Vereinbarung zur Auftragsverarbeitung der Retail.me GmbH

Version 1.3
Letzte Aktualisierung: 13.04.2021

Präambel

Die Retail.me GmbH bietet internetbasierte Anwendungen zur Digitalisierung von Vertriebs- und Einkaufsabläufen für Handelskunden und Lieferanten, welche über die Website https://www.gotoemma.de abgerufen werden können. Wenn und soweit der Kunde auf von der Retail.me GmbH technisch verantworteten IT-Systemen personenbezogene Daten verarbeitet, ist die Retail.me GmbH **Auftragsverarbeiter** gemäß Art. 4 Nr. 8 DSGVO (nachfolgend auch „Auftragnehmer" genannt) und ist der Kunde **Verantwortlicher** gemäß Art. 4 Nr. 7 DSGVO (nachfolgend auch „Auftraggeber" genannt).

Um den gesetzlichen Anforderungen an die Auftragsverarbeitung zu erfüllen, schließen die Retail.me GmbH und der Kunde mit Abschluss des Nutzungsvertrages über die Software diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO. Eine gesonderte Unterzeichnung dieser Vereinbarung zur Auftragsverarbeitung ist nicht erforderlich.

1. Vertragsgegenstand

Im Rahmen des zwischen den Parteien bestehenden Leistungsverhältnisses über die Bereitstellung und Nutzung der Software (nachfolgend „Hauptvertrag" genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO ist (nachfolgend „Auftraggeber-Daten" genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen, Dauer der Auftragsverarbeitung

Der Auftragnehmer verarbeitet die personenbezogenen Daten während der Dauer des Hauptvertrages im Auftrag und nur nach Weisung des Auftraggebers. Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien betroffener Personen werden in **Anlage 1** festgelegt. Jede davon abweichende oder darüber hinaus gehende Verarbeitung von personenbezogenen Daten, insbesondere zu eigenen Zwecken, ist dem Auftragnehmer untersagt.

3. Weisungsrechte des Auftraggebers

3.1 Der Auftragnehmer verwendet die Auftraggeber-Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden.

3.2 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag, gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen.

3.3 Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber den Grund der Verarbeitung und die entsprechenden rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.4 Die Datenverarbeitung durch den Auftragnehmer erfolgt im Rahmen der Zurverfügungstellung einer standardisierten, aber konfigurierbaren Software über das Internet. Der Auftraggeber übt sein Weisungsrecht in Bezug auf die Daten durch Einrichtung und Benutzung der Software aus. Im Übrigen sind Weisungen mindestens

in Textform (z.B. E-Mail) zu erteilen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform (z.B. E-Mail). Weisungsfrei ist die angemessene Fortentwicklung und Anpassung der Software durch den Auftragnehmer.

3.5 Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers. Aufgrund der Standardisierung der Software beschränken sich Einzelweisungen im Wesentlichen auf gesondert zu vereinbarenden Anpassungen der Software oder auf Datenmigrationen. 4

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber ist nach außen, also gegenüber Dritten und den Betroffenen, für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

4.2 Der Auftraggeber ist Inhaber aller etwaigen Rechte, die für die Verarbeitung der Auftraggeber-Daten erforderlich sind.

4.3 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.4 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen (insbesondere in Bezug auf technische und organisatorische Maßnahmen der Datensicherheit) des Auftragnehmers vertraulich zu behandeln. Dieser Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4.5 Soweit sich der Auftragnehmer gegen einen Anspruch auf Schadenersatz nach Art. 82 DSGVO, gegen ein drohendes oder bereits verhängtes Bußgeld nach Art. 83 DSGVO oder sonstige Sanktionen im Sinne des Art. 84 DSGVO mit rechtlichen Mitteln verteidigen will, erlaubt der Auftraggeber dem Auftragnehmer Details der Auftragsverarbeitung inklusive erlassener Weisungen zum Zweck der Verteidigung offenzulegen.

4.6 Der Auftraggeber unterstützt den Auftragnehmer bei Kontrollen durch eine Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

5. Pflichten des Auftragnehmers

5.1 Soweit sich eine betroffene Person in Wahrnehmung ihrer Rechte aus Kapitel 3 DSGVO (Art. 12 bis 23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32 bis 37 BDSG) unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und den Auftraggeber auf zumutbare Weise mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung solcher Anträge auf Wahrnehmung der in Kapitel 3 DSGVO benannten Rechte der betroffenen Person nachzukommen.

