Vertrag zur Auftragsverarbeitung

Stand 24.05.2018

Vereinbarung zwischen dem/der **Verantwortlichen**

_____

_____

_____

nachstehend **Auftraggeber** genannt

und der

web-me.de Internet Service e.K.
Merowingerstraße 6
D-78662 Bösingen

nachstehend **Auftragsverarbeiter** genannt,

nachstehend zusammen als **Partei/Parteien** bezeichnet.

Es besteht ein Kundenkonto im Rahmen einer Anmeldung unter https://www.teammessage.de unter der Kundennummer _____ .

Vom Auftragsverarbeiter benannter **Ansprechpartner für Datenschutz / Datenschutzbeauftragter**:

Dipl. Ing. (FH) Rainer Thieringer (+49-7404-910386, dsb@web-me.de / dsb@teammessage.de).

Präambel

1. Der Auftragsverarbeiter stellt eine Gatewayfunktionalität zum Versand von SMS und E-Mail zur Verfügung.
2. Der Auftraggeber und der Auftragsverarbeiter haben unter Umständen bereits einen Einzelvertrag im Rahmen einer Anmeldung über die Internetseite https://www.teammessage.de abgeschlossen. Unter diesem Namen bietet der Auftragsverarbeiter die Weiterleitung eingehender Nachrichten an.
3. Die Parteien möchten die Vereinbarung der Parteien in Bezug auf die Verarbeitung personenbezogener Daten unter Einhaltung der maßgeblichen Datenschutzgesetze und -vorschriften, insbesondere unter Einhaltung von Artikel 28 der EU-Datenschutz-Grundverordnung, abbilden.
4. In Bezug auf die Verarbeitung personenbezogener Daten ersetzen die Bestimmungen dieses Vertrags zwischen dem Auftraggeber und dem Auftragsverarbeiter sämtliche vorherigen Übereinkommen und Vereinbarungen zwischen den Parteien. Bei Widersprüchen zwischen den Bestimmungen des Einzelvertrags und diesem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter ist Letzterer maßgebend.

BEGRIFFSBESTIMMUNGEN UND AUSLEGUNG

Vertrag bezeichnet diesen Vertrag samt den beigefügten Anhängen.
Nebendienstleistungen bezeichnet Dienstleistungen, die unabhängig vom Gegenstand dieses Vertrags sind, wie etwa Telekommunikationsdienste, Post-/ Transportdienste, Instandhaltungs- und unterstützende Dienstleistungen für Nutzer oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hardware und Software von Datenverarbeitungsanlagen.
Anhang bezeichnet jeden Anhang zu diesem Vertrag, der als Vertragsbestandteil anzusehen ist.
Weiterer Auftragsverarbeiter bezeichnet einen von dem Auftragsverarbeiter im Lauf der Erbringung der Dienstleistungen beauftragten Datenverarbeiter.
Verantwortlicher bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.
Datenschutzgesetze bezeichnet die EU-Datenschutzgesetze sowie das BDSG in der Fassung ab 25.05.2018und, soweit anwendbar, die Datenschutzgesetze eines anderen Landes.
EWR bezeichnet den Europäischen Wirtschaftsraum und besteht aus sämtlichen Ländern der Europäischen Union,

Liechtenstein, Norwegen und Island.
DS-GVO bezeichnet 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).
Personenbezogene Daten bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Als identifizierbar wird eine natürliche Person angesehen, 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.
Verarbeitung bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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.
Auftragsverarbeiter bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Dienstleistungen bezeichnet sämtliche Dienstleistungen, die der Auftragsverarbeiter, wie im Rahmen des Dienstleistungsvertrags vereinbart, erbringt.
Dienstleistungsvertrag bezeichnet den Vertrag, den die Parteien in Bezug auf die Erbringung von Dienstleistungen durch den Auftragsverarbeiter abgeschlossen haben.
"SMSC" bezeichnet einen Server, der SMS-Kurznachrichten an die Mobilfunknetzbetreiber übergibt, so dass die SMS-Kurznachricht einem Mobilfunkteilnehmer zugestellt werden kann.

1) Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags
Der Auftragsverarbeiter stellt eine Gatewayfunktionalität zum Versand von SMS und E-Mail zur Verfügung. Die Leistung umfasst die unverzügliche Weiterleitung eingehender Nachrichten an die Betreiber der Mobilfunknetze und Mailserver.

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich weisungsgebunden für den Auftraggeber. Er hat keine Entscheidungsbefugnis über die übermittelten Daten und deren Verarbeitung. Außer der Übermittlung an nachgeordnete Telekommunikationsdienstleister ist eine Weitergabe der Daten an Dritte ausgeschlossen.

Weisungsberechtigt beim Auftraggeber sind:

1. Amtierende Geschäftsführer
2. IT Administratoren
3. Datenschutzbeauftragter

Die beim Dienstleister als Weisungsempfänger befugte Personen sind

1. Geschäftsführer (CEO)
2. Technischer Geschäftsführer (CTO)

(2) Dauer des Auftrags
Der Auftrag ist unbefristet erteilt und kann von beiden Parteien jeweils bis zum Ablauf jedes angefangenen monatlichen Zahlungszeitraums gekündigt werden.

2) Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Die Dienstleistung besteht primär im Versand von Textnachrichten per SMS oder E-Mail an die Adressaten, die der Auftraggeber als Dienstleistung im Kundenauftrag umsetzt oder an eigene Kunden adressiert.
Die Erbringung dieser Datenverarbeitung findet ausschließlich in Deutschland oder einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung der Dienstleistung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Arten von Daten

1. Kommunikationsdaten (Telefonnummer, Mobilfunknummer, E-Mail-Adresse)
2. Betreff und textueller Inhalt der vom Auftraggeber übergebenen und zu übermittelnden Nachricht

Daten folgenden Inhalts sind von der Übermittlung zur Auftragsverarbeitung ausgeschlossen:

1. Gesundheitsdaten
2. Daten zum Sexualleben oder zur sexuellen Orientierung
3. genetische Daten
4. Daten, aus denen die rassische oder ethnische Herkunft hervorgeht
5. Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht
6. Daten über strafrechtliche Verurteilungen oder Straftaten

(3) Kategorien betroffener Personen
Die Kategorien der durch die Datenverarbeitung betroffenen Personen aus Sicht des Auftraggebers umfassen eine oder mehrere der folgenden Personengruppen:

1. Kunden des Auftraggebers
2. Mitarbeiter verbundener Gesellschaften des Auftraggebers
3. Auftragsverarbeiter
4. Interessenten
5. Ansprechpartner in Firmen

3) Technisch-organisatorische Maßnahmen

(1) 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 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 dieser einvernehmlich umzusetzen.

(2) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen. Die technisch-organisatorischen Maßnahmen sind in Anlage 1 dokumentiert.

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

(4) Die Dienstleistungen, die der Auftragsverarbeiter erbringt, unterliegen neben der DS-GVO und dem BDSG (gültige Fassung ab 26.05.2018) auch dem Telekommunikationsgesetzes (TKG) und dem Telemediengesetzes (TMG) in den jeweils gültigen Fassungen bzw. zukünftig der e-Privacy Verordnung der EU. Der Auftragsverarbeiter ist verpflichtet, diese und auch darüber hinausgehende gesetzlichen Anforderungen zu erfüllen.

4) Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter 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 Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Eine Löschung, Berichtigung, die Umsetzung des Rechts auf Auskunft, Vergessenwerden und der Datenportabilität nach dokumentierter Weisung des Auftraggebers ist unmittelbar durch den Auftragnehmer sicherzustellen. Der Auftragsverarbeiter hat den Auftraggeber nach Möglichkeit bei der Erfüllung der Pflicht des Auftraggebers zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person zu unterstützen. Zu diesen Rechten zählen das Recht auf Vergessenwerden sowie die Rechte auf Berichtigung, Datenübertragbarkeit und Auskunft.

