Vereinbarung zur Auftragsverarbeitung

DIE VERTRAGSPARTEIEN

NY digital, Nicole Y. Jodeleit		Lots of Ways GmbH
Unternehmensbezeichnung, Firma		Unternehmensbezeichnung, Firma
Mühlweg 12		Mühlweg 12
Straße, Hausnummer		Straße, Hausnummer
72414 Rangendingen		72414 Rangendingen, Deutschland
PLZ, Stadt		PLZ, Stadt
- im Folgenden: Auftraggeber -		- im Folgenden: Auftragsverarbeiter *oder* Auftragnehmer -

SCHLIEßEN FOLGENDEN VERTRAG:

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind Anlage 1 zu entnehmen.

1.2 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.

1.3 Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.

1.4 Die Vergütung wird außerhalb dieses Vertrags vereinbart.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

3.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.4 Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3 Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragsverarbeiters

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2 Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.

5.3 Sofern der Auftragsverarbeiter nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

5.4 Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice des Auftragsverarbeiters) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

5.5 Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

5.6 Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.

6.2 Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

7. Unterstützungspflichten des Auftragsverarbeiters

7.1 Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

7.2 Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragsverarbeiters sind diesem Vertrag abschließend in Anlage 2 beigefügt. Für die in Anlage 2 aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden.

8.2 Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen.

Der Auftragsverarbeiter wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

8.3 Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können. Der Auftragsverarbeiter ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragsverarbeiters einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.

8.4 Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. dem Subunternehmer zur Ausübung der gleichen Kontrollrechte, wie ggü. dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.

8.5 Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO ggü. den ihm unterstellten Personen erfüllt hat.

8.6 Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.

8.7 Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.

8.8 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragsverarbeiters

9.1 Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9.2 Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.

9.3 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

9.4 Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

11. Datengeheimnis und Vertraulichkeit

11.1 Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B.
203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.

11.2 Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.
11.3 Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

Rangendingen, 1.6.2018

Ort, Datum

Nicole Y. Jodeleit
NY digital

Name, Funktion,
Unterschrift Auftraggeber

Rangendingen, 03.06.2018

Ort, Datum

Bernhard Jodeleit,
Geschäftsführender Gesellschafter,
Lots of Ways GmbH

Name, Funktion,
Unterschrift Auftragsverarbeiter

Anlage 1 – Auftragsdetails

Der vorliegende Vertrag umfasst (ggf. Im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

Gegenstand der Vertrages ist die Bereitstellung von Webhosting-Dienstleistungen bzw. eines oder mehrerer Webhosting-Pakete sowie der damit in Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung etc. Im Rahmen des Hauptvertrages hat der Auftraggeber, je nach Tarif, Zugang zur Nutzung eines Webhosting-Pakets für Websites sowie auf FTP-Zugänge und Zugänge zum Webhosting Management Panel (Parallels Plesk), mit dem alle Webhosting-Funktionen verwaltet und gesteuert werden können. Der Kunde konfiguriert und überwacht seine Webhosting-Pakete in der Regel selbst, hat jedoch die Möglichkeit, im Rahmen weiterer erteilter Aufträge den Auftragsdatenverarbeiter mit der Pflege, Weiterentwicklung und ggf. der technischen Optimierung seiner Webhosting-Pakete zu betrauen.

Gegenstand des Vertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragsdatenverarbeiter. Regelmäßig kommt der Auftragsdatenverarbeiter lediglich mit Verkehrsdaten wie IP-Adressen der Website-Besucher des Auftraggebers in Kontakt.

Sofern der Auftraggeber innerhalb seiner Webhosting-Pakete personenbezogene Daten darüber hinaus speichert, insbesondere Namen, E-Mail-Adressen und weitere persönliche Daten, obliegt ihm die Verantwortung für diese Daten selbst. Der Auftragnehmer wird mit diesen Daten nur im Rahmen von Routineaufgaben (wie Backup und Speicherung in der verschlüsselten Backup Cloud) in Berührung kommen.

Aktiv arbeiten wird der Auftragnehmer mit solchen Daten nur auf gesonderte Weisung des Auftraggebers.

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

[Hier muss eine detaillierte Aufstellung der verarbeiteten Datenarten erfolgen (z.B.: Daten von Bürgern, Name, Vorname, Anschrift Geburtsdatum, Beruf, etc.)]