5.2 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

5.3 Wenn dem Auftragnehmer hinsichtlich der verarbeiteten Auftraggeber-Daten eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO bekannt wird („Datenschutzvorfall“), meldet er dies dem Verantwortlichen unverzüglich. Im Rahmen der Meldung gem. Art. 33 Abs. 2 DSGVO teilt der Auftragnehmer dem Auftraggeber nach Möglichkeit den Zeitpunkt sowie Art und Ausmaß des Vorfalls, das betroffene IT-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, alle denkbaren nachteiligen Folgen des Datensicherheitsvorfalls sowie die daraufhin ergriffenen Maßnahmen mit.

5.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn Rechte des Auftraggebers an den personenbezogenen Daten beim Auftragnehmer durch Maßnahmen Dritter oder durch sonstige Ereignisse maßgeblich berührt werden.

5.5 Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers sämtliche Auftraggeber-Daten herauszugeben. Vom Auftraggeber erhaltene Datenträger sind gesondert zu kennzeichnen und laufend zu

verwalten. Kopien und Duplikate der personenbezogenen Daten dürfen ausschließlich nach vorheriger Zustimmung durch den Auftraggeber angefertigt werden, sofern sie nicht zur ordnungsgemäßen Durchführung dieser Vereinbarung bzw. des jeweiligen Projektauftrags oder zur Einhaltung von gesetzlichen Aufbewahrungspflichten dienen.

5.6 Sofern eine gesetzliche Pflicht besteht, benennt der Auftragnehmer einen Datenschutzbeauftragten (Art. 37 ff. DSGVO) und teilt dessen Kontaktdaten sowie ggf. den Wechsel des Datenschutzbeauftragten dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mindestens in Textform mit.

6. Sicherheit der Verarbeitung

6.1 Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen insbesondere die Fähigkeit ein, die Vertraulichkeit, die Integrität, die Verfügbarkeit sowie der Belastbarkeit der Systeme auf Dauer sicherzustellen und die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Der Auftragnehmer führt regelmäßig eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch und dokumentiert die Ergebnisse.

6.2 Der Auftragnehmer garantiert, dass er vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen implementiert, während der Dauer der Verarbeitung aufrechterhält und wenn erforderlich dem Stand der Technik und dem Risiko der Verarbeitung anpassen wird.

6.3. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftragnehmer räumt dem Auftraggeber ein Kontrollrecht zur Prüfung der Datenverarbeitung sowie Einhaltung dieses Vertrags bzw. des jeweiligen Projektauftrags ein. Insbesondere stellt der Auftragnehmer dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht die Durchführung von Überprüfungen einschließlich Inspektionen. Die Kontrollhandlungen können ebenfalls durch einen zur Geheimhaltung verpflichteten Dritten vorgenommen werden, sofern es sich bei dem Dritten um keinen Konkurrenten des Auftragnehmers handelt.

7.2 Die Parteien sind sich einig, dass der Auftraggeber eine Überprüfung nach Ziffer 7.1 durchführt, indem er den Auftragnehmer anweist, nach seiner Wahl ein geeignetes Testat, einen Bericht oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Datenschutzauditor oder Qualitätsauditor) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit – z.B. nach ISO 27001 oder BSI-Grundschutz – („Prüfungsbericht“) vorzulegen. In begründeten Ausnahmen kann der Auftraggeber eigenständige Inspektionen durchführen.

7.3 Der Auftragnehmer verpflichtet sich, die Durchführung der Kontrollen zu unterstützen. Dies beinhaltet die Gewährung sämtlicher benötigter Zugangs-, Auskunfts- und Einsichtsrechte. Gleiches gilt für öffentliche Kontrollen durch die zuständige Aufsichtsbehörde gemäß den anwendbaren Datenschutzvorschriften.

7.4 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens vier Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

8. Unterauftragsverhältnisse

8.1 Der Auftragnehmer darf Unterauftragsverhältnisse mit weiteren Auftragsverarbeitern (Subdienstleister) begründen. Zurzeit beschäftigt der Auftragnehmer die in **Anlage 3** bezeichneten Subdienstleister. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer informiert den Auftraggeber

immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subdienstleistern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen innerhalb von zwei Wochen Einspruch zu erheben. Sofern der Auftraggeber keine begründeten Einwände innerhalb von 2 Wochen ab Mitteilung über die Änderung erhebt, gilt diese als durch den Auftraggeber genehmigt.

8.2 Ist die Beauftragung eines Subdienstleisters mit einer Übermittlung der Auftraggeber-Daten in ein Land außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraum (EWR) („Drittland“) verbunden, gelten zusätzlich die Vorgaben aus Ziffer 9.

