Auftragsdatenverarbeitung der internetbasierten Hotelmanagement-Software

Diese Auftragsdatenverarbeitung ist Anlage 3 zum Vertrag über die Nutzung der internetbasierten Hotelmanagement-Software der HotelFriend Service GmbH zwischen HotelFriend („Auftragnehmer") und dem Kunden ("Auftraggeber"). Sofern in diesem Vertrag nicht anders definiert, haben die im Folgenden verwendeten Begriffe die Bedeutung, die ihnen im Vertrag über die Nutzung der internetbasierten Hotelmanagement-Software der HotelFriend Service GmbH zukommt. Für diesen Auftragsverarbeitungsvertrag gelten zudem die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO"), insbesondere des Art. 4 DSGVO.

1. Gegenstand des Auftrags

1.1 Gegenstand dieses Auftragsverarbeitungsvertrages ist die Festlegung des datenschutzrechtlichen Rahmens für die vertraglichen Beziehungen zwischen den Parteien.

1.2 Der Gegenstand des Auftrags ergibt sich aus dem Softwarevertrag, auf den hier verwiesen wird (im Folgenden „Leistungsvereinbarung) sowie aus den noch zu schließenden Verträgen.

2. Support und Dienstleistungen

2.1 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

2.2 Jede Verlagerung der Verarbeitung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in schriftlicher Form und darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

3. Laufzeit

3.1 Die Dauer dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung.

3.2 Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

4. Umfang, Art & Zweck der Datenverarbeitung (Art. 4 Nr. 2 DSGVO)

4.1 Die Verarbeitung ist für die Erfüllung eines Vertrags oder einer vorvertraglichen Maßnahme gem. Art. 6 Abs. 1 lit. b DSGVO erforderlich. Die Verarbeitung ist zudem zur Wahrung des berechtigten Interesses des Verantwortlichen oder eines Dritten gem. Art. 6 Abs. 1 lit. f DSGVO erforderlich.

4.2 Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

4.2.1 Personenstammdaten (Name, Adresse, eventuell Geburtsdatum)

4.2.2 Kontaktdaten der betroffenen Mitarbeiter und Dienstleister des Auftraggebers

4.2.3 Kommunikationsdaten (z.B. Telefon, E-Mail)

4.2.4 Vertragsstammdaten (Vertragsbeziehung, Informationen zum Auftragsstatus, Produkt- bzw. Vertragsinteressen)

4.2.5 Kundenhistorie (Daten aus Angeboten, Angebotsbestätigungen und Rechnungen)

4.2.6 Vertragsabrechnungs- und Zahlungsdaten (Bank-, Zahlungs- und Kontoinformationsdaten, steuerrelevante Daten)

4.2.7 Planungs- und Steuerungsdaten

5. Kategorien betroffener Personen

Betroffen von der Verarbeitung sind nachstehende Kreise von Betroffenen des Auftraggebers:

5.1 Bestandskunden und Interessenten an den Produkten und/oder Leistungen

5.2 Beschäftigte, sowie externe Dienstleister des Auftraggebers, die mit der Erfüllung der o.g. Verarbeitungszwecke beauftragt sind

5.3 Handelsvertreter und sonstige Ansprechpartner seitens des Auftraggebers und Auftragnehmers, die mit der Erfüllung der o.g. Verarbeitungszwecke beteiligt sind

5.4 Steuerberater

6. Weisung

6.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten.

6.2 Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrages und anschließend noch für drei Jahre aufzubewahren.

6.3 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. In einem solchen Fall ist der Auftragnehmer nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber die Weisung

geändert hat oder diese bestätigt. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

6.4 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Der Auftragnehmer legt Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

7. Unterstützungspflichten des Auftragnehmers

7.1 Der Auftragnehmer ergreift angesichts der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen.

7.2 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO. Im Einzelnen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen an die Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei einer Verletzung, der Datenschutz-Folgeabschätzung und bei der Konsultation der zuständigen Aufsichtsbehörde.

