profihost

Gemeinsam. Echt. Begeistert.

Vereinbarung zur Auftragsdatenverarbeitung

zwischen

Firmierung, Strasse + Nr, PLZ Sitz

ggf. Kunden-Nr.

- Verantwortlicher – nachstehend Auftraggeber genannt

und

Profihost AG, Expo Plaza 1, 30539 Hannover

- Auftragsverarbeiter – nachstehend Auftragnehmer genannt

Profihost AG
Expo Plaza 1 · 30539 Hannover
Telefon +49 511 5151 8181
Telefax +49 511 5151 8282
info@profihost.com
www.profihost.com

Commerzbank AG
BLZ 27040080 · Konto 6511646
Swift/BIC COBADEFFXXX
IBAN DE20270400800651164600
USt.-Ident.-Nr. DE813460827
Steuer-Nr. 2325 271 05518

Vorstand Cristoph Bluhm
Sebastian Bluhm
Stefan Priebe
Vorsitzender des Aufsichtsrats
Prof. Dr. iur. Winfried Huck
Amtsgericht Hannover · HRB 202350

1 Allgemeines

1.1 Der Auftragnehmer verarbeitet aufgrund des zwischen den Parteien geschlossenen Hauptvertrages personenbezogene Daten im Auftrag des Auftraggebers. Voraussetzung für die Verarbeitung von personenbezogenen Daten im Auftrag ist gemäß Art. 28 Abs. 2 DSGVO (Datenschutzgrundverordnung) ein Auftragsverarbeitungsvertrag, mithin dieser Vertrag, der die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung regelt.

1.2 Dieser Vertrag findet Anwendung auf alle Tätigkeiten, die mit dem o. g. Hauptvertrag im Zusammenhang stehen und bei denen Mitarbeiter, Vertreter oder Organe des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1.3 Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer 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 schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Falls ein Unterauftragnehmer beauftragt werden soll, gelten diese Anforderungen ebenfalls für diese.

1.4 Umfang, Art und Zweck der Datenerhebung-, -verarbeitung oder -nutzung

Weitere Einzelheiten zu Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung ergeben sich aus dem Hauptvertrag

1.5 Arten der Daten

Auswahl	Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:
☐	Stammdaten
☐	Adressdaten
☐	Kommunikationsdaten (z.B. Telefon, E-Mail)
☐	Termindaten
☐	Abrechnungsdaten
☐	Vertragsdaten
☐	Bankverbindungsdaten
☐	Planungsdaten
☐	Kundenhistorie
☐	Auskunftsangaben (z.B. von Auskunfteien)
☐	Sensible Daten (z.B. Gesundheitsdaten, Religionszugehörigkeit)
☐	Sonstige

1.5 Kreis der Betroffenen

☐ Mitarbeiter ☐ Kunden/Interessenten ☐ Abonnenten ☐ Handelsvertreter

☐ Rentner ☐ Angehörige ☐ Lieferanten/Dienstleister

☐ Kontaktpersonen

☐ Sonstige:

2 Rechte und Pflichten des Auftragnehmers

2.1 Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu den personenbezogenen Daten hat, dürfen diese personenbezogenen Daten ausschließlich im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

2.2 Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu den personenbezogenen Daten hat, dürfen diese personenbezogenen Daten ausschließlich im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber mitteilen.

2.3 Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung aller erforderlichen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 3 S. 2 lit.c iVm Art. 32 DSGVO und diese Maßnahmen zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Die zu treffenden Maßnahmen müssen ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme erreichen. 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 zu berücksichtigen. Das Ergebnis ist zu dokumentieren (vgl. Art. 28 Abs. 3 lit. C, 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO). Diese Maßnahmen werden diesem Vertrag als **Anlage 1** beigefügt. Da die technischen und rechtlichen Gegebenheiten Änderungen unterliegen, sind sich die Parteien bewusst, dass Änderungen an den Maßnahmen erforderlich sein können. Daher wird der Auftragnehmer die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren und anpassen. Dem Auftragnehmer ist es gestattet, alternative adäquate Maßnahmen umzusetzen. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

2.4 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldepflichten bei Datenschutzverletzungen, Datenschutz-Folgeabschätzungen oder vorheriger Konsultationen). Für

diese Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten sind, kann der Auftragnehmer eine Vergütung beanspruchen.

2.5 Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden (Art. 28 Abs. 3 S. 2 lit.b, 29, 32 Abs. 4 DSGVO.

2.6 Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten bestellt hat. Seine Kontaktdaten lauten: RA Daniel Rink, Rink Rechtsanwaltsgesellschaft mbH, Expo Plaza 1, 30539 Hannover

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

2.8 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei dem Verdacht von Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Auch wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber dem Auftragnehmer tätig wird, 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.

2.9 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 Personen gewährleistet wird.

2.10 Kopien 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.

2.11 Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer stellt sicher, dass Daten bzw. Datenträger nach Beendigung der Auftragsdatenverarbeitung an den Auftraggeber zurück oder datenschutzkonform vernichtet werden.

2.12 Nach Abschluss der vereinbarten Arbeiten oder zuvor nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrages sind sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Auftragsdatenverarbeitung stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung zu belegen.

2.13 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über die Beendigung der vereinbarten Arbeiten / der Leistungserfüllung hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Beendigung der vereinbarten Arbeiten / der Leistungserfüllung dem Auftraggeber übergeben.

3 Rechte und Pflichten des Auftraggebers

3.1 Der Auftraggeber hat jederzeit das Recht, ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Der Auftraggeber erteilt alle Aufträge schriftlich oder per E-Mail. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail bestätigen.

Weisungsbefugte Mitarbeiter des Auftraggebers werden im Rahmen des Hauptvertrages mitgeteilt.

3.2 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Erfüllung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

3.3 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.4 Dem Auftraggeber obliegen die sich aus der DSGVO resultierenden Informationspflichten.

3.5 Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen.

3.6 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durzuführen oder durch eine dritte Person 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. Das Kontrollrecht kann nicht durch Dritte wahrgenommen werden und findet seine Grenze bei Betriebs- oder Geschäftsgeheimnissen des Auftragnehmers. Das Ergebnis der Kontrolle wird durch den Auftraggeber jeweils dokumentiert. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

4 Unterauftragsverhältnisse

4.1 Der Auftragnehmer darf nur nach vorheriger ausdrücklicher schriftlicher Zustimmung Subunternehmen im Rahmen der in 1.1. konkretisierten Tätigkeiten beauftragen. Zum Vertragsschluss bestanden keine Subunternehmerverhältnisse. Der Auftraggeber stimmt der Beauftragung dieser genannten Subunternehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

Umfasst sind ausschließlich solche Unterauftragsverhältnisse, die sich auf die Erbringung der Hauptleistung beziehen. Ausgenommen sind Nebendienstleistungen (z.B. Telekommunikationsdienstleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice, Entsorgung von Datenträgern)

4.2 Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, so hat der Auftragnehmer den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, ob die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen eingehalten werden können. Insbesondere hat der Auftragnehmer vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat und einen betrieblichen Datenschutzbeauftragten bestellt hat, sofern dies erforderlich ist.

5 Laufzeit, Kündigung

5.1 Der Auftraggeber kann diese Vereinbarung zur Auftragsdatenvereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrags vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert.

5.2 Unabhängig von den vorstehenden Regelungen zu den Laufzeiten gelten die Verpflichtungen zum Datengeheimnis, die Geheimhaltungspflicht und vereinbarte Aufbewahrungsfristen über das Vertragsende hinaus.

6 Schlussbestimmungen

6.1 Sollten die 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. Der Auftragnehmer 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 Datenschutzgrundverordnung liegen.

