E-Commerce. Cloud. Hosting.

Vereinbarung zur Auftragsdatenvereinbarung im Rahmen von Wartung und Pflege von DV-Anlagen

zwischen

Profihost AG, Expo Plaza 1, 30539 Hannover

(nachfolgend AN – Auftragnehmer)

und

Firma _____ **Kunden-Nr.:** _____

(nachfolgend AG – Auftraggeber)

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem zwischen den Parteien geschlossenen Leistungsvertrag zur Bereitstellung von Hostinglösungen ergeben. Sie findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des AN oder durch den AN beauftragten Dritten mit personenbezogenen Daten des AG in Berührung kommen könnten. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Leistungsvertrages.

§ 1 Definitionen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

(2) Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch den AN im Auftrag des AG.

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

(3) Eine Weisung erfolgt regelmäßig durch die Beschreibung im Leistungsvertrag, sie kann von dem AG jederzeit bei Bedarf in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich und Verantwortlichkeit

Der AN übernimmt im Rahmen des zugrunde liegenden Leistungsvertrages die Wartung und Pflege von Datenverarbeitungsanlagen. Je nach Leistungsvertrag handelt es sich um die Wartung und Pflege einer Serverhostingumgebung (bei Managed-Server Produkten) oder die Wartung und Pflege eines Wirthostsystems bei virtuellen Servern (vroot Server). In diesem Zusammenhang kann technisch der Zugriff auf personenbezogene Daten des AG nicht ausgeschlossen werden. Die Verantwortlichkeit innerhalb des Kundenspeicherplatzes bzw. auf Kundenapplikationsebene liegt ausschließlich beim AG selbst, da der AN für diesen Bereich keine Wartung und Pflege der kundenspezifischen Daten übernimmt.

§ 3 Pflichten des Auftragsnehmers

(1) Der AN führt die Wartung und Pflege an Datenverarbeitungsanlagen für den AG durch. Die automatisierte Erhebung, Verarbeitung oder Nutzung von Daten im Auftrag ist nicht vertraglich vereinbart. Der AN kann technisch den Zugriff auf Daten des AG nicht ausschließen und sichert die Beachtung gesetzlichen Vorschriften zu.

(2) Der AN sichert in seinen Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen entsprechend § 9 Bundesdatenschutzgesetz zu. Insbesondere wird der AN seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten der AG vor Missbrauch und Verlust treffen, die den Forderungen des Bundesdatenschutzgesetzes entsprechen. Als Datenstandort wird ausdrücklich ein oder mehrere Rechenzentren in der Region Hannover (Deutschland) zugesichert.

Dies beinhaltet insbesondere die in der Anlage zu § 9 Satz 1 BDSG aufgeführten Technischen und Organisatorischen Sicherheitsmaßnahmen, welche in der Anlage „Technische und organisatorische Maßnahmen“ erläutert werden:

a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),

b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

c) dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

d) dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen,kopiert, verändert oder entfernt werden können, und dass Überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

e) 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),

f) dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

g) dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

h) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

(3) Der AN ist als Telekommunikationsanbieter bei der Bundesnetzagentur registriert und verfügt über ein abgenommenes Sicherheitskonzept.

(4) Der AN hat eine TÜV-Zertifizierung seiner Managed-Services durchgeführt, welche auch die Prüfung der datenschutzrechtlichen Vorschriften beinhaltete.

(5) Der AN führt ein entsprechendes Verfahrensverzeichnis zum Datenschutz und stellt dieses auf Antrag zur Verfügung.

(6) Der AN stellt sicher, dass die mit der Verarbeitung der Daten der AG befassten Mitarbeiter gemäß § 5 Bundesdatenschutzgesetz (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind.

(7) Der AN unterrichtet den AG unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des AG.

§ 5 Rechte und Pflichten des AG

(1) Der AG ist für die Einhaltung

(2) des Bundesdatenschutzgesetz (soweit es sich um eine nicht-öffentliche Stelle handelt) bzw.des jeweils einschlägigen Landesdatenschutzgesetzes (soweit es sich um eine öffentliche Stelle gem. § 2 Abs.2 BDSG handelt)

und die Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen allein verantwortlich.

(3) Der AG erteilt alle Aufträge oder Teilaufträge schriftlich oder in elektronischer Form. Der Verarbeitungsgegenstand darf nicht einseitig geändert werden.

(4) Der AG ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des AN vertraulich zu behandeln.

(5) Der AG legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(6) Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber,

(7) Der AN stellt den zeitlichen Aufwand, der im Zusammenhang mit der Kontrollfunktion nach § 7 des AG steht, gem. aktueller Preisliste (Entwicklerstundensatz) in Rechnung. Der AG stimmt der Kostenübername zu.

§ 6 Anfragen Betroffener an den Auftraggeber

Ist der AG aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet,

Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der AN den AG dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt:

- der AG hat den AN hierzu schriftlich aufgefordert und
- der AG erstattet dem AN die durch diese Unterstützung entstandenen Kosten.