7.3 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich und stimmt die weiteren Schritte mit ihm ab.

8. Prüfungsrechte des Auftraggebers

8.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung. Insbesondere erteilt der Auftragnehmer dem Auftraggeber Auskünfte über die gespeicherten Daten und die Datenverarbeitungsprogramme.

8.2 Der Auftraggeber oder von ihm beauftragte Dritte sind – grundsätzlich nach Terminvereinbarung – berechtigt, die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO zu überprüfen und beim Auftragnehmer Inspektionen vor Ort durchzuführen. Der Auftragnehmer ermöglicht dies und trägt dazu bei.

8.3 Der Auftragnehmer hat dem Auftraggeber auf Anforderung geeigneten Nachweis über die Einhaltungen der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigte Verhaltensregeln i. S. v. Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren i. S. v. Art. 42 DSGVO abbilden, erbracht werden.

9. Mitteilung bei Verstößen des Auftragnehmers

9.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

9.1.1 die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

9.1.2 die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

9.1.3 die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

9.1.4 die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

9.1.5 die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

9.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

10.1 Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

10.1.1 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des

Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

10.1.2 Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Kapitel 13].

10.1.3 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

10.1.4 Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

10.2 Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10.3 Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

10.4 Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse.

11. Datenschutzbeauftragte

11.1 Der Auftragnehmer gewährleistet die Bereitstellung eines Datenschutzbeauftragten / Ansprechpartners / Vertreter als Kontaktperson durch die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

11.2 Datenschutzbeauftragter des Auftragnehmers ist: Herr Dr. Wilfried Röder, E-Mail: datenschutz@infai.org

12. Vertraulichkeit

12.1 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er wahrt bei der Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis sowie die Vertraulichkeit. Diese Pflicht besteht auch nach Beendigung dieses Vertragsverhältnisses fort.

12.2 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er verpflichtet diese Mitarbeiter durch schriftliche Vereinbarung für die Zeit der Tätigkeit und auch nach Beendigung des Beschäftigungsverhältnisses zur Wahrung der Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

12.3 Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung, oder Zustimmung in einem elektronischen Format, durch den Auftraggeber erteilen.

13. Technische und organisatorische Maßnahmen

13.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit eine Prüfung bzw. ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

13.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

13.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer

gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

13.4 Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

13.4.1 Bei der HotelFriend Service GmbH werden die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen ergriffen, um den Schutz und die Sicherheit der personenbezogenen Daten und das Recht auf Privatsphäre der betroffenen Personen zu gewährleisten.

13.4.2 Diese Maßnahmen werden im Rahmen des Datenschutzkonzeptes regelmäßig überprüft und fortlaufend aktualisiert. Bei der Konzeption dieser Maßnahmen wurden die gesetzlichen Schutzziele - Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste – umfassend berücksichtigt, sodass ein angemessener Maßnahmenplan entwickelt werden konnte.

13.4.3 Jegliche Verarbeitungsprozesse orientieren sich dabei im Wesentlichen an den Vorgaben der Art. 24, 25 und 32 DS-GVO. Dadurch kann auch in Hinsicht auf die Belastbarkeit der Systeme in Bezug auf Art, Umfang, Umstand und Zweck der Datenverarbeitungen das potentielle Risiko, welches bei dem Umgang mit personenbezogenen Daten entsteht, auf Dauer beschränkt werden.

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

13.5.1 Zutritts- und Zugangskontrolle

13.5.1.1 Technische Maßnahmen: Zäune, Pforten und andere räumliche Begrenzungen; Sicherung von Fenstern und Türen; Sichere VPN-Verbindung; Verschlüsselung von Datenträgern und mobilen Endgeräten, Firewall, File-Servern; Front-End- und Applikationssysteme sowie Antiviren-Software werden – sofern anwendbar – eingesetzt; Protokollierung der Zutrittsrechte; Authentifikation mittels Passworteingabe oder biometrischer Scans; zentraler Schließplan mit Dokumentation der vergebenen Schlüssel.

13.5.1.2 Organisatorische Maßnahmen: Besuchermanagement; Schlüsselregelungen; Passwortregeln inkl. Vorgaben für die Komplexität des Passwortes (Richtlinie); Vertrauenswürdiges Personal für die Bereiche Sicherheit und Reinigung; Generierung von Benutzerprofilen; Zuordnung von Benutzerrechten; Rollen- und Berechtigungskonzept; Kontrolle des Wartungs-, Reparatur-und Reinigungspersonals; Die Mitarbeiter sind gem. DS-GVO belehrt; Die Mitarbeiter sind belehrt, Fenster und Türen außerhalb der Bürozeiten verschlossen zu halten; Mitarbeiter sind zur Aktivierung der automatischen Desktopsperre verpflichtet; Alle Mitarbeiter werden zur Clean-Desk-Policy angewiesen; Es gibt für alle Informationssysteme und Dienste eine formale Benutzer-Registrierung und Deregistrierung zur Vergabe und Rücknahme von Zugangsberechtigungen.

13.5.2 Zugriffskontrolle

13.5.2.1 Technische Maßnahmen: Datenschutzkonforme Vernichtung von Datenträgern, Verschlüsselung von Datenträgern und mobilen Endgeräten; Identifizierungs- und Authentifizierungssystem (Zwei-Faktor-Authentifikation); Sichere Aufbewahrung von Datenträgern; Datenschutzkonforme Vernichtung von Datenträgern; Verschlüsselung von Datenträgern und mobilen Endgeräten.

13.5.2.2 Organisatorische Maßnahmen: Passwortregeln (Richtlinie, zentrale Passwortvergabe); Berechtigungskonzepte; Anpassung der Anzahl an Administratoren, die die volle Zugriffsberechtigung haben; Für den Zugang zur Datenverarbeitungssystemen ist eine Authentifikation mit Benutzerprofil, Passwort oder Zertifikat erforderlich; Für sämtliche schutzwürdige Systeme der Datenverarbeitung wird eine personenbezogene Benutzerverwaltung durchgeführt; Berechtigungen und Profile werden differenziert und aufgabenbezogen erstellt. Die Verwaltung von Benutzerrechten erfolgt durch Administratoren; Es existiert eine Regelung mit einzuleitenden Folgemaßnahmen bei Verlust von Ausweisen und Schlüsseln; Der Bereich IT-Betrieb führt einen Nachweis des Zugriffs durch Vorgangsprotokolle über Änderungen und Löschungen in Bezug auf Daten, Zeitpunkte der Verarbeitung und Benutzer; Papierakten (sofern vorhanden) werden vor Ort kontrolliert über einen Aktenvernichter der DIN-Sicherheitsstufe 3 vernichtet. Es existiert eine klare Anweisung zur Entsorgung oder Weiterverwendung von Geräten, die mit Speichermedien ausgerüstet sind; Die Überprüfung von Zugriffsrechten findet laufend durch den Systemadministrator statt.

13.6 Integrität (Art. 32 Abs. 1 DSGVO)

13.6.1 Eingabekontrolle

13.6.1.1 Technische Maßnahmen: Digitales Berechtigungskonzept; Elektronische Signatur; E-Mail-Verschlüsselung.

13.6.1.2 Organisatorische Maßnahmen: Einrichtung und Verwendung von individuellen Benutzernamen; Vergabe von Zugriffsberechtigungen; Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt auf Basis eines Berechtigungskonzepts.

