Vereinbarung zur Auftragsverarbeitung

Zwischen

dem Auftragsverarbeiter (Anbieter)
Protectweb IT-Sicherheit
Ajuan Kamran Hassan
Eichkamp 22
24217 Schönberg

und

dem Verantwortlichen
bei Klick auf "Jetzt registrieren"

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 Verarbeitung 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 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, Auftraggebers. 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 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 dass sich die zur Verarbeitung 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 3 beigefügt. Für die in Anlage 3 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.

Anlage 1 – Auftragsdetails

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

- Informationen werden registriert und in der Datenbank gespeichert
- Öffentliches Profil wird erstellt (Safetycheck-Seite) mit individueller URL
- Die Adressdaten des Betriebs werden auf dem öffentlichen Profil angezeigt
- Die Postleitzahl wird genutzt, um das Bundesland herauszufiltern
- Nach erfolgreicher verifizierung der Domain erfolgen automatisierte Sicherheitsüberprüfungen (sog. Penetrationstests).

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

- Logo (Bilddatei)
- Branche
- Betriebsname
- Kontakt- und Identifikationsdaten einschließlich E-Mail-Adressen
- IP-Adresse
- Benutzername
- Vor- & Nachname
- Email
- Rufnummer
- Faxnummer
- USt-IdNr. und HR-Nr.
- Adresse
- Datum/Uhrzeit

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

- Registrierte Nutzer von Protectweb

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:

- Mit einem Datenverarbeitungssystem

Die Löschung auf die betroffenen Daten geschieht in folgender Weise:

- Nach erfolgtem Kontakt mit dem Support, der die erforderlichen Schritte zur Datenlöschung einleitet.

Anlage 2 - Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO

Die Wirksamkeit der TOM von Protectweb wird regelmäßig überprüft. Protectweb setzt die Alfahosting GmbH als Subunternehmen ein. Konkret betreibt die Alfahosting GmbH das Backend (Datenebene) der Anwendung in ihrem Rechenzentrum.

Technische und organisatorische Maßnahmen von Protectweb

1. Vertraulichkeit

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden:

Hier sind die TOMs des Subunternehmers Alfahosting GmbH einschlägig.

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Login mit E-Mail und Passwort
- Erzwungene Passwortkomplexität (min. 8 Zeichen, 1 Großbuchstabe, 1 Kleinbuchtsabe & 1 Ziffer)

Unser Subunternehmer Alfahosting GmbH ergreift in diesem Bereich weitere TOM.

1.3. Zugriffskontrolle

Maßnahmen, 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:

- Regelmäßige Aktualisierung der Sicherheitskonzepte
- Vergabe differenzierter Berechtigungsstufen innerhalb der Verfahren
- Protokollierung von Veränderungen oder Löschungen der Daten
- Datenträgervernichtung gemäß DIN 66399

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Festlegung von Datenbankrechten
- Steuerung über Berechtigungskonzept

Unser Subunternehmer Alfahosting GmbH ergreift in diesem Bereich weitere TOM.

1.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System
- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe (z.B Gesundheitsamt) oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu pseudonymisieren

2. Integrität

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Datenübermittlung über gesicherte Datenverbindungen (SSL)

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Keine Modifizierbarkeit der Protokolle
- Kontrolle der Protokolle

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Hier sind die TOMs des Subunternehmers Alfahosting GmbH einschlägig.

Technisch-organisatorische Maßnahmen der Alfahosting GmbH nach Art. 32 DSGVO

Präambel

Die Alfahosting GmbH vermietet die Datenverarbeitungsanlage an den Auftraggeber. Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung. Der Auftraggeber entscheidet allein und ausschließlich darüber, welche personenbezogene Daten in welcher Weise verarbeitet werden. Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Auftraggeber erstellt und eingesetzt. Die Alfahosting GmbH sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Buch darüber, welche Anlagen durch den Auftraggeber in welchem Umfang genutzt werden. Die Datenverarbeitung erfolgt durch den Auftraggeber. Die Alfahosting GmbH hat keinerlei Einfluss auf die durch den Auftraggeber durchgeführten Datenverarbeitungsvorgänge.

