

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen denen sich aus den AGB ergebenden Vertragsparteien

§ 1 Einleitung

1. Dieser Vertrag regelt das Auftragsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer über die Verarbeitung personenbezogener Daten durch den Auftragnehmer. Die Parteien vereinbaren die Auftragsverarbeitung nach den Regelungen der DSGVO abzuwickeln, um ein angemessenes Datenschutzniveau zu erreichen. Er begründet das Rechtsverhältnis der Auftragsverarbeitung nach Art. 28 DSGVO.
2. Der Auftragnehmer verarbeitet als Auftragsverarbeiter (Art. 4 Abs. 2 DSGVO / Art. 5 Abs. 11 DSG neu CH) personenbezogene Daten für den Auftraggeber. Diese Dienstleistungen werden auf Grundlage des zwischen den Parteien bestehenden, im folgenden bezeichneten Hauptvertrags erbracht.
3. Der Vertrag bezieht sich auf alle Tätigkeiten des Auftragnehmers, seiner Mitarbeiter und seiner Subunternehmer, bei denen es zur Verarbeitung von personenbezogenen Daten oder zur Berührung mit solchen personenbezogenen Daten kommt, die der Auftragnehmer vom Auftraggeber zur Verfügung gestellt bekommen hat.

§ 2 Auftragsgegenstand und -dauer

1. Der Gegenstand des Auftrags ergibt sich aus den AGB und weiteren schriftlichen Nebenabreden, auf welche(n) / welches hierdurch verwiesen wird (nachstehend Hauptvertrag genannt).
2. Die Dauer der Auftragsverarbeitung richtet sich nach dem Hauptvertrag und endet bei unbestimmter Laufzeit durch Kündigung des Haupt- oder diesen Vertrags.

§ 3 Auftragsinhalt

1. Die Verarbeitung dient folgendem Zweck:
Bereitstellung der vereinbarten Dienstleistungen
2. Folgende Verarbeitungsvorgänge gem. Art. 4 Nr. 2 DSGVO personenbezogener Daten finden Anwendung:
 - Erheben
 - Erfassen
 - Organisieren
 - Ordnen
 - Speichern
 - Anpassen
 - Auslesen
 - Abfragen
 - Verändern
 - Verwenden
 - Offenlegen
 - Verbreiten
 - Andere Formen der Bereitstellung
 - Abgleich und Verknüpfung
 - Einschränkung
 - Löschung
 - Vernichtung
3. Der Auftragnehmer darf Daten auch außerhalb der EU oder dem EWG verarbeiten oder von Drittanbietern verarbeiten lassen, ohne vorher eine explizite Einwilligung des Auftraggebers einzuholen. Die besonderen Anforderungen der Art. 44 ff. DSGVO sind zu beachten. Ihre Einhaltung ist festgestellt bzw. wird hergestellt durch:
 - Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO)

- Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO)
4. Folgende Datenkategorien können durch den Auftragnehmer verarbeitet werden:
 - Personenstammdaten
 - Zahlungsdaten
 - Kommunikationsdaten
 - Adressdaten
 - Vertragsdaten
 - Termine
 - Verhaltensdaten
 - Standortdaten
 - Bild- und Videodaten
 - Planungs- / Steuerungsdaten
 5. Die Verarbeitung betrifft die Daten folgender Personengruppen des Auftraggebers:
 - Beschäftigte
 - Dienstleister
 - Interessenten
 - Kunden
 - Geschäftspartner
 - Ansprechpartner
 - Lieferanten
 - Teilnehmer (Markt- und/oder Meinungsforschung)
 6. Rechtsgrundlage der Verarbeitung für den Auftraggeber ist nach Art. 6 DSGVO:
 - Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben (Art. 6 Abs. 1 lit. a DSGVO)
 - Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen (Art. 6 Abs. 1 lit. b DSGVO)
 - Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt (Art. 6 Abs. 1 lit. c DSGVO)
 - Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6 Abs. 1 lit. d DSGVO)
 - Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich (Art. 6 Abs. 1 lit. f DSGVO)
 - Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 6 Abs. 1 lit. e DSGVO)
 Rechtsgrundlage der Verarbeitung für den Auftragnehmer ist Art. 28 DSGVO.

§ 4 Umgang mit den Daten, Weisungsrecht des Auftraggebers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich gemäß dieser vertraglichen Vereinbarung oder nach Weisungen des Auftraggebers. Etwas anderes gilt bei einer gesetzlichen oder behördlichen Verpflichtung des Auftragnehmers zu einer anderweitigen Verarbeitung. Dann hat der Auftragnehmer den Auftraggeber unverzüglich darüber in Kenntnis zu setzen. Eine Verarbeitung personenbezogener Daten des Auftraggebers zu eigenen Zwecken des Auftragnehmers ist ausgeschlossen.
2. Der Auftragnehmer verpflichtet sich, die Anforderungen des Auftragsverarbeiters nach Art. 28 und 32 DSGVO sicherzustellen und den diesbezüglichen Nachweis dem Auftraggeber zu erbringen.
3. Der Auftragnehmer verpflichtet sich, diesen Grundsätzen auch dadurch zu genügen, dass er sein Personal ausreichend in Fragen des Datenschutzes schult und entsprechend nur fachkundiges Personal in Kontakt mit den Daten des Auftraggebers treten lässt. Die Vereinbarung von Geheimhaltungspflichten des Personals ist möglich.
4. Der Auftragnehmer verpflichtet sich zur Einhaltung der Regeln zum Datenschutz und bestätigt die Kenntnis dieser einschlägigen Regelungen zur ordnungsgemäßen Verarbeitung personenbezogener Daten. Er ergreift die erforderlichen technisch-organisatorischen Maßnahmen, um eine ordnungsgemäße Verarbeitung sicherzustellen (siehe § 7).

5. Der Auftragnehmer darf personenbezogene Daten, die er im Auftrag des Auftraggebers verarbeitet, nicht eigenmächtig und nur nach dessen Anweisungen berichtigen, löschen, portieren oder beaskunften oder deren Verarbeitung einschränken. Dies gilt auch dann, wenn eine betroffene Person einen entsprechenden Antrag stellt.
6. Die dem Auftragnehmer vom Auftraggeber zur Verfügung gestellten Daten sind unter strikter Trennung von anderen Datenbeständen zu verarbeiten.
7. Der Auftragnehmer darf keine Kopien der zur Verfügung gestellten Daten ohne Wissen des Auftraggebers erstellen. Eine Ausnahme gilt für technisch notwendige und im Rahmen einer ordnungsgemäßen Verarbeitung erforderliche Vervielfältigungen, bei denen eine Gefährdung der Rechte der betroffenen Personen und eine Absenkung des Datenschutzniveaus ausgeschlossen ist.
8. Der Auftraggeber stellt die Erfüllung der Rechte auf Auskunft, Berichtigung, Einschränkung Löschung sowie Datenportabilität sicher, soweit dies dem Leistungsumfang des Vertrags entspricht.

§ 5 Sonstige Pflichten des Auftragnehmers und Qualitätssicherung

1. Der Auftragnehmer hat zusätzlich gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; darüber hinaus gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
 1. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt, falls rechtlich erforderlich.
 2. Die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO ist zu wahren. Beschäftigte des Auftragnehmers, die er zur Durchführung der Verarbeitung bestellt, müssen zur Vertraulichkeit verpflichtet und mit den für sie zu beachtenden Vorschriften zum Datenschutz vertraut gemacht werden. Der Auftragnehmer und alle ihm unterstellten Personen, die Zugang zu personenbezogenen Daten des Auftraggebers haben, verarbeiten diese ausschließlich gemäß den Weisungen des Auftraggebers und den Bestimmungen dieses Vertrags, sofern gesetzlich keine anderweitigen Vorgaben bestehen. Die Vertraulichkeitsregeln gelten nach Beendigung des Vertrags fort.
 3. Die Einhaltung der für diesen Auftrag erforderlichen organisatorischen und technischen Maßnahmen nach Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (siehe Anlage 1).
 4. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf Gegenstände dieses Vertrags beziehen. Dies gilt auch bei Ermittlungen der zuständigen Aufsichtsbehörde in einem Straf- oder Ordnungswidrigkeitenverfahren, das die Verarbeitung personenbezogener Daten aufgrund dieses Vertragsverhältnisses betrifft.
 5. Auftraggeber und Auftragnehmer verpflichten sich zur Zusammenarbeit mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben.
 6. Der Auftragnehmer ist verpflichtet, in regelmäßigen Abständen die internen Prozesse und die technischen und organisatorischen Maßnahmen zu kontrollieren. Dadurch soll gewährleistet werden, dass sich die Verarbeitung stets im Einklang mit dem geltenden Datenschutzrecht befindet und die Rechte der betroffenen Person geschützt sind.
 7. Unterliegt der Auftraggeber einer Kontrolle oder Maßnahme der Aufsichtsbehörde, einem Straf- oder Ordnungswidrigkeitenverfahren, Haftungsansprüchen oder anderen Ansprüchen betroffener oder dritter Personen im Zusammenhang mit der Auftragsverarbeitung im Rahmen dieses Vertragsverhältnisses, ist der Auftraggeber verpflichtet, den Auftragnehmer nach besten Kräften zu unterstützen.
 8. Der Auftragnehmer hat die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber nach dessen Kontrollbefugnissen nach § 8 dieses Vertrags nachzuweisen.

