Vereinbarung über Auftragsverarbeitung

zwischen der

…

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

MessengerPeople GmbH
Herzog-Heinrich-Str. 9
80336 München

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1. Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die vorliegend über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO vorliegend die Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person definiert, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
(4) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO 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.

2. Gegenstand und Dauer des Auftrags

(1) Der Auftragnehmer erbringt für den Auftraggeber Dienste im Bereich der Kommunikation über Messenger-Plattformen von Drittanbietern (im Folgenden auch Messenger-Services) auf Grundlage der bei Auftragserteilung geltenden Allgemeinen Geschäftsbedingungen des Auftragnehmers (im Folgenden Auftrag).
(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Auftrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

(3) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Auftrags vor.
(4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Auftrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

3. Konkretisierung des Auftragsinhalts

(1) Grundsätzlich findet die Datenverarbeitung des Auftragnehmers, insbesondere die Speicherung und Nutzung von Kunden- und Endnutzerdaten zum Zweck der Erbringung der Messenger-Services, ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
(2) Die Beschränkung des Abs. 1 gilt nicht, soweit der Auftragnehmer für den Auftraggeber Daten und Informationen bestimmungsgemäß über einen Messenger eines Drittanbieters an dessen Kunden/Endnutzer/Abonnenten überträgt. Hierfür gilt die Zustimmung des Auftraggebers als erteilt.
(3) Die Beschränkung des Abs. 1 gilt auch nicht, sofern der Auftragnehmer auf Wunsch des Auftraggebers Daten und Informationen bestimmungsgemäß über einen Mailanbieter an dessen Mitarbeiter überträgt. Hierfür gilt die Zustimmung des Auftraggebers als erteilt.

4. Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das geltende Recht zu weiteren Verarbeitungsarten verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.
(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Auftrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.
(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.
(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers 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.

5. Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Speicherung und Nutzung von Kunden- und Endnutzerdaten zum Zweck der Erbringung der Messenger-Services.

(2) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden/Endnutzer/Abonnenten des Auftraggebers
  Mit diesen Personen kommuniziert der Auftraggeber über den Messenger-Service und verwendet dafür bestimmte personenbezogene Daten
- Beschäftigte des Auftragsgebers
  Diese Personen agieren im Verhältnis von Auftraggeber und Auftragnehmer, wodurch bestimmte personenbezogene Daten verwaltet werden.

(3) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- Kunden/Endnutzer/Abonnenten/Beschäftigte des Auftraggebers:
  - Evtl. Name, Vorname, Profilbild und andere Profildaten
  - Kommunikationsdaten (z.B. Telefonnummern, E-Mailadressen)
  - Chathistorie und davon abgeleitete Daten.

6. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer 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 zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dies einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage].

(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.

7. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(3) Wenn der Auftraggeber einen Endnutzer/Abonnenten manuell über die Benutzeroberfläche löscht, so werden

a) alle Chats und abgeleiteten Profildaten sofort in der Datenbank gelöscht;
b) der Nutzereintrag mit der Telefonnummer nach etwa 1-2 Stunden gelöscht. Die Verzögerung ist nötig, damit der Kunden/Endnutzer/Abonnent des Auftraggebers noch aus den Broadcastlisten in der App entfernt und die Statistik aktualisiert werden kann;
c) Nach der Löschung in der Datenbank sind die Informationen zu dem Kunden/Endnutzer/Abonnenten des Auftraggebers noch in den Backupdaten vorhanden. Diese werden nach spätestens 61 Tagen überschrieben, s. auch Punkt 13 (4).

8. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu den Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO zu beachten; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt und dessen jeweils aktuelle Kontaktdaten auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt werden;
b) die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind;
c) die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in der Anlage];
d) Zusammenarbeit der Parteien mit den Aufsichtsbehörden
e) unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag 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 Auftragnehmer ermittelt;

f) soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen;

g) der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird;

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

9. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Die Erhebung etwaiger Daten von einem Messenger bzw. die Übermittlung von Daten an diese ist im Verhältnis zwischen dem Auftragnehmer und dem Betreiber des jeweiligen Messenger nicht als Unterauftragsverhältnis zu verstehen. Unterauftragsverhältnisse sind auch nicht solche Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen und Post-/ Transportdienstleistungen in Anspruch nimmt. Der Auftragnehmer 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 Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen, soweit

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu:

Unterauftragnehmer	**Anschrift**	**Leistung**
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Bereitstellung der Rechenzentrums-infrastruktur für das Serviceangebot

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit der wirksamen Unterbeauftragung gestattet.
(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer 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 Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

10. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch eigens zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).

(4) Falls der Auftraggeber eine Überprüfung (Audit) beim Auftragnehmer bzw. dessen Unterauftragnehmern veranlasst, kann der Auftragnehmer einen branchenüblichen Vergütungsanspruch geltend machen, der eventuell anfallende Reisekosten, externe Hosting Provider Aufwandskosten und Aufwand durch den Datenschutzbeauftragten des Auftragnehmers abdeckt. Diese Kosten werden vor Beginn der Prüfung zwischen Auftraggeber und Auftragnehmer abgestimmt.

11. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.
Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische

Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
d) die Unterstützung des Auftraggebers bei der Datenschutz-Folgenabschätzung;
e) die Unterstützung des Auftraggebers im Rahmen der Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten bzw. nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

12. Haftung

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

13. Beendigung des Auftrages

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Auftrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern keine rechtliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.
(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Auftrags hinaus, die ihm im Zusammenhang mit dem Auftrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Auftrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

(4) Personenbezogene Daten des Auftraggebers werden 28 Tagen nach der Beendigung des Auftrags gelöscht. Im Backup sind die Daten noch maximal weitere 61 Tage vorhanden.

14. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(3) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist München.

Anlage

Technisch-organisatorische Maßnahmen (Art. 32 DSGVO)

Technisch-Organisatorische Maßnahmen
(Art. 32 DSGVO, § 64 BDSG (neu))

DSGVO	BDSG	Maßnahmen
Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)		
	Verschlüsselung	
		Die Kennwörter von Bearbeitern werden als Hash mit einem Salt gespeichert
Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)		
	Zutrittskontrolle	
		Elektronisches Zutrittskontrollsystem mit Protokollierung (Hetzner)
		Dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für sein Colocation Rack) (Hetzner)
		Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude (Hetzner)
		24/7 personelle Besetzung der Rechenzentren (Hetzner)
		Videoüberwachung an den Ein- und Ausgängen (Hetzner)
		Dokumentierte Schlüsselvergabe an Mitarbeiter
		Spezialschlüssel mit Kopierschutz
	Zugangskontrolle	
		Passwortvergabe (Klein- und Großbuchstaben, Sonderzeichen, Zahlen, min. 8 Zeichen, regelmäßiger Wechsel, Passworthistorie)
		Regelmäßige Passwortänderung

		Bildschirmsperre bei Abwesenheit mit Passwort-Aktivierung
		Rollenbezogene Rechte sind an Zugangs-kennungen gebunden (Einteilung nach Administrator, Benutzer etc.)
	Zugriffskontrolle	
		Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung
		Schriftliches Berechtigungskonzept -und ein programmtechnisches Berechtigungskonzept
		Nur ein kleiner Kreis von Administratoren hat Zugriff auf die Datenbank
		Clear Desk Policy
		Kontrollierte Vernichtung von Datenträgern (Papier per Schredder)
		Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches
	Trennungskontrolle	
		Buchungsinformationen und Abonnenten Informationen werden in verschiedenen Datenbanken gespeichert
		Die Daten der Mandanten werden getrennt verarbeitet und sind durch eindeutige Identifikationen voneinander getrennt
Integrität (Art. 32 Abs. 1 lit. b DSGVO)		
	Weitergabekontrolle	
		Die Datenübertragung vom Auftraggeber an den Auftragnehmer kann auf unterschiedliche Arten erfolgen. Im Regelfall werden die Daten über die Kundenoberfläche zur Verfügung gestellt. Die Übertragung ist SSL verschlüsselt

		Der Auftragnehmer unterstützt gängige sichere Varianten
		Verschlüsselte Tunnelung von Verbindungen oder sichere Übertragung via VPN
	Datenträgerkontrolle	
		Verbot der Nutzung privater Datenträger am Arbeitsplatz
	Eingabekontrolle	
		Personen identifizierbare Eigenschaften (Telefonnummer) können über die Kundenoberfläche nicht geändert werden
		Statusänderungen bei Abonnenten werden bis zur Löschung gespeichert
		Protokollierung von Änderungen
		Gegenseitige Überwachung (4 Augen Prinzip)
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)		
	Verfügbarkeitskontrolle	
		Die Datenbank wird online gespiegelt. Die Spiegelung kann mit Hilfe von Failover IPs aktiviert werden
		Ein Backup-Verfahren ist eingerichtet
		Einsatz unterbrechungsfreier Stromversorgung
		Virenschutz ist installiert
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d und Art. 25 DSGVO)		
	Belastbarkeit	

		Es ist eine Notfallplanung vorhanden und in Notfallkonzepten dokumentiert
		Die Funktionsfähigkeit dieser Konzepte wird in regelmäßigen Abständen (meist jährlich) geprüft
		Die Notfallpläne werden einem regelmäßigen Prüf- und Verbesserungsprozess unterzogen
	Incident-Response-Management	
		Ein Ticketsystem stellt die zeitnahe Abarbeitung aller Anfragen sicher
	Datenschutzfreundliche Voreinstellungen	
		Double-Opt-in-Verfahren
	Auftragskontrolle	
		Die Änderung von personenbezogenen Daten durch den Auftragsverarbeiter im Sinne von Art. 28 DSGVO erfolgt nur nach entsprechender Weisung des Auftraggebers
		Regelmäßige Kontrolle eingesetzter Unterauftragnehmer