§ 7 Kontrollrecht

Der AG kann sich nach Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zu Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen. Der AN verpflichtet sich, dem AG auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind.

§ 8 Subunternehmer

(1) Die Weitergabe von Aufträgen im Rahmen der in § 2 konkretisierten Tätigkeiten an Subunternehmer durch den AN bedarf der schriftlichen Zustimmung des AG.

§ 9 Schlussbestimmungen

(1) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(2) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wir die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(3) Für Nebenabreden ist die Schriftform erforderlich.

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

(5) Es gilt deutsches Recht.

_____	_____
Auftraggeber	Auftragnehmer

Anlage
Technische und organisatorische Sicherheitsmaßnahmen im Rahmen von Wartung und Pflege von DV-Anlagen

Zutrittskontrolle

Folgende Maßnahmen wurden etabliert, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit den personenbezogene Daten potentiell verarbeitet oder genutzt werden, zu verwehren:

(1) Büro:
Im Bürobereich der Profihost AG sind keine relevanten Datenverarbeitungsanlagen, nach den Beschreibungen dieser Vereinbarung, vorhanden.

(2) Rechenzentrum:
Der Zutritt zu den Rechenzentren wird durch den AN und den Betreiber es Rechenzentrums selbst geregelt. Folgende Maßnahmen sind etabliert:

- Alarmanlage und Sicherheitsfirma
- 24/7/365 Personal vor Ort
- Videoüberwachung relevanter Bereiche
- Personenkontrolle beim Empfang
- Chipkarten-/Transponder-Schließsystem
- Protokollierung von Besuchern und RZ Zugängen

Zugangskontrolle

Folgende Maßnahmen wurden etabliert, um Unbefugten die Nutzung von Datenverarbeitungsanlagen, mit den personenbezogene Daten potentiell verarbeitet oder genutzt werden, zu verwehren:

(1) Büro:
Im Bürobereich der Profihost AG sind keine relevanten Datenverarbeitungsanlagen, nach den Beschreibungen dieser Vereinbarung, vorhanden. Es besteht jedoch die Möglichkeit, dass über Computersysteme im Büro ein Zugang zu entsprechenden Serversystemen im RZ erfolgen kann. Daher sind folgende Maßnahmen etabliert:

- Verschlüsselung der Clientsysteme
- Zugang nur mit individuellen Benutzerkennungen
- Nutzung von abgesicherten internen Datenleitungen für den Zugriff auf RZ-Systeme

(2) Rechenzentrum:
Folgende Maßnahmen sind etabliert:

- Maßnahmen gem. Punkt Zutrittskontrolle
- Abgeschlossene Serverschränke
- Zugriff nur mit Benutzerkennung
- Einsatz von VPN-Technologie
- Zugriff mittels SSH2 inkl. individuellem Key

Zugriffskontrolle

Folgende Maßnahmen wurden etabliert, welche gewährleisten sollen, dass die Benutzung von DV-Anlagen nur durch berechtigte Nutzer erfolgt und somit eventuelle personenbezogene Daten nicht durch unbefugte Personen gelesen, verändert, kopiert oder entfernt werden können:

Folgende Maßnahmen sind etabliert:

- Berechtigungskonzept für den Zugriff
- Protokollierung durch die serverseitig vorhandenen Logmethoden
- Sicherstellung der ordnungsgemäßen Löschung von Datenträgern
- Sichere Aufbewahrung von Datenträgern
- Einsatz von zertifizierten Unternehmen für die Akten- und Datenträgervernichtung inkl. Protokollierung

Weitergabekontrolle

Folgende Maßnahmen sind etabliert:

- Möglichkeit zur Nutzung von VPN bzw. IPSec Verbindungen

Eingabekontrolle

Folgende Maßnahmen sind etabliert:

- Nutzung der serverseitig möglichen Logmethoden zur Erfassung von Veränderungen
- Nutzung eines Berechtigungskonzeptes

Auftragskontrolle

Bei der Wartung von Pflege von DV-Anlagen erfolgt keine direkte Auftragsdatenverarbeitung, sondern besteht potentiell eine technische Zugriffsmöglichkeit auf eventuelle personenbezogene Daten.

Folgende Maßnahmen sind etabliert:

- Verpflichtung der Mitarbeiter auf das Datengeheimnis gem. BDSG
- Datenschutzbeauftragter bestellt
- Möglichkeit der Kontrolle durch prüfende Drittunternehmen oder den AG

Verfügbarkeitskontrolle

Folgende Maßnahmen im Rechenzentrum sind etabliert:

- Alarmanlage
- Unterbrechungsfreie Stromversorgung (USV)
- Redundante Klimaanlagen
- Feuer- und Brandmeldeanlagen
- Automatische Feuerlöschanlage (Stickstoff)
- Notstromaggregat
- Möglichkeit der Etablierung von Backup- und Recoverykonzepten gem. Bestellung des AG

Trennungsgebot

Folgende Maßnahmen im Rechenzentrum sind etabliert:

- Maßnahmen können nur applikationsseitig etabliert werden und fallen nicht in die Aufgabe es AN.