität etc.)

(2) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen nach Art. 33, 34 DSGVO.

(3) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Datenschutzfolgenabschätzung nach Art. 35 DSGVO mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation nach Art. 36 DSGVO der zuständigen Aufsichtsbehörde unterstützt der Auftragsverarbeiter den Auftraggeber auch hierbei.

§ 13 Mitteilungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterrichtet den Auftraggeber unverzüglich

a) bei Verstößen des Auftragsverarbeiters oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab;

b) wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt;

c) über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörden, soweit sie sich auf den Gegenstand der vorliegenden Vereinbarung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.

(2) Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

§ 14 Rückgabe und Löschung von Daten und Datenträgern bei Vertragsende

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder diesem zurückgeben, sofern nicht nach dem Unionsrecht oder dem für den Auftragsverarbeiter geltendem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen

(2) Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragsverarbeiter angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen. Die Maßnahmen und die anzuwendenden Löschverfahren werden bei Bedarf ergänzend zu den Leistungsbeschreibungen konkretisierend vereinbart.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(4) Sollte dem Auftraggeber eine Rücknahme der Daten nicht möglich sein, wird er den Auftragsverarbeiter rechtzeitig schriftlich informieren. Der Auftragsverarbeiter ist dann berechtigt, personenbezogene Daten im Auftrag des Auftraggebers zu löschen.

(5) Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung bzgl. einer Löschung nicht erforderlich, diese müssen gelöscht werden.

§ 15 Kontrollrechte des Auftraggebers und Duldungs- und Mitwirkungsrechte

(1) Der Auftragsverarbeiter weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Der Auftragsverarbeiter kann den Nachweis insbesondere durch Vorlage der folgenden Informationen erbringen:

a) Durchführung eines Selbstaudits
b) Testat eines Sachverständigen
c) unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung
d) Zertifikat zu Datenschutz und/oder Informationssicherheit (z. B. ISO 27001)
e) genehmigte Verhaltensregeln nach Art. 40 DSGVO
f) Zertifikate nach Art. 42 DSGVO

(3) Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen, hat der Auftragsverarbeiter gegen diesen ein Einspruchsrecht.

(4) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragsverarbeiter unterstützt. Insbesondere verpflichtet sich der Auftragsverarbeiter, dem Auftraggeber auf schriftliche Anforderung, welche auch in einem elektronischen Format erfolgen kann, innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

(5) Der Auftraggeber wird den Auftragsverarbeiter unverzüglich und vollständig informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 16 Bestellung eines Datenschutzbeauftragten

(1) Der Auftragsverarbeiter wird einen Datenschutzbeauftragten benennen, soweit die Voraussetzungen des Art. 37 DSGVO vorliegen.

(2) Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich oder in Textform mitzuteilen. Der Auftragsverarbeiter gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DSGVO erfüllt werden.

(3) Sofern kein Datenschutzbeauftragter beim Auftragsverarbeiter benannt ist, benennt der Auftragsverarbeiter dem Auftraggeber einen Ansprechpartner.
(4) Sofern sich der Sitz des Auftragsverarbeiters außerhalb der Union befindet, benennt er einen Vertreter in der Union nach Art. 27 Abs. 1, 3 Abs. 2 DSGVO.
(5) Die nach Abs. 1-4 zu benennenden Personen werden in der Anlage 2 zu dieser Vereinbarung benannt.

§ 17 Haftung

(1) Auftraggeber und Auftragsverarbeiter haften für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird, gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.
(2) Der Auftragsverarbeiter haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der
    a) er den aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
    b) er unter Nichtbeachtung der rechtmäßig erteilten Weisungen des Auftraggebers handelte oder
    c) er gegen die rechtmäßig erteilten Weisungen des Auftraggebers gehandelt hat.
(3) Soweit der Auftraggeber zum Schadensersatz gegenüber der betroffenen Person verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragsverarbeiter vorbehalten.
(4) Im Innenverhältnis zwischen Auftraggeber und Auftragsverarbeiter haftet der Auftragsverarbeiter für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er
    a) seinen ihm speziell durch die DSGVO auferlegten Pflichten nicht nachgekommen ist oder
    b) unter Nichtbeachtung der rechtmäßig erteilten Weisungen des Auftraggebers oder gegen diese Weisungen gehandelt hat.
(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 18 Schriftformklausel

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

§ 19 Salvatorische Klausel

(1) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages vor.

(2) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge von Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

(3) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedacht Werdens vereinbart worden wären.