§ 6 Unterauftragsverhältnisse

1. Der Auftragnehmer darf Subunternehmer als weitere Auftragsverarbeiter in einem Unterauftragsverhältnis nur nach vorheriger schriftlicher Information des Auftraggebers einsetzen und nur, soweit der Auftraggeber dem Einsatz des Subunternehmers nicht widersprochen hat. Ein Unterauftragsverhältnis liegt vor, wenn der Auftragnehmer den Dritten mit der vollständigen oder teilweisen Erfüllung dieses Vertrags beauftragt. Erforderlich ist, dass die Tätigkeiten des

Subunternehmers in unmittelbarem Zusammenhang mit der Hauptleistung dieses Vertrags stehen. Nebenleistungen wie der Transport, die Bewachung oder die Reinigung stellen keine Unterauftragsverhältnisse in diesem Sinn dar.

2. Die Auswahl des Subunternehmers ist unter Berücksichtigung der Voraussetzungen des Art. 28 DSGVO und den Standards dieses Vertrags durch den Auftragnehmer zu treffen. Die Eignung des Subunternehmers zur ordnungsgemäßen Datenverarbeitung und zur Einhaltung der technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO ist zu gewährleisten.
3. Der Auftragnehmer stellt sicher, dass dem Subunternehmer im Hinblick auf das Schutzniveau der personenbezogenen Daten solche Verpflichtungen auferlegt werden, die mit den in diesem Vertrag begründeten Anforderungen vergleichbar sind. Der Auftragnehmer hat dem Auftraggeber die Kontaktdaten des Subunternehmers zu übermitteln.
4. Der Auftragnehmer stellt sicher, dass die aus diesem Vertrag oder dem Gesetz folgenden Rechte des Auftraggebers auch im Verhältnis zum Subunternehmer wirksam ausgeübt werden können.
5. Die Kontrolle des Subunternehmers durch den Auftragnehmer gestaltet sich nach den in diesem Vertrag geregelten Grundsätzen zur Kontrolle des Auftragnehmers durch den Auftraggeber. Der Auftragnehmer hat regelmäßige Kontrollen durchzuführen und die Ergebnisse zu dokumentieren und dem Auftraggeber auf Verlangen vorzulegen. Der Nachweis der Kontrollmaßnahmen kann erfolgen durch:
 - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
 - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz)
6. Der Beauftragung folgender Subunternehmer in der nachfolgenden Liste stimmt der Auftraggeber unter Einhaltung der vorstehenden Voraussetzungen zu:

- **Netlify** (VeraSafe Ireland Ltd., Unit 3D North Point House, North Point Business Park, New Mallow Road, Cork T23AT2P, Ireland)

- **All-Inkl** (All-inkl.com - Neue Medien Münnich, Hauptstraße 68, D-02742 Friedersdorf)

- **Cloudflare** (Cloudflare Germany GmbH, Rosental 7, 80331 München)

- **OpenAI** (OpenAI Ireland Limited, at 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland)

- **Algolia** (Algolia SAS, 55 Rue d'Amsterdam, 75008 Paris, France)

- **MongoDB** (MongoDB, Inc., 1633 Broadway, 38th Floor New York, NY 10019.)