8.3 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Datenschutzpflichten, auch gegenüber dem Subdienstleister gelten und diesen gem. Art. 28 Abs. 4 DSGVO vor Aufnahme der Tätigkeiten entsprechend im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zu verpflichten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

9. Übermittlung von Auftraggeber-Daten an Drittländer

9.1 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Übermittlung der Auftraggeber-Daten in ein Land außerhalb von EU/EWR („Drittland“) erfolgt nur wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

9.2 Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, im Namen des Auftraggebers mit einem Subdienstleister, an den Auftraggeber-Daten zur Verarbeitung in einem Drittland übermittelt werden sollen, die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern gem. Beschluss der Kommission 2010/87/EU v. 5.2.2010, ABl. 2010 L 39 abzuschließen.

10. Rückgabe und Löschung von Auftraggeber-Daten

10.1 Nach Beendigung des Hauptvertrags wird der Auftragnehmer die Auftraggeber-Daten in angemessener Zeit löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, dürfen durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden.

10.2 Der Auftragnehmer ist nicht verpflichtet, Daten für den Auftraggeber über die Vertragslaufzeit hinaus vorzuhalten.

10.3 Den Auftragnehmer treffen keine Unterstützungspflichten bei Migration der Auftraggeber-Daten zu einem anderen Anbieter. Das Recht der betroffenen Personen auf Datenübertragbarkeit gemäß Art. 20 DSGVO wird jedoch nicht eingeschränkt.

11. Freistellung

Sofern gegen den Auftragnehmer wegen eines Verstoßes gegen die DSGVO bei der Verarbeitung der Auftraggeber-Daten Ansprüche auf Zahlung von Schadenersatz gemäß Art. 82 DSGVO geltend gemacht werden, ohne dass der Auftragnehmer gegen eine vom Auftraggeber erlassene Weisung verstoßen hat, stellt der Auftraggeber den Auftragnehmer auf erstes Anfordern von allen Ansprüchen frei. Der Auftraggeber übernimmt hierbei auch die Kosten der notwendigen Rechtsverteidigung des Auftragnehmers einschließlich sämtlicher Gerichts- und Anwaltskosten. Die Freistellungspflicht gilt nicht, soweit der Schadenersatzanspruch auf die Verletzung einer speziell den Auftragsverarbeitern auferlegten Pflicht aus der DSGVO gestützt wird.

12. Vergütung

Der Auftragnehmer kann vom Auftragnehmer für Unterstützungsleistungen nach Ziffer 5.1 und Ziffer 5.2 dieser Vereinbarung sowie für die Mitwirkung an eigenständigen Inspektionen des Auftraggebers nach Ziffer 7.2 eine angemessene Vergütung verlangen. Dies gilt nicht, wenn die Unterstützung notwendig ist, weil der Auftragnehmer gegen eine Weisung des Auftraggebers verstoßen oder einer speziell den Auftragsverarbeitern

auferlegte Pflicht aus der DSGVO verletzt hat. Geht der Inhalt der Einzelweisung nach Ziffer 3.5 über die Leistungen des Hauptvertrages hinaus, hat der Auftraggeber die entsprechenden Leistungen dem Auftragnehmer gesondert zu vergüten.

13. Laufzeit und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

14. Verhältnis zum Hauptvertrag

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrages. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

Anlagen:
Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen
Anlage 2: Technische und organisatorische Maßnahmen
Anlage 3: Unterauftragnehmer

Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Art und Zweck der Datenverarbeitung:

Die Software umfasst im Wesentlichen folgende Funktionen, die der Auftraggeber nutzen kann:

Verarbeitung der Daten für Trade-Marketing in den Handel, Vertriebsanfragen und digitale Vertriebsbesuche. Auswertung und Aggregation von Rückmeldungen, sowie Versand von E-Mails zur Information.

Der vollständige Funktionsumfang ergibt sich aus der Funktionsbeschreibung des gewählten Serviceplans des Auftragnehmers auf der Internetseite www.gotoemma.de.

Zum Auftrag gehören Hosting und Wartung der Software sowie Support.

Art der personenbezogenen Daten:

Vorname, Nachname, E-Mail, u.U. Profilfoto, Position, Telefon/Mobil

Kategorien betroffener Personen:

Beschäftigte des Auftraggebers; Kunden und Ansprechpartner bei Kunden des Auftraggebers (insbesondere Großhandelseinkäufer, Marktleiter /-mitarbeiter, Außendienstmitarbeiter, Key Accounter, Marketer); sonstige Kontakte des Auftraggebers

Anlage 2: Technische und organisatorische Maßnahmen

Verantwortlicher: Retail.me GmbH, Baumwall 3, 20459 Hamburg

Datenschutzbeauftragter: Herting Oberbeck Datenschutz GmbH, Herr Sebastian Herting, Hallerstr. 76, 20146 Hamburg, Telefon 040-228691140, herting@datenschutzkanzlei.de

Hinweis zu Maßnahmen bei (Unter)-Auftragnehmern:

Die maßgebliche Datenverarbeitung erfolgt auf IT-Systemen, die auf Managed Servern von dem Unterauftragnehmer Alice And the Builders GmbH betrieben werden. Bitte beachten Sie diesbezüglich ergänzend das Sicherheitskonzept der Alice And the Builders GmbH (Anlage).

Das Hosting der IT-Systeme der Alice And the Builders GmbH erfolgt in Rechenzentren der Hetzner Online GmbH. Bitte beachten Sie diesbezüglich ergänzend das Sicherheitskonzept Hetzner GmbH (Anlage).

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Zutrittskontrolle
Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- Eingangstüren werden stets verschlossen gehalten.
- Kontrollierte Schlüsselvergabe
- Electronic Keys für Gebäude- und Bürotüren + Schlüssel für Bürotür (Sicherheitsschloss)
- Besucher/Externe werden stets beaufsichtigt.
- Videoüberwachung mit Aufzeichnung im Korridor des Gebäudes

Zugangskontrolle/Verschlüsselung
Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Jedes System ist mit einer Benutzerauthentifizierung aus Betriebsebene geschützt
- Jeder Nutzer hat persönliche Zugangsdaten
- Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit
- Zugänge von Mitarbeitern, die nicht mehr im Unternehmen beschäftigt sind (zeitweise oder endgültig) werden gesperrt (gelöscht)
- Abschottung des Netzwerkes gegen ungewollte Zugriffe von außen (Firewall).
- Fernzugriff auf Serverumgebungen nur per SSH möglich.

Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Individuelle Zugriffsrechte für jeden einzelnen Benutzer, zentrale Verwaltung und Steuerung.
- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt.
- Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen.

Trennungskontrolle/Zweckbindungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Trennung von Produktiv- und Testsystemen
- applikationsseitige Mandantentrennung

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

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:

- Alle Mitarbeiter/innen sind i.S.d Art 32 Abs 4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
- Alle personenbezogenen oder geheimen Daten werden verschlüsselt bzw. mit Passwortschutz übermittelt
- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN.
- Mitbringen und verwenden privater Datenträger ist untersagt.

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Protokollierung der Aktivitäten aller Nutzer
- automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung.
- Protokollierung gescheiterter Zugriffsversuche.
- Protokollierung aller Aktivitäten auf dem Server.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

- Versionierte Daten- und Systembackups nach Backup-Plan (stündlich (Delta), 6-stündlich, täglich).
- Festplattenspiegelung (RAID), Backup-Rechenzentrum.
- Schadsoftwareschutz. Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt.
- Unterbrechungsfreie Stromversorgung

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

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können:

- Auftragnehmer werden sorgfältig ausgesucht.
- Es geschieht keine Auftragsverarbeitung ohne Weisung des Auftraggebers
- Klare und unzweifelhafte vertragliche Regelungen zur Datenverarbeitung
- Kontrolle des Auftragnehmers durch die Geschäftsführung oder den Datenschutzbeauftragten.
- Pflicht zur Vorbewertung
- Jeder Mitarbeiter der ein System betreut, ist hinsichtlich des Datenschutzes sensibilisiert worden (auch Art. 25 DSGVO)

Datenschutz-Management

Maßnahmen, die eine Steuerung der Datenschutzprozesse ermöglichen und die Einhaltung der datenschutzrechtlichen Vorgaben nachweisbar sicherstellen:

- Es wurde eine fachkundige Person zum Datenschutzbeauftragten benannt
- Beschäftigte werden regelmäßig im Datenschutz geschult und sensibilisiert und sind über die Vertraulichkeit von Daten belehrt.

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO, Art. 25 Abs. 1 DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

- User-ID

Anlage 3: Unterauftragnehmer

Name, Anschrift/Land, Auftragsinhalt

Alice And The Builders GmbH, Grantham-Allee 2-8, 53757 Sankt Augustin / Deutschland, Pflege und Hosting der Server-Infrastruktur
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen / Deutschland (als Unterauftragnehmer von Alice And The Builders GmbH / Hosting der Server-Infrastruktur
InScript GmbH, Wipplingerstraße 31, 1010 Wien / Österreich, Entwicklungsagentur mit beschränktem, projektbezogenem Zugriff auf Beta/Prelive Instanz/Quellcode/Datenbank (sofern eine Offenbarung von Auftraggeber-Daten nicht ausgeschlossen werden kann).
SendGrid, 1801 California Street, Denver CO 80202 / USA, transaktionaler E-Mail Versand