§ 20 Anwendbarkeit

(1) Diese Vereinbarung findet mit Unterzeichnung durch die Vertragsparteien Anwendung.

(2) Ab dem 25. Mai 2018 gilt die VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

§ 21 Rechtswahl und Gerichtsstand

(1) Es gilt niederländisches Recht.

(2) Gerichtsstand ist der Sitz des Auftragsverarbeiters.

[Ort], den [TT.MM.JJJJ]	Amsterdam, den [TT.MM.JJJJ
[vollständiger Name AG]	Idiligo B.V.
_____	_____
[Auftraggeber]	[Auftragsverarbeiter / -nehmer]

Anlagen:

Anlage 1: Technische und organisatorische Maßnahmen

Anlage 2: Benennung des Datenschutzbeauftragten, Ansprechpartners und/oder Vertreters innerhalb der Union

Anlage 3: Eingesetzte Unterauftragnehmer

Anlage 4: Vereinbarte Leistungsstandorte gem. § 7

Anlage 1

Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. a, b DS-GVO)

Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.
Technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- ☒ Festlegung befugter Personen inklusive Umfang der jeweiligen Befugnisse
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☒ Ausgabe von Zutrittsberechtigungsausweisen
- ☒ Existenz von Regelungen für Unternehmensexterne (Begleitung des Besuchers durch Mitarbeiter, Trennung von Bearbeitungs- und Publikumszonen)
- ☒ Umsetzung einer Schlüsselregelung
- ☒ Protokollierung der ein- und ausgehenden Personen
- ☐ Physische Maßnahmen vorhanden und regelmäßig überprüft:
- ☒ Gesicherter Eingang (z. B. abschließbare Türen, Sicherheitsschlösser)
- ☒ Türsicherung (elektrische Türöffner)
- ☒ Einbruchhemmende Fenster
- ☐ Gerätesicherung gegen Diebstahl, Manipulation oder Beschädigung
- ☐ Überwachungseinrichtung (z. B. Alarmanlage, Videoüberwachung)
- ☐ Vereinzelungsanlage (z. B. Drehkreuz, Schleuse)
- ☐ Wachpersonal, Pförtner
- ☐ Unterteilung in verschiedene Sicherheitszonen

Sonstiges:

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme und die unbefugte Systemnutzung sind zu verhindern.

Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- ☒ Konzeption und Implementierung eines Berechtigungskonzepts
- ☒ Berechtigungskonzept für Endgeräte (Rechner)
- ☒ Berechtigungskonzept für Software/Systeme
- ☒ Identifikation und Berechtigungsprüfung eines Benutzers
- ☒ Implementierung eines Systems zur Verwaltung von Benutzeridentitäten
- ☐ Monitoring der Zugangsversuche mit Reaktion auf Sicherheitsvorfälle
- ☒ Festlegung und Kontrolle der Zugangsbefugnisse
- ☐ Authentisierungsverfahren dem Schutzbedarf der Informationen entsprechend (Klassifizierung)
- ☒ Verschlüsselung
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☒ Angemessener Passwortschutz (Verhaltensregeln, verschlüsselte Archive)
- ☒ Spezielle Sicherheitssoftware (Anti-Malware, Viren-Scanner, Soft- und Hardware-Firewall)
- ☐ Zwei-Faktor-Authentifizierung
- ☐ Existenz von Regelungen für Unternehmensexterne
- ☐ Zugangsfunktion über Token

Sonstiges:

Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung anhand:

- ☒ Berechtigungs- und Rollenkonzept für Applikationen
- ☒ Umsetzung von Regelungen zur Zugriffs- und Benutzerberechtigung
- ☒ Überprüfung der Berechtigungen
- ☒ Funktionsbegrenzung (funktional/zeitlich)
- ☒ Zugriffsbeschränkungen (gemäß „Need-to-Know“ und „Least Privilege“)
- ☒ Verschlüsselte Speicherung der Daten
- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☒ Protokollierung von unberechtigten Zugriffsversuchen
- ☐ Regelmäßige Auswertung
- ☒ Anlassbezogene Auswertung
- ☒ Umsetzung von Regelungen zur Löschung von Daten
- ☐ Umsetzung von Regelungen zur Entsorgung von Speichermedien (Einsatz von Aktenvernichtern bzw. Dienstleistern gem. DIN 66933)
- ☐ Umsetzung von Regelungen zum Umgang mit elektronischen Speichermedien
- ☒ Integritätskontrolle

Sonstiges:

Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- ☐ Mandantenfähigkeit:
- ☒ Physische Trennung
- ☒ Logische Mandantentrennung (softwareseitig)
- ☒ Trennung von Produktiv- und Testsystemen
- ☐ Sandboxing
- ☒ Festlegung von Datenbankrechten
- ☐ Dokumentation der Funktionstrennung
- ☒ Vorhandensein von Richtlinien und Arbeitsanweisungen
- ☐ Vorhandensein von Verfahrensdokumentationen
- ☒ Regelmäßige Prüfung der bestimmungsgemäßen Nutzung der Informationen und IT-Systeme

Sonstiges:

Pseudonymisierung und Verschlüsselung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen:

- [x] Trusted Third Party
- [ ] Blinde Signatur
- [ ] Softwarebasierte Verschlüsselung bei Datenspeicherung
- [ ] Hardwarebasierte Verschlüsselung bei Datenspeicherung

Sonstiges:

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Aspekte der Weitergabe und Übertragung personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Für elektronische Datenträger:

- ☒ Verschlüsselung der Datenübermittlung (z. B. VPN, S/MIME)
- ☐ Elektronische Signatur
- ☒ Durchführung von Protokollierungen der Datenweitergabe oder Übermittlung
- ☒ Anlassbezogene Durchführung von Plausibilitäts-, Vollständigkeits- und Richtigkeitsprüfungen
- ☐ Maßnahmen zur Verhinderung von unkontrollierten Informationsabflüssen (z. B. Deaktivierung der USB-Schnittstellen, regelmäßige Kontrolle der zulässigen Empfänger, technische Beschränkung auf zulässige Empfänger)
- ☐ Dokumentation der Formen der Weitergabe von Daten (z. B. Ausdruck, Datenträger, automatisierte Übermittlung)
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Auflistung der Empfänger der Daten
- ☐ Dokumentationen der Schnittstellen und der Abruf- und Übermittlungsprogramme

Für Ausdrucke und Datenträger:

- ☒ Durchführung von regelmäßigen Bestandskontrollen
- ☐ Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- ☐ Anlassbezogene Sicherungen des Transports (z. B. Behälter, Verschlüsselung von Speichermedien, Übergabeprotokolle)

Sonstiges:

Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- ☐ Protokollierung der Eingaben und Überprüfung der Protokolle
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
- ☒ Organisatorisch festgelegte Zuständigkeiten für die Eingabe

Sonstiges:

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DS-GVO)

Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physisch/logisch):

- ☐ Regelmäßige Kontrolle des Systemzustands (Monitoring)
- ☒ Kurzfristige Wiederherstellbarkeit des normalen Systemzustands
- ☐ Backup- und Wiederanlaufkonzept (regelmäßige Datensicherungen):
- ☐ offline ☒ online ☒ onsite ☐ offsite ☐
- ☒ Datenarchivierungskonzept
- ☒ Vorhandensein eines Notfallkonzepts (Business Continuity, Disaster Recovery)
- ☐ Regelmäßige Tests des Notfallkonzepts
- ☒ Vorhandensein von redundanten IT-Systemen (z. B. Server, Speicher)
- ☐ Replizierbarkeit virtueller Maschinen
- ☒ Funktionsfähige physische Schutzeinrichtungen (Brandschutz, Energie: USV, Klima)
- ☐ Meldewege und Notfallpläne

Sonstiges:

Belastbarkeitskontrolle

Die Verarbeitung der Daten soll tolerant gegenüber Störungen und Fehlern sein.

- ☒ Virenschutz/Anti-Malware/Anti-Ransomware
- ☒ großzügig vorhandene Netzwerkkapazität
- ☒ gehärtete Hardware gegen insbesondere DoS- und DDoS-Angriffe
- ☐ IDS/IPS
- ☒ geeignete Systemarchitektur/DMZ
- ☒ Firewall

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- ☒ Schriftlich fixierte Regelungen der Verantwortlichkeiten für Datenschutz
- ☒ Schriftlich fixierte Regelungen der Verantwortlichkeiten für Informationssicherheit
- ☐ Existenz eines angemessenen Informationssicherheitsmanagements
- ☐ Existenz eines angemessenen Incident Response Managements
- ☒ Durchführung einer Informationsklassifizierung
- ☒ Regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte
- ☒ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- ☐ Auftragskontrolle, um weisungsgemäße Auftragsverarbeitung zu gewährleisten:
  - ☐ Strikte Einhaltung der festgeschriebenen Vereinbarungen und diesbezügliche Überprüfungen
  - ☒ Konzept dahingehend, wie die regelmäßige Kontrolle des Auftragsprozesses erfolgt (z. B. Vorlage von Self-Assessments, Vorlage der Verträge mit Unterauftragnehmern, Durchführung von Kontrollen bei Subunternehmern durch den Auftragnehmer)
  - ☐ Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z. B. anhand: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Sonstiges:

Anlage 2

Benennung des Datenschutzbeauftragten, Ansprechpartners oder Vertreters innerhalb der Union gem. § 16 AV-Vereinbarung

Der Auftragsverarbeiter benennt:

Als Datenschutzbeauftragten Herrn Dr. Timo Hoffmann

Anschrift: Eckweg 1, 78048 Villingen-Schwenningen

E-Mail: timo.hoffmann@hub24.de

Als Ansprechpartner Herrn Frank Korthouwer

Anschrift: Kabelweg 57, 1014 BA Amsterdam

Tel.: +31 23 3000000

E-Mail: frank.korthouwer@idiligo.com

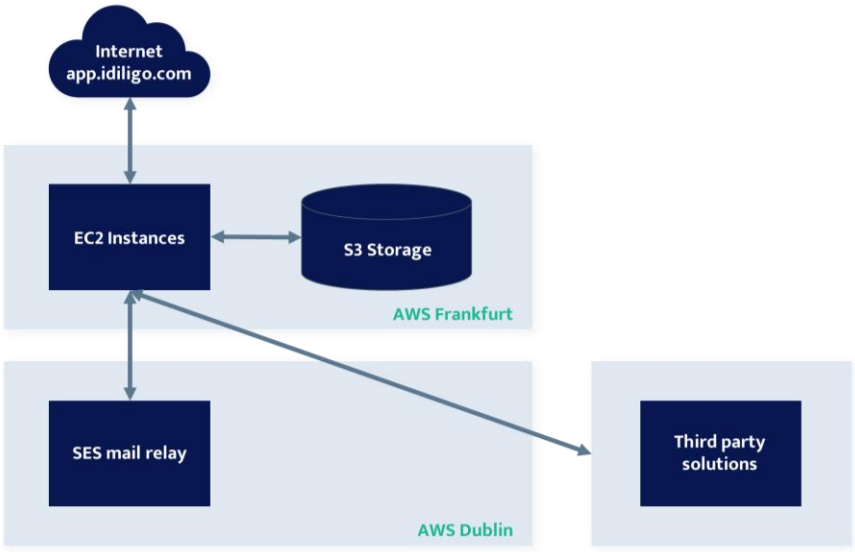
Anlage 3

Unterauftragsverhältnis beim Auftragsverarbeiter zum Zeitpunkt der Auftragsvergabe

Name Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung
Amazon (AWS)	Speicherung von Daten im Amazon S3-Speicher. Sowohl EC2 als auch S3	Frankfurt, Deutschland
Amazon (AWS)	SES Mail-Relay-Funktion	Dublin, Irland
Digital Intelligence	Entwicklung der Idiligo Applikation	Amsterdam, Niederlande
The Rocket Science Group LLC d/b/a Mailchimp	Kundeninformation per E-Mail	Drittländer, EU
Exact	Rechnungsversand	EU
Intelligent Solution Services AG	Digitale Unterschrift	Stuttgart, Deutschland

Sicherheitsmanagement & Architektur

- Die Elastic Compute Cloud (EC2) von Amazon bietet eine Funktion namens Sicherheitsgruppen, die einer eingehenden Netzwerk-Firewall ähnelt, in der Idiligo die Protokolle, Ports und Quell-IP-Bereiche angibt, die die EC2-Instanzen erreichen dürfen.
  Speicher & Backups
- Dokumente, die zur Verwendung während interaktiver Idiligo-Besprechungen hochgeladen oder generiert wurden, werden in S3 gespeichert. Die Daten werden mit AWS Key Management Service (KMS) verschlüsselt gespeichert.
  Idiligo implementiert eine tägliche Sicherung kundenspezifischer Informationen mit einer maximalen Historie von 8 Tagen in einer separaten Amazon S3-Umgebung.



Anlage 4

Vereinbarte Leistungsstandorte gem. § 7 der Vereinbarung

Name und Anschrift des Auftragsverarbeiters	**Name und Anschrift des Unterauftragnehmers**	**Ort der Leistungserbringung**
Idiligo B.V. Kabelweg 57, 1014 BA Amsterdam, Niederlande	Amazon (AWS) Frankfurt	Deutschland