6.2 **Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen**

6.3 Es bestehen keine Nebenabreden. Für Nebenabreden ist die Schriftform erforderlich. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

Auftragnehmer	**Auftraggeber**
Hannover, im März 2018	_____, den
	
Name: **Sebastian Bluhm, Vorstand**	Name:

Anlage 1 zum Auftragsverarbeitungsvertrag (Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO)

Der Auftragnehmer erklärt, dass er unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Sicherheitsmaßnahmen getroffen hat, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

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

a. Der Auftragnehmer verwehrt Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen sie personenbezogene Daten verarbeitet mit folgenden Maßnahmen (Zutrittskontrolle)

aa. Die **Räume** des Auftraggebers befinden sich: Expo Plaza 1, 30539 Hannover. Hierbei handelt es sich um ein ausschließlich geschäftlich genutztes Haus. Sämtliche Zugänge sind gegen den unbefugten Zutritt abgesichert:

- Die Außentüren sind mit manuellen (oder technischen) Schließsystemen ausgestattet und sind grundsätzlich verschlossen;
- Das Personal, sowie Dritte werden sorgfältig ausgewählt
- Die den Mitarbeitern zur Verfügung gestellten Schlüssel sind personengebunden identifizierbar und die Schlüsselausgabe ist quittiert;
- Besucher bewegen sich in den Räumlichkeiten ausschließlich in Begleitung eines Mitarbeiters;
- Diese Regelungen sind in Verfahren festgelegt.

bb. Darüber wurden für die **Rechenzentrumsflächen** folgende Maßnahmen getroffen:

- Der Zutritt zum Rechenzentrum ist nur autorisierten Personen gestaltet;
- Die Authentifizierung der autorisierten Personen erfolgt durch einen dreiteiligen Verfizierungsprozess (Telefonische Anmeldung mit Kennwort, Transponder und PIN). So wird gewährleistet, dass nur berechtigte Personen das Rechenzentrum betreten können.

- Das Zutrittskontrollsystem, sowie die vorhandenen Alarmanlagen sind über USV und eine Netzersatzanlage gegen Stromausfall gesichert
- Das Rechenzentrum wird regelmäßig innerhalb eines vorgegebenen Zeitfensters durch Personal begangen. Die zu prüfenden Punkte sind festgelegt. Bei Auffälligkeiten werden diese berichtet.

b. Der Auftragnehmer verhindert durch die nachfolgenden Maßnahmen, dass Datenverarbeitungsvorgänge von Unbefugten genutzt werden können (Zugangskontrolle)

Alle Arbeitsplatzsysteme sind vor unberechtigten Zugang geschützt. Dies erfolgt insbesondere dadurch, dass

- alle verwendeten Arbeitsplatzsysteme befinden sich hinter einer Firewall
- die Arbeitsplatzsysteme nach Inaktivität gesperrt werden
- die Arbeitsplatzsysteme über eine Zwei-Faktor Authentifizierung mit Hardware-Token verfügen
- Mitarbeiter arbeiten ausschließlich mit personalisierten Benutzerprofilen
- alle mobilen Datenträger (insbesondere Laptops) verschlüsselt sind

c. Der Auftragnehmer trägt Sorge dafür, dass die zur Benutzung eines Datenverarbeitungsprozesses Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass die personenbezogenen Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).

Die unerlaubten Zugriffe auf Datenverarbeitungsprozesse außerhalb eingeräumter Berechtigungen wird im Besonderen verhindert dadurch, dass die Tätigkeiten des Auftragnehmers protokolliert werden.

- dass die Tätigkeiten des Auftragnehmers protokolliert werden.
- Schutz durch Verschlüsselung besteht

d. Der Auftragnehmer trägt Sorge dafür, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Trennungskontrolle)

Die Trennungskontrolle obliegt dem Auftraggeber.

d. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Für die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten ist der Auftraggeber verantwortlich.

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

a. Dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass es überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist (Weitergabekontrolle)

Die unberechtigte Weitergabe personenbezogener Daten wird insbesondere hierdurch umgesetzt:

- Die Datenkommunikation wird verschlüsselt (z.B. VPN, SSL)
- Der Transport von E-Mails erfolgt grundsätzlich verschlüsselt
- Beim physischen Transport werden die Transportpersonen sorgfältig ausgewählt

b. Dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)

Diese Kontrolle erfolgt durch:

- Protokollierung von Eingaben (insbesondere durch Logfiles)
- Die Zugriffsrechte orientieren sich an der Erforderlichkeit für die Aufgabenerfüllung

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a. Dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

Der Auftragnehmer unterhält folgende Maßnahmen:

- Es besteht für alle Server, auf denen personenbezogene Daten gespeichert werden, eine unterbrechungsfreie Stromversorgung (USV)
- Serverräumlichkeiten sind in Brandabschnitte mit einzelnen Brandschutzeinrichtungen (Feuer- und Rauchmeldeanlagen, sowie Feuerlöscher) eingeteilt
- Klimaanlagen sind vorhanden
- Es besteht eine Richtlinie, wie Notfälle zu erkennen sind und wohin diese gemeldet werden müssen.

Für darüber hinausgehende Schutzmaßnahmen – insbesondere auf der Ebene des Betriebssystems – ist alleine der Auftraggeber verantwortlich. Der Auftragnehmer bietet entsprechende Optionen zur Sicherstellung durch den Abschluss von SLA- und Backup-Tarifen.

b. Dafür Sorge zu tragen, dass die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt ist.

Alle Systeme, welche für die Infrastruktur der Dienstleistung des Auftragnehmers relevant sind, werden redundant vorgehalten und überwacht . Für die Belastbarkeit der Systeme des Auftraggebers ist der Auftraggeber selbst verantwortlich. Es bestehen Schutzmaßnahmen, um DDOS Angriffe auf die Systeme des Auftraggebers zu verhindern.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a. Der Auftragnehmer hält ein Datenschutz-Management-System vor, welches laufend verbessert wird.

Dies umfasst unter anderem:

- Eine Datenschutzleitlinie der Unternehmensleitung
- Richtlinien zum Umgang mit personenbezogenen Daten und der zugehörigen IT für alle Mitarbeiter

- Verfahren die den konkreten Umgang mit personenbezogenen Daten regeln.
- Bestellung eines externen Datenschutzbeauftragten
- Regelmäßige Kontrolle durch den Datenschutzbeauftragten
- Regelmäßige Schulung und Aufklärung, um das Problembewusstsein zu fördern
- Gelegentliche unangekündigte Kontrollen, ob die Datenschutz- und Datensicherungsmaßnahmen eingehalten werden.

b. Der Auftragnehmer hat ein Incident Response Management umgesetzt

Dies umfasst unter anderem:

- Richtlinien für Mitarbeiter, wie mit möglichen Sicherheitsvorfällen umzugehen ist
- Verfahren, wie die verantwortliche Stelle mit festgestellten oder gemeldeten Sicherheitsvorfällen umzugehen hat, insbesondere, wann der Datenschutzbeauftragte und die Datenschutzbehörde zu involvieren ist.

c. Der Auftragnehmer trägt Sorge dafür, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden dürfen (Auftragskontrolle)

Dies wird erreicht durch:

- Sorgfältige Auswahl von Auftragsverarbeitern in Zusammenarbeit mit dem Datenschutzbeauftragten
- Detaillierte Regelung zum Auftragsverhältnis (insbesondere wirksame Kontroll- und Zugriffs- und Löschungsrechte)
- Regelmäßige Kontrollen durch den Datenschutzbeauftragten

Der Auftraggeber gewährleistet, dass eine Leistungserbringung in deutschen Rechenzentren und unter Beachtung des DSGVO erfolgt.