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

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen in den Rechenzentren

  1. *Zutrittskontrollsystem*

     Ein Schließsystem in Form einer mindestens 1-Faktor-Authentifizierung (z.B. Transponder, Chipkarte, Klingelsystem mit Personenkontrolle per Bild und Ton) ermöglicht den Zutritt zu Datenverarbeitungsanlagen erst nach positiver Zutrittsprüfung.
  2. *Schlüsselregelung*

     Schlüsselausgaben an Personen zum Zutritt zu Datenverarbeitungsanlagen werden dokumentiert.
  3. *Protokollierung der Besucher*

     Besucher, die Zutritt zu Datenverarbeitungsanlagen erhalten (z.B. im Falle von Hardware-Austausch durch den Hersteller) werden in einem Besucherbuch erfasst.
  4. *Einbruchmeldeanlage*

     Der Zutritt zu Datenverarbeitungsanlagen ist per Einbruchmeldeanlage abgesichert.
  5. *Videoüberwachung*

     Datenverarbeitungsanlagen werden per Videoüberwachung gesichert.

- Zugangskontrolle
  Keine unbefugte Systembenutzung

  1. *Passwortvergabe*

     Ein Zugang zu den Datenverarbeitungssystemen ist grundsätzlich nur mittels einer Kombination aus einem Benutzernamen und dem zugeordneten Passwort möglich.
  2. *Passwortrichtlinie*

     Passwörter für Datenverarbeitungsanlagen müssen Mindest-Komplexitätsanforderungen der unternehmensweiten Richtlinie entsprechen; Passwörter von Mitarbeitern müssen regelmäßig geändert werden.
  3. *Administrativer Zugriff*

Sämtliche Datenverarbeitungssysteme sind zu Wartungszwecken ausschließlich über freigegebene IP-Adressbereiche und verschlüsselt erreichbar (z.B. VPN-Beschränkungen).

4. *Firewall*

   Schutz der Infrastruktur durch Firewalls (Soft- und/oder Hardware), Beschränkungen ungenutzter Ports sowie Benutzername und Passwort vor unberechtigten Zugriffen geschützt. Systeme, die Hauptvertragsleistungen bereitstellen, werden, entsprechend der jeweiligen Vereinbarung im Hauptvertrag, mit einer Firewall ausgestattet.

5. *Einsatz von Anti-Viren-Software*

   Systeme, die zum Zugriff auf Datenverarbeitungssysteme genutzt werden, sind mit einer Anti-Viren-Software ausgestattet. Diese Software wird regelmäßig auf die neuesten Virus-Definitionen aktualisiert. Systeme, die Kundenleistungen bereitstellen, werden, entsprechend der jeweiligen Vereinbarung im Hauptvertrag, mit einer Anti-Viren-Software ausgestattet.

6. *Verschlüsselung von mobilen Datenträgern*

   Sofern mobile Datenträger oder mobile Geräte zum Einsatz kommen, werden die Inhalte verschlüsselt.

- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

  1. *Zuordnung von Benutzerrechten*

     Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt. Die Datenverarbeitung selbst erfolgt durch den Kunden Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

  2. *Sichere Aufbewahrung von Datenträgern*

     Datenträger, die personenbezogene Daten enthalten, werden verschlossen gelagert

  3. *Verwaltung der Rechte durch einen eingeschränkten Personenkreis*

     Ausschließlich berechtigte Systemadministratoren sind in der Lage, Rechte anderer Personen zu Datenverarbeitungssystem zu verwalten. Der Kreis der berechtigten Systemadministratoren wird auf die kleinstmögliche Auswahl von Personen reduziert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

  4. *Protokollierung der Zugriffe*

     Zugriffe auf Dienste (z. B. Webdienste) werden DSGVO-konform in Log-Files protokolliert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat jedoch keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

  5. *Ordnungsgemäße Vernichtung von Datenträgern*

     Datenträger, die personenbezogene Daten enthalten werden gemäß DIN 66399 vernichtet.

  6. *Regelmäßige Wartung der Datenverarbeitungssysteme*

- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

  1. *Festlegung von Datenbankrechten*

     Der Zugriff von Systemen und Benutzern auf Datenbanken wird auf die jeweils notwendigen Daten eingeschränkt.

2. *Trennung von Produktiv- und Testsystemen*

   Produktiv- und Testumgebungen werden isoliert voneinander betrieben. Ein Zugriff einer Umgebung auf Daten der jeweils anderen Umgebung wird durch den Einsatz von z.B. getrennten Datenbanksystemen und Serversystemen unterbunden.

