Vereinbarung

zwischen dem/der

_____
- Verantwortlicher –
nachstehend Auftraggeber genannt - und dem/der

_____
ggf.: Vertreter gemäß Art. 27 DS-GVO:

praxiskom GmbH, AGENTUR FÜR PRAXISMARKETING
Steinerstraße 15 - Haus B - 81369 München

_____
- Auftragsverarbeiter -
nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand
Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung zum Hosting der Webseite des Auftragsgebers nebst den zugehörigen Leistungen, die vom Auftrag umfasst sind im Folgenden Leistungsvereinbarung.

(2) Dauer
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.
Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts:

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

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.

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, namens und in Auftrag des Auftraggebers bei google.de ein Kundenkonto zu eröffnen und die damit zusammenhängenden vertraglichen Erklärungen (z.B. Auftragsdatenverabeitung) für den Kunden abzugeben.

(2) Art der Daten

Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben. Dazu gehören:

> Kommunikationsdaten (z. B. Namen und Vorname, Anschrift, Telefon, E-Mail)
> Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
> Kundenhistorie
> Vertragsabrechnungs- und Zahlungsdaten
> Planungs- und Steuerungsdaten

3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben.

3. Technisch-organisatorische Maßnahmen

(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 die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(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.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

Der Auftraggeber kann vertraglich zur Übernahme der anfallenden Mehrkosten verpflichtet werden.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Emmanuel Croué, Geschäftsführer – info@praxiskom.com – Tel: 089 307 62 162 benannt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit der 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.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

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

e) 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.

f) 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.

g) 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.

6. Unterauftragsverhältnisse

(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.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs.2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift / Land	Leistung
Netz-Haut GmbH	Friedrich-Bergius-Ring 12 - 97076 Würzburg	Web-Hosting + Mail-Server

Der Wechsel des bestehenden Unterauftragnehmers ist 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 DS-GVO zugrunde gelegt wird.

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

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

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

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

a) die Gewährleistung 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

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

c) 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

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten, erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Unterschrift	Unterschrift
Auftraggeber	Auftragnehmer

ANLAGE 1 - TECHNISCH-ORGANISATORISCHE MAßNAHMEN (VERTRAGLICH VEREINBARTE SICHERHEITSMASSNAHMEN)

1. Der Auftraggeber wird für die Verarbeitung der personenbezogenen Daten die in der Vereinbarung festgelegten technischen und organisatorischen Maßnahmen treffen. Auf schriftliche Anfrage wird der Auftragnehmer einen Nachweis dafür erbringen, dass diese Maßnahmen bereitgestellt wurden.

2. Der Auftragnehmer wird mindestens die folgenden technischen und organisatorischen Maßnahmen treffen, soweit diese in Bezug auf die Leistungen in die Verantwortlichkeit des Auftragnehmers fallen und seiner Kontrolle unterliegen:

2.1 **Zugangskontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um Unbefugten den Zugang zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, zu verwehren. Unbefugte Personen dürfen keinen Zugang zum Büro haben, in dem sich Verarbeitungsanlagen befinden, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden. Externen Prüfern darf der Zugang ausnahmsweise gewährt werden, solange sie vom Auftragnehmer überwacht werden und keinen Zugriff auf die Verarbeiteten Personenbezogenen Daten erhalten.

Der Auftragnehmer wird insbesondere

(a) berechtigte Personen benennen

(b) einen Prozess zur Zugangskontrolle einrichten, um unbefugten Zugang zu Räumlichkeiten zu vermeiden

(c) einen Prozess zur Zugangskontrolle einrichten, um den Zugang zu Rechenzentren / Serverräumen zu beschränken

(d) Drittpersonal ohne Zugangsberechtigung (z.B. Techniker oder Reinigungspersonal) durchgängig begleiten

2.2 **Datenträgerkontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verhindern.

Der Auftragnehmer wird insbesondere

(a) Datenträger in gesicherten Bereichen verwahren

(b) Regeln für die sichere und dauerhafte Zerstörung von nicht mehr benötigten Datenträgern aufstellen

(c) Zugang zu Datenträgern nur seinem Personal und dem Personal seiner Subunternehmer sowie deren Organen, Angestellten, Vertretern und zulässigen Subunternehmern und Rechtsnachfolgern gewähren, jeweils mit der zur Erfüllung ihrer Aufgabe erforderlichen Berechtigung.

2.3 **Speicherkontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um eine unbefugte Eingabe von personenbezogenen Daten sowie eine unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten zu verhindern. Für ein Datenverarbeitungssystem berechtigte Personen sollen nur solche Daten eingeben und nur auf solche Daten Zugriff haben, für die sie ein Recht zur Eingabe oder zum Zugriff haben, und Verarbeitete Personenbezogene Daten dürfen im Rahmen der Verarbeitung nicht ohne Berechtigung gelesen, kopiert, verändert oder gelöscht werden.

