profihost

Gemeinsam. Echt. Begeistert.

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 Auftragnehmers 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

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

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