13.6.2 Trennungskontrolle

13.6.2.1 Technische Maßnahmen: Klare Trennung der für verschiedene Zwecke gespeicherten Daten; Die Systeme für die Test- und Produktivumgebung sind getrennt; Sofern anwendbar, sind Datensätze sind mit Zweckattributen versehen; Sämtlichen personenbezogenen Daten ist jeweils eine individuelle Kundennummer zugeordnet. Eine logische Trennung ist gewährleistet.

13.6.2.2 Organisatorische Maßnahmen: Mandantentrennung; Steuerung über

Berechtigungskonzept; Besuchermanagement (hier: Gastzugänge); Die Zielstellung des Trennungsgebots wird durch die restriktive Zugriffs- und Auftragskontrolle sichergestellt; Die betriebliche Nutzung privater Geräte ist allen Mitarbeitern schriftlich untersagt.

13.6.3 Weitergabekontrolle

13.6.3.1 Technische Maßnahmen: Digitales Berechtigungskonzept; Sichere VPN-Technologie; E-Mail-Verschlüsselung; Der Bereich IT-Betrieb sichert eingeschränkte, verschlüsselte Datenfernübertragungsmöglichkeiten; Die Datenfernübertragung erfolgt verschlüsselt.

13.6.3.2 Organisatorische Maßnahmen: Es existieren Regelungen und Anweisungen zur Datenvernichtung und Löschung; Vergabe von Zugriffsberechtigungen; Archivierte Unterlagen lagern in einem verschlossenen Archiv mit begrenzten Zutrittsberechtigungen; Nach Ausscheiden bzw. Versetzung eines Mitarbeiters werden nicht mehr benötigte Zugangsberechtigungen entzogen bzw. Zugänge zu IT-Systemen gesperrt; Dienstleister werden schriftlich auf die Wahrung des Datengeheimnisses verpflichtet. Es sind keine Dienstleister vorhanden, die unautorisierten Zugang zu den Büroräumen erhalten.

13.7 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 DSGVO)

13.7.1 Technische Maßnahmen: Feuer- und Rauchmelder, Feuerlöscher, Alarmanlage; Firewall; Notfall-Management; Virenschutz; Sämtliche IT-Systeme sind redundant verfügbar.

13.7.2 Organisatorische Maßnahmen: Es existiert ein Backup & Recovery-Konzept; Dokumente und Datenträger, deren gesetzliche, vertragliche oder satzungsmäßige Aufbewahrungsdauer abgelaufen ist, werden vernichtet (Löschkonzept); nach Bedarf werden Belastungstests der Systeme durchgeführt.

13.8 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

13.8.1 Technische Maßnahmen: Der externe Zugriff auf das betriebliche Lan erfolgt ausschließlich per VPN; Zugänge zu Systemen sind stets verschlüsselt (TLS, SSL); Die Datenübertragung auf der Website wird verschlüsselt (TLS, SSL); Elektronische Kommunikation erfolgt mittels SSL/TSL-Verschlüsselung.

13.8.2 Organisatorische Maßnahmen: Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren; Es ist ein unabhängiger WLAN-Gästezugang vorhanden; Die Einzelangaben, mit denen die Anonymität aufgehoben werden kann, werden getrennt von den übrigen Daten gespeichert. Je nach Verknüpfbarkeit und dem Auftraggeber wird der Personenbezug wiederhergestellt. – sofern zutreffend; Es existieren interne Anweisungen, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren. – sofern zutreffend.

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

13.9.1 Vertragskonformitäts- / Auftragskontrolle

13.9.1.1Es wird jeweils ein schriftlicher Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers geschlossen.

13.9.1.2 Es erfolgt eine vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation.

13.9.1.3 Es entstehen vertraglich festgelegte Regelungen zum Einsatz weiterer Subunternehmer.

13.9.1.4 Es entstehen vertraglich festgelegte Verantwortlichkeiten.

13.9.1.5 Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.

13.9.1.6 Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus.