(3) Wird vom Auftraggeber keine gesonderte dokumentierte Weisung übergeben, werden die zur Verarbeitung übergebenen Daten nach dem Standardverfahren des Auftragsverarbeiters sukzessive gelöscht:

1. der Textanteil eingehender Nachrichten wird in der Länge so reduziert, dass der Text in eine SMS-Nachricht passt; Dieser Textanteil sowie Absender, Empfänger, Zeitpunkt und Statusinformationen zur Zustellung werden vom Auftragsverarbeiter in einer lokalen Datenbank zum Nachweis der Leistung gespeichert.

2. verarbeitete E-Mails werden nach spätestens 2 Wochen gelöscht;
3. der Textanteil von verarbeiteten Nachrichten wird nach 400 Tagen aus der Datenbank gelöscht;

5) Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Vertrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Die Benennung eines Ansprechpartners oder Datenschutzbeauftragten. Der Auftraggeber ist über etwaige diesbezügliche Änderungen unverzüglich in Kenntnis zu setzen. Anmerkung: Der Auftragsverarbeiter ist nach dokumentierter Selbsteinschätzung auf Basis der Firmengröße und des Schutzbedarfs der verarbeiteten Daten nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet.
2. Das Führen eines Verzeichnisses der Verarbeitungstätigkeiten
3. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter 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.
4. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (siehe Anlage).
5. Der Auftraggeber und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
6. Die 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 Auftragsverarbeiter ermittelt.
7. 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.
8. Der Auftragsverarbeiter 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.
9. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6) Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung 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 Auftragsverarbeiter darf Unterauftragsnehmner (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Ausgenommen von dieser ausdrücklichen Zustimmung sind SMSC-Dienstleister und Mobilfunknetzbetreiber, insofern diese die Einhaltung der gesetzlichen Vorgaben aus dem deutschen Telekommunikationsgesetz (TKG) und dem deutschen Telemediengesetz (TMG) gewährleisten.
Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

1. Hostsharing eG, Flughafenstraße 52a, 22335 Hamburg | Land: Deutschland | Leistung: Verantwortlicher Hoster für den Betrieb der Serverinfrastruktur.
2. mehrere namentlich nicht benannte SMSC-Dienstleister | Land: Deutschland und Dänemark | Leistung: Redundant aufgebaute SMSC Infrastruktur zum Übergabe der SMS-Nachrichten an die Mobilfunknetzbetreiber. Diese Dienstleister unterliegen dem Fernmelde- und Kommunikationsgeheimnis laut TKG / TMG. Jede Weitergabe der personenbezogenen Daten an Dritte ist auch unterbeauftragten Dienstleistern untersagt.

Ein Wechsel bestehender Unterauftragnehmer ist zulässig, soweit:

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

(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) Beim Einsatz von Unterauftragnehmern stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform).

(5) Der Auftragsverarbeiter führt jegliche Verarbeitung in Rechenzentren innerhalb der Bundesrepublik Deutschland durch. Dies gilt auch für etwaige Unterauftragnehmer. Die Übergabe der verarbeiteten Nachrichten an die Mobilfunknetzbetreiber und SMSC werden über Server in Deutschland durchgeführt.

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmern aufzuerlegen.

7) Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall 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 Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter 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

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

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

8) Mitteilung bei Verstößen des Auftragsverarbeiters

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

1. 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
2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
3. 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

4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
5. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

9) Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragsverarbeiter hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10) Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder Abrechnung und Nachweis der erbrachten Leistung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Testmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(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.

11) Unterstützungspflichten

(1) Der Auftragsverarbeiter hat den Auftraggeber bei der Erfüllung der Pflichten betreffend der Sicherheit personenbezogener Daten, der Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten, der Datenschutz-Folgenabschätzungen und vorherige Konsultationen nach Maßgabe von Artikel 33 bis 36 DS-GVO zu unterstützen.

Dies umfasst insbesondere

1. die Pflicht, eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Auftraggeber zu melden.
2. die Pflicht, den Auftraggeber im Hinblick auf die Pflicht des Auftraggebers zur Bereitstellung von Informationen zur betroffenen Person zu unterstützen und dem Auftraggeber unverzüglich sämtliche relevanten Informationen zur Verfügung zu stellen. Zu den mindestens zu übermittelnden Informationen zählen die Art der Verletzung des Schutzes personenbezogener Daten, die Kategorien und die Zahl der betroffenen Personen, die Kategorien und die Zahl der Datensätze sowie die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.
3. die Unterstützung des Auftraggebers bei einer Datenschutz-Folgenabschätzung.
4. die Unterstützung des Auftraggebers in Bezug auf das Verzeichnis der Verarbeitungstätigkeiten.
5. die Unterstützung des Auftraggebers in Bezug auf die Konsultation der Aufsichtsbehörde.

Für die Unterstützung kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

12) Haftung und Sanktionen

Die gesetzlichen Bestimmungen, insbesondere Artikel 82 DS-GVO, gelten im Fall von Schadensersatz- oder Haftungsforderungen.

13) Schlussbestimmungen

(1) Eine Änderung oder Ergänzung dieses Vertrags bedarf der Schriftform und der Unterzeichnung der ordnungsgemäß bevollmächtigten Vertreter beider Parteien.

(2) Werden Daten des Auftraggebers Gegenstand einer Durchsuchung und Beschlagnahme, eines Pfändungsbeschlusses, einer Einziehung im Rahmen eines Konkurs- oder Insolvenzverfahrens bzw. ähnlicher Ereignisse oder Maßnahmen Dritter, während sie im Verantwortungsbereich des Auftragsverarbeiters sind, so hat der Auftragsverarbeiter den Verantwortlichen hierüber unverzüglich in Kenntnis zu setzen. Der Auftragsverarbeiter hat sämtlichen Beteiligten dieser Maßnahme unverzüglich mitzuteilen, dass sich hiervon betroffene Daten ausschließlich im Eigentum des Auftraggebers befinden und in dessen Verantwortungsbereich liegen, dass der Verantwortliche das alleinige Verfügungsrecht über diese Daten hat und dass der Auftraggebers für die Anwendung des Datenschutzrechts zuständig ist.

(3) Sollte eine Bestimmung dieses Vertrags gleich aus welchem Grund für ungültig, rechtswidrig oder undurchsetzbar befunden werden, wird die betreffende Bestimmung ausgenommen und bleiben die übrigen Bestimmungen dieses Vertrags so in vollem Umfang in Kraft und rechtswirksam, als wäre dieser Vertrag ohne die ungültige Bestimmung geschlossen worden.

(4) Dieser Vertrag unterliegt dem EU-Recht.

Anlagen:

1. Technisch-organisatorische Maßnahmen

Auftraggeber / Verantwortlicher:	_____
Ort / Datum:	_____
Unterschrift:	_____
Auftragnehmer / Auftragsverarbeiter:	Susanne Thieringer, web-me.de Internet Service e.K.
Ort / Datum:	_____
Unterschrift:	_____

TOM - Technisch-organisatorische Maßnahmen

Angelegt Sonntag 06 Mai 2018
Datum der letzten Änderung 06 Mai 2018

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 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 dieser einvernehmlich umzusetzen.

Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen (Einzelheiten siehe Anlage).

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

TOM001 Vertraulichkeit

Angelegt 06 Mai 2018
Datum der letzten Änderung 08 Mai 2018

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

Der Betrieb der Serverinfrastruktur ist an einen Unterauftragnehmer - hier Hoster genannt - ausgelagert. Auftragsverarbeiter aus Sicht des Endkunden ist die Firma web-me.de Internet Service e.K.

Zutrittskontrolle

Zutrittskontrolle dient dem Schutz der Datenverarbeitungsanlagen vor unberechtigtem, physischem Zutritt. Der beauftragte Hoster realisiert die Zutrittskontrolle über folgende, mehrstufige Absicherung:

1. Der Zutritt zu den Rechenzentren ist durch Videoüberwachung an Ein- und Ausgängen, Sicherheitsschleusen und Cages (extra abgesicherte Bereichen innerhalb des Rechenzentrumstandorts Berlin) gesichert. Der Zutritt zum Rechenzentrum ist ausschließlich in Begleitung autorisierten Personals zulässig. Der Zutritt zu den Rechenzentren wird kontrolliert und protokolliert.
2. Der Zutritt zu den Cages wird durch eine Schließanlage gesichert und mittels Kamera überwacht.
3. Der Zutritt zum einzelnen Cage ist ausschließlich in Begleitung autorisierten Personals zulässig.
4. Der Zutritt zu den Racks (den Serverschränken innerhalb der Cages), ist durch eine weitere Schließanlage gesichert und ausschließlich in Begleitung autorisierten Personals zulässig.
5. Der Zutritt erfolgt nach Legitimation mit Zugangskarte und PIN. Die Schlüsselvergabe erfolgt ausschließlich an autorisierte Mitarbeiter und Kunden. Jeder Kunde erhält ausschließlich Zutritt zu seinen Racks.

Zugangskontrolle

Zugangskontrolle dient dem Schutz der Datenverarbeitungsanlagen vor unberechtigtem, logischem Zugriff. Der beauftragte Hoster realisiert die Zugangskontrolle über folgende, mehrstufige Absicherung:

1. Der Zugang zur Administration der Server erfolgt ausschließlich über eine geschützte Verbindung.
2. Der Zugang ist per Public Key-Verfahren geschützt, Zugriff erfolgt über personenbezogene Benutzerkonten.
3. Der Zugang für administrative Zugriffe erfolgt über eine zweistufige Zugangssicherung mit Protokollierung.
4. Der beauftragte Hoster verantwortet die Zugangskontrolle in Bezug auf Sicherheit und Updates der betriebsbereit vorgehaltenen Software.
5. der Auftragsverarbeiter verantwortet die Zugangskontrolle in Bezug auf Sicherheit und Updates der selbst verantworteten installierten Software. Insbesondere des Content Management-Systems und der Programme zur Verteilung von Nachrichten.

Zugriffsskontrolle

Zugriffskontrolle dient dem Schutz der Daten von unbefugtem Lesen, Kopieren, Verändern oder Löschen personenbezogener Daten innerhalb des Systems. Der beauftragte Hoster realisiert die Zugriffskontrolle über folgende, mehrstufige Absicherung:

1. Support-Mitarbeiter haben generell keinen Zugriff auf die Daten in den Datenbanken oder in Benutzerverzeichnissen der Kunden.
2. für die Mitarbeiter des Hosters ist ein verbindliches Berechtigungsvergabeverfahren festgelegt.
3. im Falle des Bekanntwerdens von Sicherheitslücken sollen unverzüglich Sicherheitsupdates installiert werden.
4. der Hoster stellt sicher, dass defekte Datenträger, die nicht sicher gelöscht werden können, direkt im Rechenzentrum zerstört (geschreddert) werden.
5. der beauftragte Hoster verantwortet die Zugriffskontrolle in Bezug auf Sicherheit und Updates der betriebsbereit vorgehaltenen Software.
6. web-me.de verantwortet die die Zugriffskontrolle in Bezug auf Sicherheit und Updates der selbst verantworteten installierten Software. Insbesondere des Content Management-Systems und der Programme zur Verteilung von Nachrichten.

Trennungskontrolle

Daten unterschiedlicher Mandanten (Stammdaten, Verbindungsdaten, Mobilfunknummern, verwendete Personennamen) liegen aus technischen Gründen in einer Datenbank - Vergleichbar mit einem Mailserver. Bei besonderem Schutzbedarf und gegen separaten Auftrag und zusätzlichen Betriebskosten können die Daten komplett separiert verarbeitet werden.

Im Fall eines Löschauftrags können die Daten selektiv und wie vom Auftraggeber gefordert gelöscht werden.

Pseudonymisierung

(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Die Ablage übergebener Daten ermöglicht technisch bedingt die Zuordnung einer Textnachricht zu einer Mailadresse oder Mobilfunknummer. Nach Ermessen und in Verantwortung des Auftraggebers können auch Vorname und Nachname (Klarname) einer Person mit übergeben oder vorab angelegt werden (vom Auftraggeber im geschützten Bereich angelegte Teamlisten / Verteilerlisten). Soll die Anonymität der Empfänger bestmöglich gewahrt bleiben, kann der Auftraggeber jegliches andere Pseudonym anstelle des Klarnamens verwenden.
Bei der Weiterleitung von Nachrichten an die Empfänger werden nur die notwendigsten Daten an die weiteren Dienstleister übergeben. Neben dem Nachrichtentext ist das für SMS die Mobilfunknummer und für E-Mail die Mailadresse.
Außer technisch bedingten Kürzungen werden keine inhaltlichen Veränderungen am Nachrichtentext vorgenommen. Die Verantwortung für ausreichende Pseudonymisierung dieses Inhalts obliegt in vollem Umfang dem Auftraggeber.

Datenminimierung

Der Auftragsverarbeiter verwendet für den Betrieb seiner Dienstleistungen persönliche Daten nur in dem für die Gewährleistung des Betriebes erforderlichen Umfang. Darüber hinaus sind die Auftraggeber im Rahmen der von ihnen betriebenen Anwendungen für die Datensparsamkeit selbst verantwortlich. In der Regel sind nur E-Mailadresse und Mobilfunknummer für den Betrieb essentiell notwendig, nicht aber der öffentliche Name des Empfängers.

TOM002 Integrität

Angelegt 06 Mai 2018
Datum der letzten Änderung 06 Mai 2018

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

Der Betrieb der Serverinfrastruktur ist an einen Unterauftragnehmer - hier Hoster genannt - ausgelagert. Auftragsverarbeiter aus Sicht des Endkunden ist die Firma web-me.de Internet Service e.K.

Weitergabekontrolle

Weitergabekontrolle dient dem Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Löschen von personenbezogenen Daten bei elektronischer Übertragung oder Transport. Der Auftragsverarbeiter und der beauftragte Hoster realisieren die Weitergabekontrolle über folgende, mehrstufige Absicherung:

1. Der beauftragte Hoster realisiert die Weitergabekontrolle durch die Beschränkung der Speicherung auf die dafür vorgesehenen Rechenzentren und Serversysteme.
2. Der beauftragte Hoster unterweist alle Mitarbeiter, die in Kontakt mit personenbezogenen Daten kommen, nach Art. 32 Abs. 4 DS-GVO und verpflichtet sie zur Verschwiegenheit und Sicherstellung des datenschutzkonformen Umgangs mit personenbezogenen Daten.
3. der Auftragsverarbeiter verwendet ausschließlich verschlüsselten Datenübertragung zur Übertragung von personenbezogenen Daten.
4. der beauftragte Hoster gewährleistet die datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

Eingabekontrolle

Eingabekontrolle dient der Nachvollziehbarkeit des Lesens, Kopierens, Veränderns oder Löschens von personenbezogenen Daten. Der Auftragsverarbeiter und beauftragte Hoster realisieren die Eingabekontrolle über eine Aufzeichnung der beim administrativen Zugriff getätigten Eingaben und der täglichen Sicherung der Datenbestände.

TOM003 Verfügbarkeit und Belastbarkeit

Angelegt 06 Mai 2018
Datum der letzten Änderung 06 Mai 2018

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

Der Betrieb der Serverinfrastruktur ist an einen Unterauftragnehmer - hier Hoster genannt - ausgelagert. Auftragsverarbeiter aus Sicht des Endkunden ist die Firma web-me.de Internet Service e.K.

Verfügbarkeitskontrolle

Verfügbarkeitskontrolle dient dem Schutz personenbezogener Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust sowie der rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO). Der beauftragte Hoster realisiert die Verfügbarkeitskontrolle über folgende, mehrstufige Absicherung:

Der beauftragte Hoster

1. setzt Schutzsystemen (SPAM-Filter, Firewalls, Virenscanner, Verschlüsselung, (D)DoS-Abwehr) ein.
2. unterstützt die Verfügbarkeit der Produktivsysteme durch den Einsatz redundanter Stromversorgung, Netzteile, Speichersysteme und Netzwerkkomponenten.
3. unterstützt die Verfügbarkeit der Produktivsysteme durch Spiegelung aller im Produktivbetrieb befindlichen virtuellen Maschinen in Echtzeit auf Standby-Server oder alternativ redundante Auslegung auf Softwareebene.
4. spiegelt alle Kundensysteme in Echtzeit auf Standby-Server, welche im Versagensfall des Primär-Systems die Aufgaben mit aktuellen Daten unverzüglich übernehmen können.
5. führt täglich Datensicherungen der Konfigurations- und Serverdaten durch, welche auf separaten Servern in einem gesonderten Rechenzentrum an einem anderen Standort aufbewahrt werden.
6. verfügt über ein partielles (einzelne Dateien) und vollständiges (virtuelle Maschinen) Datensicherungs- und Wiederherstellungskonzept.
7. überwacht die produktiven Systeme von einem externen Standort aus.
8. alarmiert die Mitarbeiter der technische Rufbereitschaft im Fehlerfall auf zwei unabhängigen Wegen.
9. hat eine eine Eskalationskette für alle internen Systeme definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um ausgefallene Systeme unverzüglich wiederherzustellen.

Diese Maßnahmen und Verfahren des Hosters werden von Auftragsverarbeiter regelmäßig auf Funktionalität und Änderungen überprüft.

TOM004 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Angelegt 06 Mai 2018
Datum der letzten Änderung 06 Mai 2018

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

Der Betrieb der Serverinfrastruktur ist an einen Unterauftragnehmer - hier Hoster genannt - ausgelagert. Auftragsverarbeiter aus Sicht des Endkunden ist die Firma web-me.de Internet Service e.K.

Zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Verfahren hat der beauftragte Hoster folgende Konzepte implementiert:

1. Datenschutz-Management
2. Incident-Response-Management
3. Datenschutzfreundliche Voreinstellungen bei der Softwareentwicklung (Art. 25 Abs. 2 DS-GVO)

Auftragskontrolle

Verfügbarkeitskontrolle dient dem Schutz personenbezogener Daten gegen nicht weisungsgemäße, unbefugte Verarbeitung.

Die verordnungsgemäße Umsetzung der Auftragsverarbeitung gemäß Art. 28 DS-GVO, wird realisiert durch eindeutige Vertragsgestaltungen, sorgfältige Auswahl des Auftragsverarbeiters, Vorabüberzeugung und Nachkontrollen, insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen.

1. der Auftragsverarbeiter schließt mit dem beauftragten Hostern sowie weiteren Unterauftragnehmern vor Beginn der Auftragsverarbeitung schriftliche Vereinbarungen über die Dienstleistungen bzw. zur Auftragsverarbeitung, so dass die Daten vertraulich behandelt bzw. nur entsprechend den Weisungen verarbeitet werden. Mindestens werden jedenfalls dem Sinn und Zweck der DSGVO entsprechende technisch-organisatorische Maßnahmen vereinbart.
2. der Auftragsverarbeiter schließt eine Nutzung oder Weitergabe der Daten durch Mitarbeiter vertraglich aus.
3. der Auftragsverarbeiter verpflichtet den Hoster oder weitere Auftragsverarbeiter Weisungen nur durch autorisierte Mitarbeiter entgegenzunehmen. Diese Aufträge liegen in Textform vor und können nachträglich überprüft werden.
4. Der Hoster verfügt über Datenschutzbeauftragte sowie einen Informationssicherheitsbeauftragten.
5. Die Leistungsbeschreibungen enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.