Der Auftragnehmer wird insbesondere

(a) den Zugriff auf Dateien und Programme auf einer "Need-to-Know-Basis" beschränken

(b) Datenträger in gesicherten Bereichen verwahren

(c) die Nutzung/Installation nicht freigegebener Hardware und/oder Software verhindern

(d) Regeln für die sicher und dauerhafte Zerstörung von nicht mehr benötigten Daten aufstellen

(e) Zugang zu Daten nur seinem Personal und dem Personal seiner Subunternehmer sowie deren Organen, Angestellten, Vertretern und zulässigen Subunternehmern und Rechtsnachfolgern gewähren, jeweils mit der zur Erfüllung ihrer Aufgabe erforderlichen Berechtigung.

2.4 **Benutzerkontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte zu verhindern.

Der Auftragnehmer wird insbesondere

(a) angemessene Maßnahmen ergreifen, um Systeme, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, vor unbefugtem Zugriff mit Hilfe von Einrichtungen zur Datenübertragung zu schützen; dies beinhaltet den Einsatz von Firewalls und Intrusion Detection-Systemen

(b) den Fernzugriff auf Systeme, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, protokollieren

(c) für den Fernzugriff auf Systeme, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, Authentifizierungssysteme einsetzen

(d) Fernzugriff auf Applikationen, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, nur seinem Personal und dem Personal seiner Subunternehmer sowie deren Organen, Angestellten, Vertretern und zulässigen Subunternehmern und Rechtsnachfolgern gewähren, jeweils mit der zur Erfüllung ihrer Aufgabe erforderlichen Berechtigung

(e) Einen Prozess zur Deaktivierung von Fernzugriffsberechtigungen für den Fall etablieren, dass ein Benutzer das Unternehmen verlässt oder sich seine Aufgabe ändert

2.5 **Zugriffskontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Der Auftragnehmer wird insbesondere

(a) gewährleisten, dass alle Rechner, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden (auch bei Fernzugriff)

- nach der Boot-Sequenz und
- wenn sie für einen kurzen Zeit nicht genutzt wurden

mit einem Passwort geschützt sind, um den unbefugten Zugriff auf Verarbeitete Personenbezogene Daten zu verhindern

(b) für jede Person eine dedizierte Benutzerkennungen zur Authentifizierung gegenüber der Benutzerverwaltung des Systems verwenden

(c) individuelle Passwörter zur Authentifizierung zuweisen

(d) gewährleisten, dass für die Zugriffskontrolle ein Authentifizierungssystem eingesetzt wird, einschließlich des Fernzugriffs und der Fernnutzung von Systemen

(e) Zugriff auf Applikationen, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, nur seinem Personal und dem Personal seiner Subunternehmer sowie deren Organen, Angestellten, Vertretern und zulässigen Subunternehmern und Rechtsnachfolgern gewähren, jeweils mit der zur Erfüllung ihrer Aufgabe erforderlichen Berechtigung

(f) eine Passwortrichtlinie implementieren, die die Weitergabe von Passwörtern verbietet, einen geregelten Prozess für den Fall vorsieht, dass ein Passwort Dritten offengelegt wird und die eine regelmäßige Änderung von Passwörtern erfordert

(g) gewährleisten, dass jeder Rechner einen passwortgeschützten Bildschirmschoner hat, der sich spätestens nach 10-15 minütiger Inaktivität einschaltet

(h) gewährleisten, dass Passwörter immer verschlüsselt gespeichert werden

(i) einen Prozess zur Deaktivierung von Nutzerberechtigungen für den Fall etablieren, dass ein Benutzer das Unternehmen verlässt oder sich seine Aufgabe ändert

(j) einen Prozess zur Anpassung von Administratorberechtigungen für den Fall etablieren, dass ein Administrator das Unternehmen verlässt oder sich seine Aufgabe ändert

2.6 **Übertragungskontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

2.7 **Transportkontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Verarbeitete Personenbezogene Daten dürfen während des Transfers oder während der Speicherung nur insoweit gelesen, kopiert, geändert oder gelöscht werden, wie das für die Erbringung der Leistungen nach den Bestimmungen des Hauptvertrags erforderlich ist. Der Auftragnehmer trifft angemessene Maßnahmen, um die Vertraulichkeit und Integrität der Verarbeiteten Personenbezogenen Daten bei Übermittlung und Transport zu schützen.

Der Auftragnehmer wird insbesondere

(a) Daten für die Übermittlung verschlüsseln

2.8 **Wiederherstellbarkeit:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Der Auftragnehmer wird insbesondere

(a) Datensicherungen erstellen und diese in einer speziell geschützten Umgebung aufbewahren (soweit dies Teil der Leistungen ist)

(b) Regelmäßige Wiederherstellungstests mit solchen Datensicherungen durchführen

(c) Einen Notfall- und Wiederherstellungsplan für seinen eigenen Betrieb vorhalten

(d) Verarbeitete Personenbezogene Daten nicht von den Rechnern und aus den Räumlichkeiten des Auftragnehmers entfernen (sofern dies vom Auftraggeber nicht ausdrücklich zu Geschäftszwecken autorisiert wurde)

(e) aktuelle Anti-Viren-Lösungen auf Computersystemen einsetzen

2.9 **Zuverlässigkeit:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass alle Funktionen eines Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Insofern wird auf die Beschreibung der Leistungen, einschließlich Service Levels und Qualitätsanforderungen, sowie die Berichtspflichten des Auftragnehmers unter dem Hauptvertrag verwiesen.

2.10 **Datenintegrität**: Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können. Insofern wird auf die Beschreibung der Leistungen, einschließlich Service Levels und Qualitätsanforderungen, sowie die Berichtspflichten des Auftragnehmers unter dem Hauptvertrag verwiesen.

2.11 **Auftragskontrolle**: Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Der Auftragnehmer erbringt die Leistungen und insbesondere die Verarbeitung von Verarbeiteten Personenbezogenen Daten, nur im Einklang mit den erteilten Weisungen und wird seine Subunternehmer, die in die Verarbeitung der Verarbeiteten Personenbezogenen Daten einbezogen sind, entsprechend anweisen.

Der Auftragnehmer wird insbesondere

(a) die Leistungserbringung überwachen

(b) gemäß den schriftlichen Weisungen und vertraglichen Vereinbarungen arbeiten

(c) personenbezogene Daten, die er von verschiedenen Kunden erhalten, so verarbeiten, dass bei jedem Verarbeitungsschritt der jeweilige Verantwortliche in Bezug aufdie

personenbezogenen Daten identifiziert werden kann (physische und logische Trennung der Daten)

2.12 **Verfügbarkeitskontrolle:** Verarbeitete Personenbezogene Daten werden gegen Offenlegung sowie gegen versehentliche oder unbefugte Zerstörung oder Verlust geschützt.

Der Auftragnehmer wird insbesondere

(a) Datensicherungen erstellen und diese in einer speziell geschützten Umgebung aufbewahren (soweit dies Teil der Leistungen ist)

(b) Regelmäßige Wiederherstellungstests mit solchen Datensicherungen durchführen

(c) Einen Notfall- und Wiederherstellungsplan für seinen eigenen Betrieb vorhalten

(d) Verarbeitete personenbezoge Daten nicht zu anderen als den vertragsgemäßen Zwecken verwenden

(e) Verarbeitete Personenbezogene Daten nicht von den Rechnern und aus den Räumlichkeiten des Auftragnehmers entfernen (sofern dies vom Auftraggeber nicht ausdrücklich zu Geschäftszwecken autorisiert wurde)

(f) keine private Ausrüstung für die Erbringung der Leistungen verwenden

(g) gewährleisten, dass Nutzer, die ihren Arbeitsplatz während der Arbeitszeit verlassen oder nach Ende der Arbeitszeit verlassen, Dokumente, die Verarbeitete Personenbezogene Daten enthalten, in einem sicheren und gesicherten Umfeld verwahren, wie z.B. einer Schreibtischschublade, einem Aktenschrank oder einem gesicherten Aufbewahrungsort (Clean Desk)

(h) einen Prozess für die Zerstörung von Dokumenten und Datenträgern mit personenbezogenen Daten implementieren

(i) Firewalls auf Netzwerkebene verwenden, um unbefugten Zugriff auf Systeme und Services auf Netzwerkebene zu verhindern

(j) aktuelle Anti-Viren-Lösungen auf Computersystemen einsetzen

2.13 **Trennbarkeit:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Verarbeitete Personenbezogene Daten getrennt verarbeitet werden können. Der Auftragnehmer darf sich insoweit auf die Weisungen und Informationen des Auftraggebers verlassen, insbesondere in Bezug auf die Art der Verarbeiteten Personenbezogenen Daten und den Zweck ihrer Erhebung. Soweit Maßnahmen zur Trennung nicht unter die Pflichten des Auftragnehmers nach dem Hauptvertrag fallen, steht die Verpflichtung des Auftragnehmers zur Umsetzung solcher Maßnahmen unter dem Vorbehalt einer Vereinbarung, in der die Maßnahmen spezifiziert und eine angemessene Vergütung des Auftragnehmers vereinbart wird.