13.9.1.7 Alle Mitarbeiter werden auf das Datengeheimnis verpflichtet und es werden in regelmäßigen Abständen Schulungen und Belehrungen zum Thema Datenschutz und Datensicherheit durchgeführt. Eine Datenschutzschulung erfolgt spätestens aller 2 Jahre.

13.9.2 Datenschutzmanagement

13.9.2.1 Ein Datenschutzbeauftragter wurde schriftlich bestellt.

13.9.2.2 Das Verzeichnis von Verarbeitungstätigkeiten ist vorhanden, vollständig und aktuell.

13.9.2.3 Dienstleister werden gelistet und regelmäßig auf deren Einhaltung des Datenschutzes geprüft.

13.9.2.4 Es existiert ein Löschkonzept zur Beschränkung der Speicherfrist (Löschregeln, Verantwortlichen, Löschfristen).

13.9.2.5 Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt.

13.9.2.6 Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach.

13.9.2.7 Es existiert ein formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener sowie zum Umgang mit Datenschutzverfällen.

13.9.2.8 Mitarbeiter werden jährlich auf Vertraulichkeit und Datengeheimnis geschult bzw. aller 2 Jahre über die Grundkenntnisse im Datenschutz geschult. Bei Neuerungen im Unternehmenskontext finden

individuelle Datenschutzschulungen statt.

13.9.2.9 Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...).

13.9.2.10 Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

13.9.2.11 Die Erklärungen zu datenschutzrechtlichen Verpflichtungen der verarbeitenden Mitarbeiter liegen vor.

13.10 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

13.10.1 Beschränkung der Speicherfrist

13.10.2 Beschränkung der Zugänglichkeit

13.10.3 Beschränkung des Umfangs der Verarbeitung der erhobenen Daten

13.10.4 Überwachung externer Zugriffe (Logfiles)

13.10.5 Einsatz von Spamfilter und regelmäßige Aktualisierung.

13.10.6 Einsatz von Virenscanner und regelmäßige Aktualisierung.

13.10.7 Dokumentierte Vorgehensweise (Notfallpläne) zum Umgang mit Sicherheitsvorfällen und formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

14. Informationspflichten des Auftragnehmers und Verletzung des Schutzes personenbezogener Daten

14.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jegliche Verstöße oder vermutete Verstöße gegen diesen Vertrag oder Vorschriften, die den Schutz personengezogener Daten betreffen.

14.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Untersuchung, Schadensbegrenzung und Behebung der Verstöße.

14.3 Sollten die personenbezogenen Daten die unter dieser Vereinbarung verarbeitet werden beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über die Daten beim Auftraggeber liegt.

14.4 Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer das Ergebnis dem Auftraggeber bekannt zu geben, soweit es die Verarbeitung der personenbezogenen Daten unter diesem Vertrag betrifft. Die im Prüfbericht feststellten Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.

15. Unterauftragnehmer

15.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

15.2 Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

15.3 Der Auftraggeber stimmt der Beauftragung von Unterauftragnehmern zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO. Er stimmt insoweit bereits jetzt der Beauftragung der in diesem Kapitel benannten Unterauftragnehmer zu.

15.4 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

15.5 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher, Nummer 2, Abs. 2. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

15.6 Zum Kreis der genehmigten Unterauftragnehmer bei Abschluss dieses Vertrages gehören:

15.6.1 Amazon Web Services, Inc.

Adresse: 410 Terry Avenue North, Seattle WA 98109,
United States;

Zweck: Hosting;

Ort der Datenverarbeitung: Deutschland;

Garantie: Angemessenheitsbeschluss liegt vor. Amazon.com Inc. ist DPF-zertifiziert. Die Nutzung des Tools Amazon Web Services ist zulässig.

15.6.2 fiskaly GmbH

Adresse: Mariahilfer Straße 36/5, 1070 Wien, Österreich;

Zweck: Fiskalisierung von Rechnungen;

Ort der Datenverarbeitung: EU, Österreich;

Garantie: Auftragsverarbeitungsvertrag, geprüfte TOM, Listung geprüfter Subdienstleister, Geheimhaltungs-vereinbarung, ISO 27001 Zertifizierung.

15.6.3 Adyen N.V.

Adresse: Simon Carmiggeltstraat 6, 1011 DJ, Amsterdam, Niederlande;

Zweck: Zahlungsabwicklung;

Ort der Datenverarbeitung: Amsterdam, Niederlande;

Garantie: Auftragsverarbeitungsvertrag, geprüfte TOM, Listung geprüfter Subdienstleister, Geheimhaltungs-vereinbarung.

16. Löschung und Rückgabe personenbezogener Daten

16.1 Der Auftragnehmer ist nach Abschluss, der jeweils im Hauptvertrag vereinbarten Verarbeitungsleistungen verpflichtet, alle personenbezogenen Daten, die er im Zuge der Auftragsverarbeitung erhalten hat, nach Wahl des Auftraggebers an den Auftraggeber zurückzugeben oder zu löschen. Dies schließt insbesondere die Ergebnisse der Datenverarbeitung, überlassene Dokumente und überlassene Datenträger und Kopien der personenbezogenen Daten mit ein. Die Pflicht zur Löschung oder Rückgabe besteht nicht, sofern der Auftragnehmer nach dem Recht der EU oder der Mitgliedstaaten zur weiteren Speicherung der Daten gesetzlich verpflichtet ist. Besteht eine weitere Verpflichtung zur Speicherung, hat der Auftragnehmer die Verarbeitung der personen-bezogenen Daten einzuschränken und die Daten nur für die Zwecke zu nutzen, für die eine Verpflichtung zur Speicherung besteht. Die Pflichten zur Sicherheit der Verarbeitung bestehen für den Zeitraum der Speicherung fort. Der Auftragnehmer hat die Daten unverzüglich zu löschen, sobald die Pflicht zur Speicherung entfällt.

16.2 Die Löschung hat so zu erfolgen, dass die Daten nicht wiederherstellbar sind.

16.3 Die Vorgänge sind mit Angabe von Datum und durchführender Person zu protokollieren. Die Protokolle sowie ein Nachweis der Durchführung in schriftlicher Form sind dem Auftraggeber nach Durchführung der Vorgänge zur Verfügung zu stellen.

17. Haftung

17.1 Der Auftraggeber gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen bei der Verarbeitung personenbezogener Daten.

17.2 Es gelten grundsätzlich die Haftungsbeschränkungen aus dem Hauptvertrag. Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen frei, die Dritte wegen der Verletzung ihrer Rechte gegen den Auftragnehmer auf Grund der vom Auftraggeber Beauftragung personenbezogener Daten geltend machen, sofern nicht der Anspruch des Dritten auf einer rechtswidrigen Verarbeitung der personenbezogenen Daten durch den Auftragnehmer beruht. Art. 82 DSGVO bleibt unberührt.

18. Sonstiges, Allgemeines

18.1 Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren.

18.2 Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den personenbezogenen Daten des Auftraggebers bei dem Auftraggeber liegt.

18.3 Unbeschadet des Weisungsrechts des Auftraggebers gemäß Absatz 11 dieser Vereinbarung bedürfen Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf diese Formerfordernis.

18.4 Die Regelungen dieser Vereinbarung gelten auch nach einer Beendigung des primären Leistungsverhältnisses bis zur vollständigen Vernichtung oder Rückgabe aller personenbezogenen Daten des Auftraggebers an den Auftraggeber fort.

18.5 Sollten einzelne Teile der hier vorliegenden Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit dieser Vereinbarung im Übrigen nicht. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt.

19. Schlussbestimmungen

19.1 Für Änderungen oder Nebenabreden ist die Schriftform oder ein elektronisches Format erforderlich. Dies gilt auch für Änderungen dieses Formerfordernisses.

19.2 Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht.