Servicevertrag „Onlinemarketing (SEA)“

Zwischen

hairfree GmbH Rheinstraße 19-21,
64283 Darmstadt
vertreten durch die Geschäftsführer Chris Kettern und Jens Hilbert
(nachfolgend kurz „FG“ genannt)

und dem Franchisepartner

Betreiber/Inhaber: .....

Straße: .....

PLZ/Ort: .....
(Institutsadresse)

(nachstehend „FP“ genannt)

1. Vertragsgegenstand

Der FP beabsichtigt, im Rahmen der Online-Marketingaktivitäten des hairfree-Systems Werbeanzeigen in der Suchmaschine Google (sog. Google-Ads) zur Bewerbung seiner Dienstleistungen zu schalten.

Zu diesem Zweck schließt der FP entsprechende Vereinbarungen zur Nutzung der Dienstleistungen der Google Ads unmittelbar mit dem Dienstleister, der Google Ireland Ltd. im eigenen Namen und auf eigene Rechnung ab.

In dem entsprechenden Nutzerkonto des FP werden durch den Anbieter Google Ireland Ltd. Funktionen und Dienstleistungen zur Gestaltung von Werbeanzeigen und Kampagnen sowie deren Beauftragung und Auswertung bereit gestellt. Der FP beauftragt den FG, ihn im Rahmen dieser Aktivitäten operativ zu unterstützen.

2. Leistungen des FG

2.1 In dem vertragsgegenständlichen Bereich SEA (Search Engine Advertising) unter Verwendung von GoogleAds Dienstleistungen werden folgende Unterstützungsleistungen durch den FG erbracht:

a) Google Anzeigen Erstellung und Optimierung regional / saisonal
b) Definition der Keywords sowie Optimierung der Suchbegriffe
c) Fortlaufende Steuerung, Messung und Optimierung der Online Kampagne
d) monatliche Erfolgskontrolle und Darstellung der Kampagnenergebnisse
e) monatliche Auswertungen: Standort Kosten, Impressionen, Klicks, CTR, Leeds (InboundCalls)

2.2 Der FG erbringt die vorbenannten Leistungen auf der Grundlage seiner vielfältigen Erfahrungen mit SEA–Maßnahmen im Rahmen der Online-Marketingaktivitäten des hairfree Systems und seiner Franchisepartner nach seinem Ermessen, bestem Wissen und mit der Sorgfalt eines ordentlichen Kaufmanns. Die Parteien sind sich einig und der FP nimmt zur Kenntnis, dass ein konkreter Erfolg solcher SEA Maßnahmen naturgemäß nicht erwartet werden kann und daher auch nicht geschuldet ist.

3. Mitwirkungspflichten des FP

3.1 Der FP stellt dem FG zum Zwecke der Erbringung der Dienstleistungen die Zugangsdaten zu dem von Google Ireland Ltd. zur Verfügung gestellten Nutzerkonto zur Verfügung. Dies in der Weise, dass dem FG die entsprechenden Funktionen zur Gestaltung von Werbeanzeigen und Kampagnen, deren Beauftragung und Auswertung im Auftrag des FP unmittelbar und vollumfänglich zur Nutzung zur Verfügung stehen. Die Bereitstellung des Zugangs ist Voraussetzung für die Erbringung der Unterstützungsleistungen durch den FG.

3.2 Der FP bevollmächtigt den FG zum Zwecke der Erbringung der in Ziffer 2 genannten Dienstleistungen, unter Verwendung der Zugangsdaten im Namen und für Rechnung des FP sämtliche Funktionen des Nutzerkontos des FP zu nutzen, insbesondere Anzeigen und Kampagnen zur gestalten, zu beauftragen und auszuwerten.

3.3 Der FP hat die Pflicht, alle im Übrigen erforderlichen Mitwirkungshandlungen (insb. Informationspflichten) zu erbringen, die die Erfüllung der vereinbarten Dienstleistungen ermöglichen. Der FP ist für eventuell erforderliche Recherchearbeiten selbst verantwortlich.

3.4 Für etwaige erforderliche Datensicherungen der im Nutzerkonto des FP verfügbaren Daten oder der seitens des FG zur Verfügung gestellten Daten ist ausschließlich der FP verantwortlich.

4. Vergütung

4.1 Der FP zahlt an den FG für die Erbringung der vertragsgegenständlichen Leistungen eine Verwaltungsgebühr von monatlich 99,00 € zuzüglich gesetzlicher MwSt.

4.2 Mit Abschluss des Vertrages wird eine Initialisierungsgebühr in Höhe von 149,00 € zzgl. MwSt. erhoben.

5. Budget

5.1 Das Monatsbudget der für die Google-Ads Dienste von Google berechneten Kosten soll bei ca. _____ Euro netto liegen.

5.2 Die konkret entstehenden Kosten hängen je nach Google-Ads Produkt im Einzelfall vom konkreten weiteren Verlauf und Erfolg der Maßnahmen ab und sind daher bei Beauftragung von Anzeigen und Kampagnen im Einzelfall nicht exakt bestimmbar. Die Parteien sind sich einig, dass der FG die Planung und Beauftragung von Maßnahmen und Kampagnen nach besten Wissen an dem vorgenannten Budgetplanungen als grobe Richtschnur ausrichten wird, gewisse Über- oder Unterschreitungen des Budgetrahmens in einzelnen Monaten und im Jahresmittel im weiteren Verlauf des Maßnahmen jedoch nicht auszuschließen sind.

5.3. Das monatliche Budget soll über folgendes Bankkonto abgerechnet werden:
Die Abrechnung erfolgt direkt mit Google

Inhaber: _____

Bank: _____

IBAN: __

6. Vertragslaufzeit

6.1 Dieser Vertrag hat eine Laufzeit von 12 Monaten, beginnend mit Abschluss des Vertrages.

6.2 Der Vertrag verlängert sich automatisch um jeweils 12 Monate, sofern nicht innerhalb einer Frist von 3 Monaten vor Ablauf gekündigt wird.

6.3 Die ordentliche und außerordentliche Kündigung bedürfen zu ihrer Wirksamkeit der Schriftform und des Zugangs per Einschreiben.

6.4 Endet der sich auf diesen Standort beziehenden hairfree-Franchisevertrag, endet der vorliegende Vertrag automatisch, ohne dass es einer Kündigung bedarf (auflösende Bedingung).

7. Datenschutz

7.1 Die Einhaltung der Datenschutzrechtlichen Bestimmungen bei und im Zusammenhang mit der Inanspruchnahme der GoogleAds Dienste ist Aufgabe des FP. Der FP verpflichtet sich insoweit zur Einhaltung der datenschutzrechtlichen Bestimmungen und stellt den Abschluss etwaiger insoweit erforderlicher Vereinbarungen im Vertragsverhältnis mit Google im Einklang mit den Bestimmungen sicher (Auftragsverarbeitungsvereinbarung, Joint Controllership Vereinbarungen, etc.)

7.2 Der FG wird etwaige im Zusammenhang mit der Erbringung seiner vertragsgegenständlichen Dienstleistungen erlangte personenbezogene Daten des FP oder von Dritten ausschließlich im Rahmen dieses Vertrages und zur Erbringung der Dienstleistungen gegenüber dem FP und nicht für eigene Zwecke nutzen. Notwendige Grundlage ist eine zwischen den Parteien gesondert abzuschließende Vereinbarung zur Auftragsverarbeitung, die diesem Vertrag nebst der dortigen Anlage „Technische und Organisatorische Maßnahmen zum Datenschutz“ als Anlage beigefügt und gesondert zu unterzeichnen ist.