Von Besuchern der Websites, die der Auftraggeber beim Auftragnehmer speichern und betreiben lässt:

- Browsertyp und Browserversion
- verwendetes Betriebssystem
- Referrer URL (die Herkunft, falls von einer anderen Website per Verweis eingehend)
- Hostname des zugreifenden Rechners
- Uhrzeit der Serveranfrage
- IP-Adresse
- aufgerufene Seiten (URLs)
- weitere Daten, die Website-Besucher aktiv zum Server schicken, zum Beispiel durch Eingaben in vom Auftraggeber online gestellte Formulare

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

- Interessenten
- Kunden
- Mitarbeiter
- allgemein darüber hinaus:
  jegliche Personen, die Websites des Auftraggebers besuchen oder andere vom Auftragnehmer bereitgestellte Kommunikationsdienste nutzen, etwa E-Mail-Dienste, die der Auftraggeber dem Auftragnehmer zur Verfügung stellt

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:

- Abruf von Websites des Auftraggebers durch Dritte
- Senden und Empfangen von E-Mails über vom Auftragnehmer bereitgestellte E-Mail-Serverfunktionen

Der Auftraggeber unterliegt folgenden besonderen Geheimnisschutzregeln, die auch vom Auftragsverarbeiter zu beachten sind:

- keine

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

I. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern, nur dann, wenn dies zwischen Auftragnehmer und Auftraggeber explizit schriftlich vereinbart wurde
- regelmäßig logische Mandantentrennung (softwareseitig)
- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen, Datenfeldern oder Signaturen
- bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System
- Trennung von Produktiv- und Testsystem

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

1. **Zutrittskontrolle**

   In den Räumen des Auftragsdatenverarbeiters befinden sich keine Server-Anlagen, die personenbezogene Daten verarbeiten, jedoch Endgeräte, mit denen auf solche Server bei den beauftragten Subunternehmern zugegriffen werden kann.

   Daher wird durch folgende Maßnahmen sichergestellt, dass Unbefugte keinen Zugriff auf diese Endgeräte, die zum Zugriff auf Server verwendet werden, Zutritt haben:

   - Personenkontrolle beim Einlass
   - sorgfältige Auswahl von Reinigungs- und sonstigem Personal

- keine unbeaufsichtigen Arbeiten in den relevanten Büroräumen durch Dritte
- Zutritt zu den Räumen mit Endgeräten ausschließlich in Anwesenheit der Geschäftsführung
- manuelles Schließsystem
- Videoüberwachung der Zugänge
- Schlüsselregelung

2. **Zugangskontrolle**

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Passwort-Richtlinien (Komplexität)
- Authentifikation mit Benutzername / Passwort
- automatische Sperrung der Endgeräte nach maximal fünf Minuten Inaktivität
- Zwei-Faktor-Authentifizierung beim Zugriff auf Serversysteme mit personenbezogenen Daten
- Verschlüsselung der Daten auf Serversystemen mit personenbezogenen Daten
- Verwendung unterschiedlicher, sicherer Kennwörter für alle IT-Systeme
- Verschlüsselung sowie Kennwort- und biometrische Sicherung für tragbare IT-Geräte
- VPN-Tunnel beim Zugang über öffentliche WLAN-Hotspots beim Zugriff auf IT-Systeme
- verschlüsselte Speicherung aller Kennwörter
- Verbot des unverschlüsselten Vorhandenseins von Kennwörtern und Zugangsdaten, sowohl auf IT-Systemen als auch in Form jeglicher Form von Notizen auf Papier oder Gegenständen
- Einsatz von Intrusion-Detection-Systemen
- Einsatz mehrstufiger forensischer Firewalls auf Servern
- Einsatz mehrstufiger forensischer Firewalls als Web Application Firewall
- Datensparsamkeit bei und Verschlüsselung für mobile Datenträger
- Verschlüsselung der Datensicherungssysteme
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Verbot der Speicherung personenbezogener Daten auf externen Datenträgern
- ordnungsgemäße Vernichtung von Datenträgern (sowohl digital als auch Papier)

3. **Verschlüsselung**

- für eigene Daten und Kundendaten wie Dateien und E-Mails, die im Rahmen der Auftragsabwicklung anfallen: ausschließliche Speicherung in der Cloud mit Verschlüsselung nach mindestens AES-128

4. **Pseudonymisierung**

„Pseudonymisierung" bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

Die Pseudonymisierung erfolgt in folgender Art und Weise:

- keine Zusammenführung von IP-Adressen mit anderen Datenquellen

- Kürzung = Pseudonymisierung von IP-Adressen bei Speicherung durch die Sub-Auftragsdaten-verarbeiter, die dies im Rahmen entsprechender Verträge zusichern

Zusammenfassend: Es wurden umfassende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).
Das Berechtigungskonzept wird durch die Geschäftsführung persönlich verwaltet. Es erfolgt eine regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.). Die Anzahl der Administratoren ist das Notwendigste reduziert.

Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**):

- Protokollierung der Eingabe, Änderung und Löschung von Daten (GSuite Cloud, DPA vorhanden)
- revisionssichere Speicherung von E-Mails und Cloud-Inhalten (GSuite Cloud, DPA vorhanden)
- mehrstufiges Backupkonzept mit geographisch getrennten Speicherorten und täglicher Versionierung (GSuite Cloud, DPA vorhanden)
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche personenbezogenen Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts:

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**).

- Auswahl der Auftragsverarbeiter (Stand zum Zeitpunkt des Vertragsabschlusses siehe Anlage) unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit und Abschluss eines ADV bzw. DPA)
- vorherige Prüfung der und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag), insofern immanent Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis; insofern immanent: Auftragsverarbeiter hat Datenschutzbeauftragten bestellt
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können (Transport- bzw. Weitergabekontrolle):

- Einsatz von VPN-Tunneln

- Einsatz verschlüsselter E-Mail-Kommunikation (Open PGP)
- Verschlüsselung physischer Datenträger bei Transport

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- mehrstufiges Backupkonzept mit geographisch getrennten Speicherorten und täglicher Versionierung (GSuite Cloud, DPA vorhanden)
- Abschluss von ADV und DPA mit führenden Cloud-Anbietern, die sorgfältig ausgewählt wurden und die branchenüblichen Sicherheitsstandards vorweisen. Dazu gehören die regelmäßig an dieser Stelle zu erwartenden Maßnahmen - hier wird auf die ADV und DPA mit den Sub-Auftragsdaten verwiesen - wie, hier beispielhaft aufgeführt, regelmäßig

    - unterbrechungsfreie Stromversorgung (USV)
    - Klimatisierung der Serverräume
    - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
    - Überspannnungsschutz
    - Feuer- und Rauchmeldeanlagen in Serverräumen Feuerlöschgeräte in Serverräumen
    - Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
    - Erstellen eines Backup- & Recoverykonzepts
    - Testen von Datenwiederherstellung
    - Erstellen eines Notfallplans
    - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort Serverräume nicht unter sanitären Anlagen
    - in Hochwassergebieten: Serverräume über der Wassergrenze
    - belastbares Datensicherungs- und Wiederherstellungskonzept

IV. Besondere Datenschutzmaßnahmen

- restriktives Zugangskonzept
- Verarbeitungsverzeichnis im internen Wissensmanagement-System auf Wiki-Basis, versioniert
- Verbot unverschlüsselter Speicherung personenbezogener Daten im Unternehmen des Auftragnehmers
- mehrstufiges Firewall-Konzept in Absprache mit dem Auftraggeber
- Intrusion Detection sowohl in der Server-Architektur als auch auf lokalen Arbeitsgeräten

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten sowie anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen. Die Maßnahmen werden aufgrund der hohen Dynamik von Sicherheitsrisiken in der IT- und Internet-Landschaft laufend weiterentwickelt.

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Unternehmens-) Name und Anschrift	**Beschreibung der Leistung**	**Ort der Leistungs- erbringung**
Amazon Web Services Inc., 410 Terry Avenue North, Seattle WA, 98109, USA	Bereitstellung von Serverkapazität sowie SMTP Gateways und Serverless Applications, Abwicklung von Domain-Registrierungen und Erbringung von Dienstleistungen im Bereich des Domain Name Management (DNS)	Region EU (Irland, Frankfurt)
Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA	Bereitstellung eines Content Delivery Networks zur gegen Hackerangriffe geschützten udn auf Geschwindigkeit optimierten Auslieferung von Websites, Abwicklung von Domain-Registrierungen und Erbringung von Dienstleistungen im Bereich des Domain Name Management (DNS)	San Francisco, CA 94107, USA, sowie weltweit
Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Bereitstellung von Speicher- und Kommunikationsdiensten, Web Analytics, Karten- und Navigationsmaterial sowie Skripten und weiteren digitalen Assets für Websites, Abwicklung von Domain-Registrierungen und Erbringung von Dienstleistungen im Bereich des Domain Name Management (DNS)	Mountain View, CA 94043, USA, sowie weltweit
Host Europe GmbH, Hansestr. 111, 51149 Köln, DE	Bereitstellung von Speicher- und Serverkapazität für das Hosting von Kundenwebsites und eigenen	Köln, DE, Standort des Rechenzentrums ist Straßburg, FR

	Anwendungen des Auftrags-Datenverarbeiters, Abwicklung von Domain-Registrierungen	
Internetx GmbH, Johanna-Dachs-Str. 55, 93055 Regensburg, DE	Bereitstellung von Speicher- und Serverkapazität für das Hosting von Kundenwebsites und eigenen Anwendungen des Auftrags-Datenverarbeiters, Abwicklung von Domain-Registrierungen	Regensburg, DE
Jodeleit, Nicole, NY digital, Mühlweg 12, 72414 Rangendingen, DE	Programmierung und Pflege von Websites im Kundenauftrag als Subunternehmerin, Pflege und Administration von IT-Systemen	Rangendingen, DE
Sucuri, Inc., 30141 Antelope Rd, Menifee, CA 92584, USA	Bereitstellung eines Content Delivery Networks zur gegen Hackerangriffe geschützten udn auf Geschwindigkeit optimierten Auslieferung von Websites, Abwicklung von Domain-Registrierungen und Erbringung von Dienstleistungen im Bereich des Domain Name Management (DNS)	Menifee, CA 92584, USA, sowie weltweit