Vereinbarung über
Technischen- und Kundensupport im Rahmen der Dienstleistung der Riddle Technologies AG

zwischen

- nachstehend Auftraggeber genannt -
und
Riddle Technologies AG, Lenaustr. 1, 66125 Saarbrücken, Deutschland
- nachstehend Auftragnehmer genannt -

§ 1 Gegenstand des Auftrages

(1) Gegenstand des Auftrages sind Technischer- und Kundensupport im Rahmen *Nutzung der Leistung des Auftragnehmers, näher bezeichnet im Leistungsvertrag zwischen Auftraggeber und Auftragnehmer vom*
Hierbei kann der Auftragnehmer unter Umständen Kenntnis von den personenbezogenen Daten der Kunden des Auftraggebers erlangen.

(2) Der Auftragnehmer verarbeitet daher (im weitesten Sinne) personenbezogene Daten des Auftraggebers. Bei dem Vertragsgegenstand handelt es sich deshalb um eine Auftragsverarbeitung. Die Parteien sind sich darin einig, dass auf diesen Vertrag die Vorschriften der EU-Datenschutzgrundverordnung (DSGVO), insbesondere die Vorschriften über die Datenverarbeitung im Auftrag, anzuwenden sind. Der Auftragnehmer erklärt, dass er in der Lage ist, die aufgetragenen Leistungen nach Maßgabe des Art. 28 DSGVO ordnungsgemäß durchzuführen.

(3) Der Vertrag regelt die datenschutzrechtlichen Maßnahmen im Sinne von Art. 28 DSGVO und die Rechte und Pflichten des Auftraggebers und des Auftragnehmers zur Erfüllung der datenschutzrechtlichen Anforderungen.

§ 2 Dauer, Laufzeit des Auftrages

(1) Die Laufzeit dieses Vertrages ist an die Laufzeit des Leistungsvertrages geknüpft.
Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 3 Kategorien von betroffenen Personen

(1) Die Datenverarbeitung betrifft folgende Kategorien von natürlichen Personen:
   a. Den Auftraggeber selbst sowie dessen Mitarbeiter, die die Dienste des Auftragnehmers zur Erstellung von interaktiven Inhalten nutzen.
   b. Kunden des Auftraggebers, welche mit den erstellten Inhalten interagieren.

§ 4 Arten der personenbezogenen Daten

(1) Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien:
   a. Name, Anschrift, IP Adresse des registrierten Nutzers, der unter dem Benutzerkonto des Auftraggebers die Dienste von Riddle.com in Anspruch nimmt, um interaktive Inhalte zu erstellen.
   b. Daten von Kunden des Auftraggebers, die in eingebundene Formulare oder Freitextfelder in den erstellten interaktiven Inhalten eingegeben werden.

§ 5 Ort der Verarbeitung

(1) Die Datenverarbeitung findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland oder innerhalb der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes statt. Eine Verarbeitung in anderen Staaten ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist. Der Auftragnehmer führt den Nachweis für das Bestehen der Garantien und eines angemessenen Schutzniveaus. Der Nachweis kann durch Vorlage eines entsprechenden Zertifikates einer akkreditierten Zertifizierungsstelle nach Art. 43 DSGVO geführt werden. Der Auftragnehmer verpflichtet sich, die Einhaltung der Garantien und eines angemessenen Schutzniveaus sicherzustellen. Der Auftraggeber behält sich vor, das Vorliegen der Garantien und die Einhaltung eines angemessenen Schutzniveaus im Rahmen seiner Audit- und Kontrollrechte jederzeit zu überprüfen.

§ 6 Kontroll- und Auditrechte des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung der personenbezogenen Daten sowie für die Ausführung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Bei einer Datenverarbeitung im Auftrag arbeitet der Auftraggeber gem. Art. 28 Abs. 1 Satz 1 DSGVO nur mit Auftragsverarbeitern zusammen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen zur Erfüllung der Anforderungen der DSGVO eingerichtet sind.

(2) Der Auftraggeber ist danach verpflichtet und befugt, vor Beginn der Datenverarbeitung und nach seinem Ermessen auch wiederholt nach vorheriger Abstimmung während der üblichen Geschäftszeiten im erforderlichen Umfang die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen, zu kontrollieren.

Hierzu ist der Auftraggeber befugt, schriftliche Auskünfte und die Vorlage von Nachweisen über die eingerichteten Datenschutzmaßnahmen sowie über die Art und Weise ihrer technischen und organisatorischen Umsetzung zu verlangen, das Grundstück und die Betriebsstätten des Auftragnehmers zu betreten, nach seinem Ermessen Prüfungen und Besichtigungen vorzunehmen und im erforderlichen Umfang in verarbeitungsrelevante Unterlagen, Verarbeitungs- und Ablaufprotokolle, Systeme und gespeicherte Daten und in Regelungen, Richtlinien und Handbücher zur Regelung der beauftragten Datenverarbeitung einzusehen. Dazu gehören auch Nachweise über die Bestellung eines Datenschutzbeauftragten, die Verpflichtung der Mitarbeiter auf die Wahrung der Vertraulichkeit und technische und organisatorische Konzepte, z. B. Datenschutzhandbuch, einschlägige Verfahrensanweisungen und auch Verträge mit Unterauftragnehmern. Die gleichen Rechte besitzen auch Beauftragte des Auftraggebers, z. B. Gutachter oder Sachverständige, soweit sie besonders zur Verschwiegenheit verpflichtet sind oder strafbewehrten berufsständischen Schweigepflichten unterliegen.

(3) Die Rechte des Auftraggebers bestehen während der Laufzeit dieser Vereinbarung und darüber hinaus bis zum Eintritt der Verjährung von Ansprüchen aus diesem Vertrag, mindestens jedoch solange der Auftragnehmer personenbezogene Daten aus den beauftragten Verarbeitungen speichert.

(4) Die Prüfung erfolgt nach vorheriger Anmeldung. In besonderen Fällen, insbesondere wenn Verarbeitungsprobleme bestehen, meldepflichtige Vorfälle aufgetreten sind oder aufsichtsrechtliche Maßnahmen anstehen oder eingeleitet worden sind, kann die Prüfung auch ohne vorherige Anmeldung erfolgen.

§ 7 Weisungsbefugnisse des Auftraggebers

(1) Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der getroffenen Auftragsbeschreibung ein Weisungsrecht in Form von Einzelanweisungen über Art, Umfang und Verfahren der Datenverarbeitung sowie über Änderungen der

Verarbeitung vor. Die Weisungen betreffen insbesondere aber nicht ausschließlich die datenschutzkonforme Auftragsabwicklung und sonstige Handlungen zur Sicherstellung einer gesetzmäßigen Auftragsabwicklung. Die Weisungen werden schriftlich, in Schriftform oder in einem anderen geeigneten elektronischen Format erteilt. Mündliche Weisungen werden unverzüglich in Schriftform, schriftlich oder in einem elektronischen Format bestätigt. Die Weisungen werden über die Dauer des Auftragsverhältnisses, mindestens jedoch für die Dauer ihrer Gültigkeit aufbewahrt.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzvorschriften verstößt. Der Auftragnehmer kann die Ausführung der Anweisung bis zu einer Bestätigung durch den Auftraggeber aussetzen. Der Auftraggeber haftet für rechtswidrige Weisungen und stellt den Auftragnehmer insoweit von Schadensersatzansprüchen und sonstigen Forderungen frei.

Weisungsberechtigte Personen des Auftraggebers sind

Weisungsempfänger beim Auftragnehmer sind: Boris Pfeiffer, boris@riddle.com
Änderungen der weisungsberechtigten Person oder Weisungsempfänger sind unverzüglich mitzuteilen.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

§ 8 Pflichten des Auftragnehmers

(1) Verarbeitungspflichten
Der Auftragnehmer führt den Auftrag ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben.

Auszüge, Kopien oder Duplikate von Daten oder Datenträgern dürfen ohne Wissen des Auftraggebers nur hergestellt und verwendet werden, soweit dies für die Ausführung des Auftrages oder zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich ist oder eine gesetzliche oder sonstige Aufbewahrungspflicht besteht. Eventuell hergestellte Auszüge, Kopien oder Duplikate sind nach Abschluss der Verarbeitung oder Nutzung vom Auftragnehmer unverzüglich sicher zu löschen bzw. datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nicht oder nur nach Weisung des Auftraggebers erteilen. Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen erteilen.

Der Auftragnehmer verpflichtet sich, nur solche Software, Daten oder Datenträger einzusetzen, die zuverlässig auf Freiheit von schädlicher Software geprüft sind, um ein Einschleusen von Viren etc. zu vermeiden.

(2) Duldungspflichten bei Kontrollen
Der Auftragnehmer verpflichtet sich, in Prüfungen durch den Auftraggeber die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nachzuweisen, Auskünfte zu erteilen und die entsprechenden Unterlagen vorzulegen bzw. Einsicht in die erforderlichen Unterlagen und Systeme zu gewähren und nach vorheriger Abstimmung entsprechende Prüfungen des Auftraggebers vor Ort zu dulden und zu unterstützen. Er verpflichtet sich, bei datenschutz- und datensicherheitsrelevanten Vorfällen alle erforderlichen Auskünfte zu erteilen und die Aufklärung derartiger Vorfälle nach Möglichkeit zu unterstützen.

Der Nachweis angemessener technischer und organisatorischer Maßnahmen kann auch durch Vorlage von Testaten oder Zertifikaten oder durch eine Zertifizierung bzw. ein Datenschutzaudit einer unabhängigen Einrichtung bzw. eines autorisierten Sachverständigen geführt werden. Unabhängig von diesen Nachweisen ist der Auftragnehmer verpflichtet, Kontrollen durch den Auftraggeber gem. § 6 dieser Vereinbarung zu dulden.

(3) Informationspflichten
Der Auftragnehmer ist verpflichtet, wesentliche Änderungen in den technischen und organisatorischen Verhältnissen, die die Sicherheit und Ordnungsmäßigkeit der Durchführung der Auftragsleistungen herabsetzen, unaufgefordert dem Auftraggeber zu melden.

Der Auftragnehmer unterrichtet den Auftraggeber über Kontrollen der Aufsichtsbehörde für den Datenschutz, insbesondere gem. Art. 58 DSGVO, und über eventuelle Maßnahmen und Auflagen zum Schutz der personenbezogenen Daten.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Er informiert den Auftraggeber unverzüglich über das Erlöschen oder den Widerruf von Zertifikaten oder von Maßnahmen gem. Art. 41 Abs. 4 DSGVO.

Der Auftragnehmer teilt dem Auftraggeber Name und Kontaktdaten und Änderungen in der Person des betrieblichen Datenschutzbeauftragten oder, wenn keine Bestellpflicht besteht, den Namen und die Kontaktdaten der sonstigen zuständigen Stelle mit.

(4) Mitwirkungs- und Unterstützungspflichten
Der Auftragnehmer verpflichtet sich, im Rahmen des Art. 28 Abs. 3 lit. e und f DSGVO, die für das Verzeichnis von Verarbeitungstätigkeiten sowie für die Risikoermittlung und eventuelle Datenschutzfolgenabschätzung erforderlichen Informationen unverzüglich zur Verfügung zu stellen und, soweit es seinen Verantwortungsbereich betrifft, im erforderlichen Umfang bei der Ermittlung der Risiken und einer eventuellen Datenschutzfolgenabschätzung mitzuwirken sowie den Auftraggeber bei der Erfüllung der Rechte der Betroffenen zu unterstützen.

(5) Organisationspflichten
Der Auftragnehmer verpflichtet sich zur Einrichtung von Maßnahmen und Dokumentationen, die eine Kontrolle und Nachvollziehbarkeit aller mit der Auftragsverarbeitung zusammenhängenden Tätigkeiten und Verarbeitungsprozesse im Sinne einer Auftragskontrolle und der Ordnungsmäßigkeit der Datenverarbeitung ermöglichen. Datenschutzvorfälle und sonstige sicherheitsrelevante Störungen der Verarbeitung sind einschließlich ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen zu dokumentieren und dem Auftraggeber zu melden. Die Dokumentation ist dem Auftraggeber unverzüglich zur Verfügung zu stellen.

Die Verarbeitung findet teilweise in Privatwohnungen oder von einem dritten Ort aus statt. Der Auftragnehmer verpflichtet sich, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Verarbeitung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung vom Ort des Auftragnehmers aus der Fall ist. Soll davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers.
Der Auftragnehmer sichert zu, dass gem. Art. 37 lit. b und c DSGVO i. V. m. § 38 Datenschutzanpassungs- und Umsetzungsgesetz ein Datenschutzbeauftragter bestellt ist und der Datenschutzbeauftragte die Einhaltung der datenschutzrechtlichen Vorschriften in geeigneter Weise überwacht.

§ 9 Wahrung der Vertraulichkeit und sonstiger Geheimnisse

(1) Personenbezogene und sonstige Daten oder Informationen, die dem Auftragnehmer im Rahmen der Erfüllung dieses Vertrags bekannt werden, darf der Auftragnehmer nur für Zwecke der beauftragten Leistung verwenden. Der Auftragnehmer verpflichtet sich, die Vertraulichkeit und Integrität der personenbezogenen Daten zu wahren und alle ihm im Zusammenhang mit der Übernahme und Abwicklung des Auftrages bekannt werdenden personenbezogenen Daten und sonstige unternehmensinterne Umstände, Daten und Informationen (Betriebsgeheimnisse) vertraulich zu behandeln sowie die im Rahmen dieses Vertrages tätig werdenden Mitarbeiter auch über die Beendigung des Beschäftigungsverhältnisses hinaus auf die Wahrung der Vertraulichkeit schriftlich zu verpflichten und über die

Datenschutzpflichten aus diesem Vertrag, die Weisungsgebundenheit der Verarbeitung der Daten und deren Zweckbindung zu belehren. Diese Geheimhaltungspflicht gilt auch über die Beendigung des Vertragsverhältnisses hinaus.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er für die Durchführung der Arbeiten nur eigenes Personal einsetzt und die mit der Auftragsdurchführung beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und einer regelmäßigen Schulung unterzieht.

(3) Der Auftragnehmer verpflichtet sich zur Beachtung aller sonstigen Geheimnisse, soweit diese für die Verarbeitung einschlägig sind, wie des Sozialgeheimnisses, des Fernmeldegeheimnisses und sonstiger Berufsgeheimnisse gem. § 203 StGB sowie zur Verpflichtung und Belehrung der Beschäftigten zur Sicherstellung der Wahrung dieser Geheimnisse.

(4) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über administrative Zugangsdaten und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen. Von den ihm eingeräumten Zugriffsrechten darf der Auftragnehmer nur in dem Umfang Gebrauch machen, der für die Durchführung der Datenverarbeitung erforderlich ist. Die Verpflichtung zur Wahrung der Vertraulichkeit und der sonstigen Geheimnisse gilt auch über die Beendigung dieses Vertrages hinaus.

§ 10 Unterauftragsverhältnisse

(1) Die Einschaltung von Unterauftragnehmern ist nur zulässig, wenn der Auftraggeber vor der Vergabe der Auftragsleistung schriftlich zugestimmt hat. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes, insbesondere bei einer Gesetzes- oder Vertragsverletzung, seine Zustimmung zur Unterbeauftragung widerrufen. Die Unterbeauftragung ist dann unverzüglich einzustellen. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so zu gestalten, dass sie den Datenschutzbestimmungen dieses Vertrages entsprechen. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten an den Unterauftragnehmer ist erst zulässig, wenn ein Vertrag nach diesen Auflagen abgeschlossen worden ist und der Unterauftragnehmer alle Anforderungen dieses Vertrages erfüllt hat.
    a. Die in Anlage 2 genannten Unterauftragnehmer werden vom Auftragnehmer lediglich im Rahmen des Technischen- und Kundensupports eingesetzt. Daten der Kunden des Auftraggebers werden von den unten genannten Unterauftragnehmern weder gespeichert noch verarbeitet. Die genannten Unterauftragnehmer unterstützen mit Ihrer jeweiligen Leistung die Kommunikation sowie die Rechnungslegung zwischen Auftragnehmer und Auftraggeber.
    b. Handelt es sich beim Auftraggeber um keine juristische Person, werden mit den in Anlage 2 genannten Unterauftragnehmern jeweils separat eine dieser Auftragsverarbeitungsvereinbarung entsprechende vertragliche Vereinbarung getroffen um die Vorgaben von Art. 28 IV S.1 DSGVO zu erfüllen

(2) Bei der Unterbeauftragung sind dem Unterauftragnehmer die gleichen vertraglichen Regelungen aufzuerlegen, wie sie für den Auftragnehmer gelten. Dem Auftraggeber sind gegenüber dem Unterauftragnehmer die gleichen Weisungs-, Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und dem Art. 28 DSGVO einzuräumen, wie sie gegenüber dem Auftragnehmer gelten. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

(3) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der

Sicherheit der Daten des Auftraggebers auch bei fremdvergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(4) Eine Beauftragung von Unterauftragnehmern außerhalb des Gebiets der Bundesrepublik Deutschland oder der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist. Im Übrigen gelten die Regelungen zu § 5 dieses Vertrages auch für die Beauftragung von Unterauftragnehmern.

§ 11 Mitteilungspflichten bei Störungen und Datenschutzverletzungen

(1) Bei einer Störung der Verarbeitung oder einer Datenschutzverletzung leitet der Auftragnehmer umgehend alle geeigneten und erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung eines eventuellen Schadens für die Betroffenen und für den Auftraggeber ein.

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich über Verstöße gegen Vorschriften zum Schutz der personenbezogenen Daten oder gegen die in dieser Vereinbarung getroffenen Festlegungen zu unterrichten. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder andere Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers, die Auswirkungen auf die betroffenen Personen oder den Auftraggeber nach sich ziehen oder Schaden verursachen können. Zu den Datenschutzverstößen gehören insbesondere der Verlust der Vertraulichkeit und der Verlust oder die Zerstörung oder Verfälschung von Daten des Auftraggebers oder sonstiger vertraulicher Informationen im Sinne dieses Vertrages.

(3) Die Meldung an den Auftraggeber umfasst alle Informationen, die für den Auftraggeber erforderlich sind, um den Vorfall und seine Meldepflicht an die Aufsichtsbehörde und die Informationspflicht der Betroffenen gem. Art. 33 und 34 DSGVO beurteilen und ggf. fristgerecht die Meldung an die Aufsichtsbehörde und ggf. die Information der Betroffenen vornehmen zu können. Die Meldung an den Auftraggeber umfasst insbesondere Angaben zur Art des Vorfalls und der Verletzung des Schutzes von personenbezogenen Daten, eine Beschreibung der wahrscheinlichen Risiken für die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen und eine Beschreibung der bereits eingeleiteten Maßnahmen zur Behebung bzw. Reduzierung eines möglichen Schadens oder sonstiger Risiken für die Betroffenen und den Auftraggeber.

(4) Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Informationspflicht gem. Art. 33 und 34 DSGVO und unternimmt alle in seinen Verantwortungsbereich fallenden Maßnahmen zur Minderung nachteiliger Folgen für die Betroffenen sowie zur Aufklärung des Vorfalls und dessen Folgen. Dies gilt auch nach Beendigung des Vertragsverhältnisses.

§ 12 Rechte der Betroffenen

(1) Für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und zuständig. Der Auftragnehmer darf Rechte der Betroffenen nur nach Weisung des Auftraggebers umsetzen. Der Auftragnehmer unterstützt jedoch den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen.

(2) Anfragen von Betroffenen zu ihren Rechten oder von einem Betroffenen verlangte Auskünfte, Berichtigungen, Löschungen von Daten werden vom Auftragnehmer unverzüglich an den Auftraggeber zur Erledigung weitergeleitet. Auskünfte an Dritte dürfen nur nach Weisung des Auftraggebers erteilt werden oder sind an den Auftraggeber zur Erledigung weiterzuleiten. Ebenso dürfen Auskünfte an Beschäftigte des Auftraggebers nicht unmittelbar an diese, sondern nur über die vereinbarten Kontaktpersonen erteilt werden.

§ 13 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer sichert ein dem Risiko für die Rechte und Freiheiten der Betroffenen adäquates Schutzniveau der personenbezogenen Daten zu. Zu diesem Zweck verpflichtet sich der Auftragnehmer, seine innerbetriebliche Organisation und die erforderlichen technischen und organisatorischen Maßnahmen unter Berücksichtigung des jeweiligen Stands der Technik, der Implementierungskosten und der Art, des Umfangs sowie der Umstände und Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen so zu gestalten und laufend zu aktualisieren, dass diese den besonderen Anforderungen des Datenschutzes nach der DSGVO entsprechen und den Schutz der Rechte der betroffenen Personen gewährleisten.

Die technischen und organisatorischen Maßnahmen umfassen insbesondere

a) die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten,
b) die rasche Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen im Fall eines physischen oder technischen Zwischenfalls und
c) die Einführung und das Vorhalten von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Der Auftragnehmer sichert die Einhaltung der in der Selbstauskunft vom Mai 2018 genannten Maßnahmen und Regelungen zu. Diese Maßnahmen gelten als vereinbart und die Beschreibung der Maßnahmen wird Bestandteil dieses Vertrages.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragnehmer kann die Eignung der nach Art. 32 DSGVO zu treffenden technisch-organisatorischen Maßnahmen durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO oder eines Datenschutzsiegels oder Prüfzeichen nach Art. 42 DSGVO nachweisen, das für die vertragsgegenständlichen Verarbeitungsverfahren und Orte erteilt und für die unter diese Vereinbarung fallenden Verarbeitungsverfahren relevant ist. Der Auftragnehmer hat Veränderungen am Zertifikat oder dessen Ablauf dem Auftraggeber unverzüglich mitzuteilen. Die Kontroll- und Auditrechte des Auftraggebers bleiben unberührt.

§ 14 Verfahren nach Beendigung des Auftrages

(1) Nach Abschluss der Verarbeitung, spätestens nach Beendigung dieses Vertrages, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse oder zur Leistungserfüllung hergestellten oder kopierten personenbezogenen oder sonstige vertrauliche Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder in Abstimmung mit dem Auftraggeber datenschutzgerecht zu vernichten oder sicher zu löschen. Test- und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen. Diese Verpflichtung gilt in gleichem Maße auch für eventuell beauftragte Unterauftragnehmer. Unberührt bleiben Daten, deren Löschung aus technischen Gründen nicht möglich ist oder einen unverhältnismäßig hohen Aufwand verursachen würde, sowie Kopien, die zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung oder zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind.

(2) Für diese Daten ist die Verarbeitung gem. Art. 18 DSGVO einzuschränken. Die Daten dürfen durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden und sind nach Ablauf der Aufbewahrungsfrist unverzüglich sicher zu löschen. Der Auftraggeber ist über Art und Umfang dieser gespeicherten Daten zu unterrichten. Der Auftragnehmer kann diese Daten zu seiner Entlastung bei Vertragsende

dem Auftraggeber übergeben.

(3) Der Auftragnehmer hat dem Auftraggeber nach Beendigung dieses Vertrages die sichere Löschung bzw. die sichere Vernichtung aller in seinem Besitz befindlichen Unterlagen schriftlich zu bestätigen.

§ 15 Vertragsdauer, Kündigung

(1) Der Vertrag kann von beiden Parteien mit einer Frist von 30 Tagen zum Monatsende gekündigt werden.
Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers oder eines Unterauftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen diese Vereinbarung vorliegt, der Auftragnehmer oder ein Unterauftragnehmer einer Weisung des Auftraggebers nicht nachkommt oder ein Auftragnehmer oder der Unterauftragnehmer sich einer angemessenen Datenschutzkontrolle entzieht.

(2) Eine Kündigung des Vertrags kann nur schriftlich erfolgen.

§ 16 Wirksamkeit der Vereinbarung <Salvatorische Klausel>

(1) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

§ 17 Haftung

(1) Für die Haftung gelten die Regelungen des Art. 82 DSGVO.

§ 18 Vertragsstrafen

(1) Für Verstöße gegen Vertragspflichten des Auftragnehmers wird eine Vertragsstrafe vereinbart, deren Höhe nach billigem Ermessen durch den Auftraggeber zu bestimmen und vom zuständigen Amts- oder Landgericht überprüfbar ist (neuer Hamburger Brauch).

§ 19 Anwendbares Recht und Gerichtsstand

(1) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

(2) Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und datenschutzrelevante Streitigkeiten ist Saarbrücken, Deutschland.
Gesetzliche Regelungen über ausschließliche Zuständigkeiten bleiben unberührt.

§ 20 Geheimhaltungsvereinbarungen, Abwehr von Ansprüchen

(1) Sollten mit dem Auftraggeber geschlossene Geheimhaltungsvereinbarungen der Abwehr von Ansprüchen entgegenstehen, so ist der Auftragnehmer für diesen Fall von der vertraglich vereinbarten Geheimhaltungspflicht entbunden.
(2) Gleiches gilt für Details zur Datenverarbeitung sowie für Details zu den vom Auftraggeber erteilten Weisungen.

Ort/Datum	Ort/Datum
Unterschrift/Stempel Auftraggeber	Unterschrift/Stempel Auftragnehmer

Anlage 1
Beschreibung der vereinbarten technischen und organisatorischen Maßnahmen

Folgende technische und organisatorische Maßnahmen sind eingerichtet und gelten als vereinbart:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
- Zutrittskontrolle

Die Daten werden auf Servern des Auftragnehmers gespeichert, die sich in einem sicheren Datacenter in einem verschlossenen Cage bei Equinix EMEA B.V. Frankfurt/Main befinden. Zugang zu den Servern erhalten nur vom Auftragnehmer autorisierte Personen. Der Zugang ist über eine elektronische Zutrittskontrolle gesichert.

- Zugangskontrolle

Der Zugang zu den Servern ist über eine elektronische Zutrittskontrolle und sichere Passwörter gesichert. Externer Zugriff erfolgt über ein gesichertes VPN.

- Zugriffskontrolle

Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten innerhalb des Systems durch Zugangssicherung via VPN, Eingabe eines Masterpassworts für den Zugang zum Administrationsbereich und Abfrage eines weiteren Passworts zur Autorisierung des Nutzers.

- Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden durch Speicherung der Daten der Kunden in einzelnen, von einander getrennten Bereichen in den Datenbanken:

2. Integrität, Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
- Weitergabekontrolle

Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung der personenbezogenen Daten, die von den Kunden des Auftraggebers über Formulare eingegeben werden. Zugang zu den Daten hat lediglich der Auftraggeber. Berechtigte Mitarbeiter des Auftragnehmers können nach Weisung durch den Auftraggeber lediglich Leseoperationen auf diese Daten durchführen.

- Eingabekontrolle

Feststellung, ob, wann und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch Speicherung eines Timestamps bei der Löschung der Daten und Speicherung des Namens derjenigen Person, die eine Löschung durchführt.:

3. Verfügbarkeit, Belastbarkeit und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)
- Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung von Hard- und Software bzw. Verlust von personenbezogenen Daten durch tägliche Backups.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)
- Datenschutz- und Datensicherheitsmanagement
- Bestellung eines betrieblichen Datenschutzbeauftragten
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle
- Verfahren zur Überwachung von Verarbeitungsprozessen, Protokollierungen, Überwachung von Wartungstätigkeiten, vertragliche Regelungen.

Anlage 2
Unterauftragnehmer

Unterauftragnehmer, Name, Adresse	Beauftragte Leistungen	Vertragsbeginn
Chargebee Inc. 340 S Lemon Avenue, #1537 Wal nut, California 91789, USA.	Abwicklung der, im Rahmen der vom Auftraggeber in Anspruch genommenen Supportleistung, angefallenen Kosten und Entgelte.	Mai 2018
Intercom Inc., 55 2nd St, 4th Fl. San Francisco, CA, 94105 USA	Betrieb der Support- und Kommunikationsplattform zwischen Auftragnehmer und Auftraggeber.	Mai 2018