- **AWS S3** (Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg)

- **DigitalOcean** (DigitalOcean, 101 6th Ave New York, NY 10013)

- **Starbüro** (MWC - Mobile World Communications GmbH, Kavaliertstraße 9, 13187 Berlin, Deutschland)

- **Render** (Render Services Inc., 525 Brannan Street, Ste 300 San Francisco, CA 94107)

- **MailChimp** (Bird & Bird GDPR Representative Services Ireland, Deloitte House, 29 Earlsfort Terrace, Dublin 2, DO2 AY28)

§ 7 Technisch- organisatorische Maßnahmen (TOMs)

1. Der Auftragnehmer hat bei seinen Verarbeitungstätigkeiten ein Schutzniveau zu gewährleisten, dass eine Gefährdung für die Rechte und Freiheiten der betroffenen Personen ausschließt. Alle Tätigkeiten des Auftragnehmers müssen sich im Einklang mit der des Art. 28 i.V.m. Art. 5 I DSGVO sowie des Art. 32 DSGVO zur Sicherheit der Verarbeitung halten. Dafür verpflichtet sich der Auftragnehmer, die in der Anlage aufgeführten technisch-organisatorischen Maßnahmen, die in seinem Verantwortungsbereich liegen, einzuhalten.
2. Die vereinbarten technisch-organisatorischen Maßnahmen unterliegen der durch den technischen Fortschritt bedingten Weiterentwicklung. Insofern darf der Auftragnehmer in der Zukunft alternative adäquate Maßnahmen ergreifen, wenn damit keine Absenkung des Sicherheitsniveaus der festgelegten Maßnahmen verbunden ist.

§ 8 Kontrollrechte des Auftraggebers

1. Der Auftraggeber kann, die Einhaltung der Vorschriften über den Datenschutz und der Vorgaben dieses Vertrags durch Kontrollen feststellen. Die Kontrollen können auch von Dritten durchgeführt werden, die der Auftraggeber nach seinem Ermessen bestimmt. Der Auftragnehmer hat das Recht, die Kontrolle durch den Dritten bei Vorliegen besonderer Umstände abzulehnen (oder z.B. Bestehen eines Wettbewerbsverhältnisses zwischen Auftragnehmer und Dritten). Der Auftragnehmer ist verpflichtet, den Auftraggeber bei den Kontrollen nach seinen Kräften zu unterstützen, indem er unter anderem die erforderlichen Auskünfte gibt, Einsicht in seine Unterlagen gewährt und Zutritt zu seinen Räumlichkeiten gewährt.
2. Bei Ermöglichung der Kontrollen durch den Auftraggeber wird der Auftragnehmer einen Vergütungsanspruch laut AGB geltend machen.
3. Der Auftraggeber muss die Kontrollen in der Regel in einem angemessenen zeitlichen Abstand ankündigen. Sie sind in einem angemessenen Rahmen und mit Rücksicht auf die Interessen des Auftragnehmers durchzuführen, soweit der Auftragnehmer nicht nach § 6 (5) dieses Vertrages die Kontrollen durch dort genannte Nachweise (durch Kontrollen unabhängiger Dritter) abwendet. Dies schließt ein, dass sie zu den gewöhnlichen Geschäftszeiten des Auftragnehmers stattfinden und den ordentlichen Geschäftsablauf soweit möglich nicht übermäßig stören.

§ 9 Mitteilungs- und Unterstützungspflichten des Auftragnehmers

1. Der Auftragnehmer hat den Auftraggeber im Fall einer vertragswidrigen, gesetzeswidrigen oder anderweitig rechtswidrigen Verarbeitung durch den Auftragnehmer oder durch bei ihm beschäftigte Personen unverzüglich zu informieren. Dies gilt auch, wenn lediglich ein Verdacht einer Datenschutzverletzung besteht, sowie bei festgestellten Unregelmäßigkeiten. Das weitere Vorgehen wird vom Auftraggeber und Auftragnehmer einvernehmlich bestimmt.
2. Der Auftragnehmer hat den Auftraggeber bei der Erfüllung seiner datenschutzrechtlichen Pflichten nach Art. 28 III (f) DSGVO, insbesondere bei der Erfüllung nach den Art. 32-36 DSGVO zu unterstützen.

§ 10 Weisungsbefugnisse des Auftraggebers

1. Der Auftraggeber hat im Hinblick auf die durchzuführenden Verarbeitungstätigkeiten ein umfassendes Weisungsrecht. Die Erteilung einer Weisung ist vom Auftragnehmer unverzüglich zu bestätigen.
2. Ausschließlich die folgenden Personen sind zur Erteilung und zur Annahme von Weisungen befugt. Ein Wechsel der Personen ist der jeweils anderen Vertragspartei unverzüglich mitzuteilen.

Erteilung von Weisungen:

Der Auftraggeber oder von ihm ernannte Personen

Annahme von Weisungen:

Geschäftsführung der Faktor Mensch MEDIA UG (haftungsbeschränkt) und durch diese beauftragte Personen.

3. Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen Datenschutzvorschriften oder Vorschriften dieses Vertrags verstößt, hat er den Auftraggeber unverzüglich darüber zu informieren. Er darf die Durchführung der Weisung so lange unterlassen, wie der Auftraggeber sie nicht bestätigt, geändert oder widerrufen hat. Mündliche Weisungen sind ausgeschlossen.

§ 11 Verpflichtungen nach Beendigung des Auftragsverhältnisses

1. Die Verpflichtungen ergeben sich aus dem Hauptvertrag und ggf. dem Gesetz. Nach Vertragsbeendigung im Besitz des Auftragnehmers befindliche Daten sind nach Wahl des Auftraggebers an diesen zurückzugeben oder zu vernichten. Der Auftraggeber kann den Auftragnehmer zur Wahl auffordern. Die Vernichtung hat in einer mit der DSGVO konformen Weise zu erfolgen, die die Wiederherstellung der Daten ausschließt. Die ordnungsgemäße Vernichtung ist vom Auftragnehmer nachzuweisen.
2. Selbige Anforderungen gelten auch im Verhältnis des Auftragnehmers zu seinen Subunternehmern.

3. Der Auftragnehmer ist verpflichtet, alle Dokumentationen, die dem Beleg der Rechtmäßigkeit der Vereinbarung dienen, nach dem Vertragsende für die Dauer von 12 Monaten aufzubewahren. Wahlweise kann er sie dem Auftraggeber übergeben.

§ 12 Telearbeit beim Auftragnehmer

1. Der Auftragnehmer ist berechtigt, seinen Beschäftigten Telearbeit anzubieten. Er schließt mit ihnen eine betriebliche Vereinbarung über die Telearbeit, die die Einhaltung aller Vorschriften zum Datenschutz und zur Datensicherheit sicherstellt.
2. Eine Gefährdung der Daten muss ausgeschlossen sein. Die Sicherheit der Daten ist insbesondere durch einen sicheren Dienstrechner und das Einrichten einer verschlüsselten Verbindung zu gewährleisten.

§ 13 Betroffenenrechte

1. Macht eine betroffene Person Rechte gegenüber dem Auftragnehmer geltend, hat dieser die Person unverzüglich an den Auftraggeber zu verweisen und den Antrag an diesen weiterzuleiten. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von Ansprüchen betroffener Personen in angemessenem Umfang (Art. 28 III lit. e, f DSGVO).
2. Der Auftragnehmer verpflichtet sich, Weisungen des Auftraggebers Folge zu leisten, die den Inhalt haben, Daten aus dem Auftragsverhältnis zu löschen, zu berichtigen oder deren Verarbeitung einzuschränken. Dies gilt nicht, wenn berechtigte Interessen des Auftragnehmers entgegenstehen.
3. Auskünfte über personenbezogene Daten darf der Auftragnehmer nicht ohne vorherige Zustimmung oder Weisung des Auftraggebers an Dritte erteilen.
4. Als Rechte des Betroffenen gemäß dieses Abschnitts kommen die folgenden in Betracht:
 - Art. 7 III, 8 DSGVO bzw. § 7 UWG und/oder § 203 StGB: Widerruflichkeit der Einwilligung
 - Art. 15 DSGVO: Recht auf Auskunft über die verarbeiteten personenbezogenen Daten
 - Art. 16 DSGVO: Recht auf Vervollständigung bzw. Berichtigung der verarbeiteten personenbezogenen Daten
 - Art. 17 DSGVO: Recht auf Löschung der verarbeiteten personenbezogenen Daten (Recht auf Vergessenwerden)
 - Art. 18 DSGVO: Verlangen auf Einschränkung der Verarbeitung personenbezogener Daten
 - Art. 20 DSGVO: Recht auf Datenportabilität
 - Art. 77 DSGVO: Recht auf Beschwerde bei einer Aufsichtsbehörde
 - § 8 UWG: Anspruch auf Beseitigung und Unterlassung
 - Art. 34 DSGVO: Recht auf Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten
 - Art. 13, 14 DSGVO: Recht auf Information über die Erhebung personenbezogener Daten, die bei der betroffenen Person und nicht bei der betroffenen Person erhoben werden
 - Art. 19 DSGVO: Recht auf Mitteilung im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
 - Art. 38 IV DSGVO: Recht auf Konsultation des Datenschutzbeauftragten
 - § 41 BDSG: Recht auf Konsultation der zuständigen Staatsanwaltschaft
 - Art. 82 DSGVO bzw. §§ 280 ff., 823 ff. BGB: Anspruch auf Schadensersatz bei Rechtsverletzung in Bezug auf personenbezogene Daten
 - Art. 22: Recht, nicht ausschließlich automatisierten Entscheidungen unterworfen zu werden, das für eine rechtliche oder in ähnlicher Weise erhebliche Beeinträchtigung sorgt
 - Art. 12: Recht auf Information über die Rechte nach Art. 13-22, 34 in transparenter Weise

§ 14 Sonstiges

1. Wenn Daten des Auftraggebers oder seines Kunden beim Auftragnehmer oder Subauftragnehmer durch Beschlagnahme oder Pfändung, durch ein Insolvenz- oder Vergleichsverfahren oder sonstige Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich hierzu

zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich hierzu informieren, dass die Hoheit an den Daten beim Auftraggeber vorliegt.

2. Die Vertragspartner behandeln alle im Rahmen dieses Vertragsverhältnisses erlangten Kenntnisse vertraulich, auch nach Beendigung des Vertragsverhältnisses.
3. Nebenabreden müssen in schriftlicher oder elektronisch dokumentierter Form (z.B. E-Mail) unter Bezugnahme auf diesen Vertrag getroffen werden. Dasselbe gilt für Änderungen und Ergänzungen dieses Vertrags. Diese müssen die geänderte Regelung ausdrücklich bezeichnen.
4. Der Auftragnehmer hat kein Zurückbehaltungsrecht im Hinblick auf die Daten des Auftraggebers und die zugehörigen Datenträger.
5. Sind einzelne Bestandteile dieses Vertrags unwirksam, berührt dies die Wirksamkeit des Vertrags im Übrigen nicht. Bei Vorliegen einer unwirksamen Regelung oder einer Lücke sind diese durch die Regelung zu ersetzen, die die Parteien in Kenntnis der Unwirksamkeit oder der Lücke vereinbart hätten und die der fehlerhaften Regelung möglichst nahekommen.
6. Der Gerichtsstand ist Stuttgart.
7. Es gilt deutsches Recht.

Dieser Vertrag gilt ohne Unterschriften der Parteien als Bestandteil der AGB des Auftragnehmers.

Anlage 1: Technische und organisatorische Maßnahmen des Auftragnehmers nach Art. 5, 24, 25, 28, 32 DSGVO

Informationen zum Standort von Datenverarbeitungsanlagen und Rechenzentren:

Der Standort des Rechenzentrums des Auftragnehmers (hauptsächlich Hosting und E-Mail-Server) liegt bei ALL-INKL.COM - Neue Medien Münnich, Inhaber: René Münnich, Hauptstraße 68, 02742 Friedersdorf sowie bei Render (Render Services Inc., 525 Brannan Street, Ste 300 San Francisco, CA 94107).

1. Grundsätze für die Datenverarbeitung (Art. 5 DSGVO)

Transparenzgrundsatz nach Art. 5 Abs. 1 lit. a DSGVO, Maßnahmen:

- Erstellung von Datenschutzdokumentationen
- Informationen zum Datenschutz können leicht zugänglich und verständlich von Betroffenen abgerufen werden
- Siehe auch unter „1. Rechenschafts- & Wirksamkeitsnachweise“
- Siehe auch unter „2. Pflichten des Verantwortlichen“

Zweckbindungsgrundsatz nach Art. 5 Abs. 1 lit. b DSGVO, Maßnahmen:

- Darstellung der Verarbeitungszecke im Verzeichnis der Verarbeitungstätigkeiten
- ausschließlich schriftliche (bzw. in Textform E-Mail) Weisungen in Auftragsverarbeitung
- Erlass von Dienstanweisungen insbesondere zu Telearbeit
- Mitarbeiterverpflichtung zur Verschwiegenheit

Datenminimierungsgrundsatz nach Art. 5 Abs. 1 lit. c DSGVO, Maßnahmen:

- Umsetzung des Löschkonzepts manuell
- Siehe ausführlich unter „7. datenschutzfreundliche Systemgestaltung“

Richtigkeitsgrundsatz nach Art. 5 Abs. 1 lit. d DSGVO, Maßnahmen:

- Einsatz von Identifikationsverfahren
- Unverzögliche Korrektur- & Lösungsverfahren unrichtiger Daten
- Siehe ausführlich unter „3. Vertraulichkeit“

Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO, Maßnahmen:

- Anonymisierte bzw. pseudonyme Auswertung von Nutzerstatistiken
- Umsetzung des Löschkonzepts

Vertraulichkeitsgrundsatz nach Art. 5 Abs. 1 lit. f DSGVO, Maßnahmen:

- Siehe unter 3. ausführlich, insbesondere Umsetzung der ErwGr 39 und 83 zur DSGVO

Integritätsgrundsatz nach Art. 5 Abs. 1 lit. f DSGVO, Maßnahmen:

- Siehe unter 4. und 5. ausführlich

Rechenschaft- & Wirksamkeitsnachweise Art. 5 Abs. 1 lit. f DSGVO, Maßnahmen:

2. Pflichten des Verantwortlichen (Art. 12, 24 DSGVO) Maßnahmen:

- Dokumentation der Pflichten nach Art. 13 bis 34 DSGVO (insbesondere in der Datenschutzerklärung)
- Siehe oben 1. insbesondere Rechenschafts- & Wirksamkeitsnachweise

3. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO):

Zutrittskontrolle - Es findet eine Zutrittskontrolle (kein Betreten der Datenverarbeitungsanlagen durch Unbefugte) statt. Dies umfasst die folgenden Maßnahmen:

- Manuelles Schließsystem

Zugangskontrolle - Verweigerung der Systembenutzung für Unbefugte. Es findet eine Zugangskontrolle (keine Systembenutzung durch Unbefugte) statt. Dies umfasst die folgenden Maßnahmen:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit biometrischen Verfahren
- Authentifikation mit Benutzername / Passwort
- Einsatz von VPN-Technologie

Trennungs- bzw. Verwendungszweckkontrolle - Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden). Maßnahmen:

- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

Verschlüsselung Art. 32 Abs. 1 lit. a DSGVO:

- Angebot zum E-Mail-Verkehr mit PGP-Verschlüsselung
- Websiteangebote nur mit SSL/TLS-Verschlüsselung
- E-Mail-Verkehr (IMAP/SMTP) nur mit SSL/TLS-Verschlüsselung
- Datenaustausch verschlüsselt zwischen Büro und Rechenzentren wie FTPS

4. Belastbarkeit und Verfügbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Wiederherstellbarkeit - Zügige Zurückgewinnung von Originaldaten nach einem Datenverlust (nach Verlust durch Störfall werden Daten zurückgewonnen) auf einem Datenträger ggf. auch die Erkennung fehlerhaft übertragener Dateneinheiten.

- IT-Dienstleister auf Abruf verfügbar

5. Technische und organisatorische Umsetzung des Rechts auf Löschung, "Recht auf Vergessenwerden" (Art. 17 DSGVO)

Zur Umsetzung des Rechts auf Löschung (sichere möglichst nicht wiederherstellbare Beseitigung von Daten) wurden folgende Maßnahmen getroffen:

- Einfache Datenlöschung (ohne Überschreiben)

6. Auftragskontrolle (Art. 28 DSGVO)

- Verpflichtung der Mitarbeitenden des Auftragnehmers auf das Datengeheimnis