3. *Logische Mandantentrennung*

   Durch den Einsatz unterschiedlicher softwareseitiger Mechanismen wird eine Trennung der Daten von Mandanten gewährleistet.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

  1. *Transport*

     Sofern personenbezogene Daten weitergegeben werden, findet dies grundsätzlich verschlüsselt statt. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

  1. *Zuordnung von Benutzerrechten*

     Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt.

  2. *Protokollierung von Dateneingaben*

     Die Datenverarbeitung erfolgt durch den Kunden, Seitens des Auftragnehmers besteht kein Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme. Die Eingabekontrolle der Daten kann daher ausschließlich durch den Kunden umgesetzt werden.

  3. *Nachvollziehbarkeit der Eingabe*

     Die Datenverarbeitung erfolgt durch den Kunden. Seitens des Auftragnehmers besteht kein Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme. Die Eingabekontrolle kann daher ausschließlich durch den Kunden umgesetzt werden. Bei Änderungen durch den Auftragnehmer werden die Administrationszugriffe adäquat protokolliert.

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

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

  1. *Unterbrechungsfreie Stromversorgung in Serverräumen (Rechenzentren)*

     Serverräume sind durch unterbrechungsfreie Stromversorgungen geschützt. Der Schutz ist zweistufig aufgebaut. Bei Bedarf wird ein Notstrom-Aggregat automatisch aktiviert, das die Stromversorgung der Serverräume übernimmt.

  2. *Klimaanlagen in Serverräumen (Rechenzentren)*

Eine für den Betrieb von Serversystemen angemessene Temperatur und Luftfeuchtigkeit wird in Serverräumen durch ausreichend dimensionierte Klimaanlagen gewährleistet.

3. *Feuer- und Rauchmeldeanlagen in Serverräumen (Rechenzentren)*

   Durch den Einsatz von Feuer- und Rauchmeldeanlagen wird ein Brand frühzeitig erkannt. Feuerlöschanlagen löschen auftretende Brände.

4. *Datensicherungskonzept und Aufbewahrung von Datensicherungen*

   Datensicherungen von personenbezogenen Daten werden nur nach Vereinbarung bzw. gemäß des abgeschlossenen Hauptvertrages angefertigt und auf separaten und für Datensicherungen dediziert eingesetzten Systemen aufbewahrt.

5. *Monitoring*

   Systemkritische Instanzen werden durch Monitoring überwacht. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management
  Der Auftragnehmer etabliert ein Datenschutzmanagement, das den Schutz der personenbezogenen Daten sicherstellt.

- Incident-Response-Management
  Regelmäßige Überprüfung der IT-Infrastruktur. Der Auftragnehmer etabliert einen Vorfallreaktionsplan.

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
  Der Auftragnehmer stellt innerhalb seiner Möglichkeiten sicher, dass durch Voreinstellung nur Daten, die für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind, verarbeitet werden. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

- Auftragskontrolle
  Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers

  1. *Auswahl von geeigneten Auftragnehmern*

     Bei der Auswahl von Auftragnehmern, die personenbezogene Daten im Auftrag verarbeiten, werden nur solche Auftragnehmer ausgewählt, die mindestens die gesetzlich vorgeschriebenen Anforderungen an die Verarbeitung von personenbezogenen Daten einhalten

  2. *Überwachung der Auftragnehmer*

     Der Auftragnehmer wird regelmäßig auf die Einhaltung der zugesicherten technischen und organisatorischen Maßnahmen bei der Verarbeitung von personenbezogenen Daten überprüft.

Anlage 3 - Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

Subunternehmer	Anschrift	Dienstleistung
Alfahosting GmbH	Edmund-von-Lippmann-Straße 13-15 06112 Halle (Saale) Deutschland	Hosting-Dienste, Domaindienstleistungen, Backup, Cloud Server Dienste

Beauftragte Subunternehmer der Alfahosting GmbH im Rahmen der Auftragsverarbeitung entsprechend Ziffer 8 der Zusatzvereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO

Subunternehmer	Anschrift	Dienstleistung
Host Europe GmbH	Hansestraße 111, 51149 Köln	Hosting-Dienste
United-domains Reselling GmbH	Gautinger Straße 10, 82319 Starnberg	Domaindienstleistungen
Content Management AG	Im Mediaparkt 6, 50670 Köln	Softwarelizenzen für eigene Endkunden
BUSYMOUSE Business Systems GmbH	Am Mittelfelde 29, 30519 Hannover	Backup
dogado GmbH	Saarlandstraße 25, 44139 Dortmund	Cloud Server Dienste