8. Haftung

Der FG haftet in Fällen des Vorsatzes oder der groben Fahrlässigkeit von dem FG oder eines Vertreters oder Erfüllungsgehilfen nach den gesetzlichen Bestimmungen. Im Übrigen haftet der FG nur wegen der Verletzung des Lebens, des Körpers oder der Gesundheit oder wegen der schuldhaften Verletzung wesentlicher Vertragspflichten. Der Schadensersatzanspruch für die Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen, vorhersehbaren Schaden begrenzt, wenn nicht zugleich ein Fall von S. 1 bzw. S. 2 dieses Absatzes vorliegt. Die Haftung nach dem Produkthaftungsgesetz bleibt von den vorstehenden Haftungsregelungen unberührt. Eine weitergehende Haftung des FG besteht nicht.

9. Allgemeine Bestimmungen

9.1 Mündliche Nebenabreden bestehen nicht. Änderungen und Ergänzungen bedürfen der Schriftform. Dies gilt auch für eine Vereinbarung, die das Schriftformerfordernis aufhebt.

9.2 Durch von dem Vertrag abweichendes Verhalten werden vereinbarte Rechte und Pflichten weder geändert oder aufgehoben, noch werden neue Rechte und Pflichten begründet.

9.3 Der FP darf nur mit unbestrittenen und/oder rechtskräftig festgestellten Forderungen gegenüber Forderungen des FG aufrechnen.

9.4 Allgemeine Geschäftsbedingungen des FP finden keine Anwendung.

9.5 Der Bestand und die Beendigung des vorliegenden Vertrages lässt den Bestand des Franchisevertrages unberührt.

9.6 Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

9.7 Erfüllungsort und Gerichtsstand ist der Sitz des FG.

Ort, Datum: Darmstadt, ...

Franchisegeber

Ort, Datum: .....

Franchisepartner

Auftragsverarbeitungsvereinbarung zum Servicevertrag „Onlinemarketing (SEA)“

Zwischen

hairfree GmbH Rheinstraße 19-21,
64283 Darmstadt
vertreten durch die Geschäftsführer Chris Kettern und Jens Hilbert
(nachfolgend kurz „Auftragsverarbeiter“ genannt)

und dem Franchisepartner

Betreiber/Inhaber: .....

Straße: .....

PLZ/Ort: .....
(Institutsadresse)

(nachstehend „Auftraggeber“ genannt)

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung
(1) Die Parteien sind über den Abschluss eines Hauptvertrages „Servicevertrag Onlinemarketing (SEA)“ miteinander vertraglich verbunden, der die Erbringung von Unterstützungsleistungen durch den Auftragsverarbeiter bei der Planung, Beauftragung und Auswertung von Maßnahmen des Suchmaschinenmarketings gegenüber dem Auftraggeber zum Gegenstand hat. Dieser Hauptvertrag bringt es mit sich, dass der Auftragsverarbeiter personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Aus diesem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.
(2) Die Dauer dieser Vereinbarung zur Auftragsverarbeitung richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen aus der hiesigen Vertragsurkunde nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit
(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist in diesem Rahmen für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.
(2) Die Weisungen werden anfänglich durch den Hauptvertrag und durch die Vereinbarung zur Auftragsverarbeitung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform an die vom Auftragsverarbeiter bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag oder in der Vereinbarung zur Auftragsverarbeitung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragsverarbeiters
(1) Der Auftragsverarbeiter darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 lit. a DSGVO vor. Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragsverarbeiter darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
(2) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der DSGVO genügen. Der Auftragsverarbeiter hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
Hinsichtlich der seitens des Auftragsverarbeiters getroffenen technischen und organisatorischen Maßnahmen wird auf die Anlage zu dieser Vereinbarung zur Auftragsverarbeitung Bezug genommen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
(3) Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragsverarbeiter tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragsverarbeiter, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
(4) Der Auftragsverarbeiter unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragsverarbeiter trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
(5) Der Auftragsverarbeiter nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Hauptvertrages anfallende Datenschutzfragen.
(6) Der Auftragsverarbeiter gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
(7) Der Auftragsverarbeiter berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.
(8) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so

trägt diese der Auftraggeber.

§ 4 Pflichten des Auftraggebers
(1) Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
(2) Der Auftraggeber nennt dem Auftragsverarbeiter den Ansprechpartner für im Rahmen des Hauptvertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen
Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragsverarbeiter, wird er die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragsverarbeiter leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten
(1) Der Auftragsverarbeiter weist dem Auftraggeber, auf Verlangen, die Einhaltung der in dieser Vereinbarung zur Auftragsverarbeitung niedergelegten Pflichten mit geeigneten Mitteln nach.
(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragsverarbeiter darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen, hat der Auftragsverarbeiter gegen diesen ein Einspruchsrecht.
(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Weitere Auftragsverarbeiter als Subunternehmer
(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber zustimmt.
(2) Der Auftraggeber stimmt zu, dass der Auftragsverarbeiter Subunternehmer hinzuzieht. Zwei Wochen vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragsverarbeiter den Auftraggeber, wobei sich diese Frist auf eine angemessene Frist verkürzt, sofern außergewöhnliche Umstände eintreten, die ein zweiwöchiges Zuwarten für die Auftragsverarbeiter unzumutbar machen. Der Auftraggeber kann der Änderung – innerhalb einer angemessen gesetzten Frist - nur aus wichtigem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als erteilt.
(3) Erteilt der Auftragsverarbeiter Aufträge an Subunternehmer, so obliegt es ihm, seine datenschutzrechtlichen Pflichten aus dieser Vereinbarung zur Auftragsverarbeitung auch dem Subunternehmer aufzuerlegen.

§ 8 Haftung
(1) Der Auftragsverarbeiter haftet – sofern der Hauptvertrag oder diese Vereinbarung zur Auftragsverarbeitung keine anderslautenden Regelungen treffen – gleich aus welchem Rechtsgrund nur für Vorsatz und grobe Fahrlässigkeit. Diese Haftungsbeschränkung gilt auch für seine Erfüllungs- und Verrichtungsgehilfen.
(2) Für leichte Fahrlässigkeit haftet der Auftragsverarbeiter nur bei der Verletzung vertragswesentlicher Pflichten. In diesem Fall ist jedoch die Haftung für mittelbare Schäden, Mangelfolgeschäden und entgangenen Gewinn ausgeschlossen. Die Haftung für positive Forderungsverletzung, Verschulden bei Vertragsschluss und aus unerlaubter Handlung ist außerdem auf den Ersatz des typischen, vorhersehbaren Schadens begrenzt.
(3) Die Haftungsbeschränken aus den Absätzen 2 und 3 gelten nicht für die Verletzung von Leben, Körper und Gesundheit.

§ 9 Schlussbestimmungen
(1) Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der Datenschutz-Grundverordnung liegen.
(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung, die auch in Textform erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsdatenverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
(4) Es gilt das Recht der Bundesrepublik Deutschland.

Darmstadt, den ....
Auftragsverarbeiter (hairfree GmbH)

Ort, Datum: .....
Auftraggeber (Franchisepartner)

Anlage zur Auftragsverarbeitungsvereinbarung zum Servicevertrag „Onlinemarketing (SEA)“
Technische und Organisatorische Maßnahmen des Auftragsverarbeiters zum Schutz personenbezogener Daten

Technisch-organisatorische Maßnahmen
der **hairfree GmbH**
Rheinstraße 19-21, 64283 Darmstadt
vertreten durch die Geschäftsführer Chris Kettern und Jens Hilbert

1.Vertraulichkeit der Daten (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, durch:
- elektronisches Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)

b) Zugangskontrolle
Keine unbefugte Systembenutzung, durch:
- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Schlüsselregelung (Schlüsselausgabe etc.)
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall bei allen mobilen Arbeitsplätzen

c) Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, durch:
- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste" reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

d) Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, durch:
- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträger
- Logische Kunden-/Auftraggebertrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
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;

2. Datenintegrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Über-tragung oder Transport, durch:
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- E-Mail-Verschlüsselung
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

b) Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumenten-Management;

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
- Virenschutz
- Firewall
- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
- Datenschutz-Management;
- Incident-Response-Management (IT Störungsmanagement);
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle: eindeutige Vertragsgestaltung und formalisiertes Auftragsmanagement
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten