Verantwortliche Stelle:

Hostway Deutschland GmbH
Am Mittelfede 29
30519 Hannover
- nachfolgend HWD genannt -

vertreten durch die Geschäftsführer:
Dr. Achilleas Anastasiadis und Ilja Kassühlke

Präambel
HWD ist regelmäßig im Rahmen der Auftragsdatenverarbeitung als datenverarbeitendes Unternehmen tätig. Aufgrund dieser Tätigkeiten unterliegt HWD gemäß Bundesdatenschutzgesetz (BDSG) speziellen Verpflichtungen.

1. Datenschutzkonzept
HWD unterwirft sich dem Grundsatz der Datensparsamkeit und erhebt, verarbeitet oder nutzt so wenig personenbezogene Daten wie möglich. Personenbezogene Daten werden erhoben, um Mitarbeiter, Auftraggeber, Mittler, Lieferanten, Interessenten und Kunden in der EDV zu erfassen um die tägliche Zusammenarbeit so effizient wie möglich zu gestalten. Interessentendaten werden erhoben, um potenzielle Kunden im gesetzlich zugelassenen Rahmen werblich anzusprechen. Sofern wir Kenntnis darüber erlangen, dass einzelne personenbezogene Datensätze ungültig geworden sind, entscheiden wir im Einzelfall, ob die Daten gelöscht werden oder ob ein Kennzeichen gesetzt wird, dass den Datensatz als nicht mehr gültig charakterisiert. Im Kundenauftrag verarbeitete oder genutzte Daten werden in Absprache mit unseren Kunden nach dem gleichen Grundsatz behandelt. Überlassene Adressdaten werden ausschließlich zur auftragsgemäßen Durchführung der beauftragten Leistung verwendet.

Sofern Betroffene HWD um Auskunft über die Herkunft der Datensätze bitten, wird HWD im Rahmen seiner Möglichkeiten entsprechende Auskünfte erteilen Auftraggeber bzw. sonstige relevante Beteiligte werden darauf hingewiesen, dass Widersprüchen von Betroffenen zur Nutzung von personenbezogenen Daten für Werbezwecke zu entsprechen ist.

Die Beteiligten werden darauf hingewiesen, dass eine Lieferung von Adressen nur verschlüsselt erfolgen soll und der Versender bei unverschlüsselter Übermittlung haftet.

Die Lieferung von personenbezogenen Daten außerhalb des EWR/EU – Bereiches erfolgt nur nach Sicherstellung eines entsprechenden Datenschutzniveaus.

2. Technische und organisatorische Maßnahmen

Unternehmen, die personenbezogene Daten erheben, verarbeiten oder nutzen, müssen technische und organisatorische Maßnahmen treffen, um den Bestimmungen des BDSG insbesondere dem §9 und der Anlage zu §9 zu entsprechen. HWD erfüllt diesen Anspruch durch folgende Maßnahmen:

a. Zutrittskontrolle

Die Zugänge zum Gebäude sind stets geschlossen und können von außen nur mit Sicherheitsschlüsseln geöffnet werden. Der Zugang zum Gebäude wird rund um die Uhr durch Mitarbeiter am zentralen Empfang überwacht und jeder Mitarbeiter und Lieferant muss sich am Empfang anmelden. Besucher werden von einer Mitarbeiterin oder einem Mitarbeiter persönlich am Empfang abgeholt. Organisatorisch ist geregelt, dass Fremde sich im Gebäude niemals allein aufhalten oder frei bewegen dürfen. Außerhalb der Arbeitszeiten erfolgt die Überwachung der Räumlichkeiten durch eine Alarmanlage gemäß VDENorm. Meldungen der Anlage werden durch einen Sicherheitsdienst überwacht und nach einem dokumentierten Interventionsplan verfolgt. Bei wichtigen Räumlichkeiten besteht eine zusätzliche Videoüberwachung. Diese ist insbesondere in allen Räumlichkeiten des Rechenzentrums vorhanden und wird durch zusätzliche Bewegungssensoren unterstützt.

b. Zugangskontrolle zu EDV-Systemen

Unbefugten wird der Zugang zu Datenverarbeitungssystemen nicht gewährt. Der Zugang über Außenschnittstellen zu unseren EDV-Systemen ist durch eine Firewall geschützt. Öffentlich erreichbare Systeme, wie E-Mail oder Internetzugang werden über entsprechende Trennungen vom internen Netz gesichert (DMZ). Sämtliche PCSysteme sind passwortgeschützt. Passwörter müssen hohen Ansprüchen genügen und werden regelmäßig zwangsweise erneuert. Die Detaillierung der Zugriffsberechtigungen zu dem Equipment des Vertragspartners liegt im Verantwortungsbereich des Auftraggebers.

c. Zugriffskontrolle

Der Zugriff auf Netzwerkverzeichnisse, in denen personenbezogene Daten gespeichert werden, ist auf die jeweiligen Personen beschränkt, die mit den Aufträgen beschäftigt sind, für die solche Daten verwendet werden sollen. Diese Personen müssen sich gegenüber dem System identifizieren. Insbesondere Produktionssysteme haben ausschließlich zu einem einzigen, für sie eingerichteten Netzwerkverzeichnis Zugang. Auf diesen Verzeichnissen werden Daten nur so lange gespeichert, wie sie für den unmittelbaren Auftragsprozess benötigt werden.

d. Weitergabekontrolle
Es wird Sorge getragen, 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.

Der Versand personenbezogener Daten erfolgt ausschließlich im gesetzlich vorgesehenen Rahmen. Der Datenaustausch erfolgt verschlüsselt. Die Übertragungswege sind passwortgeschützt. Mobile Datenträger mit personenbezogenen Daten werden nur in gesicherten Räumen gehalten, bei Nichtverwendung im Tresor. Daten, die für eine Auftragsdurchführung nicht mehr benötigt werden, wie z.B. gesperrte Daten, werden in einem separiertem zugriffsgeschützten Speicherbereich abgelegt. Datenträger/Hardware werden nur durch entsprechend verpflichtete und zertifizierte Unternehmen repariert oder entsorgt. Gleiches gilt für die Entsorgung von Daten auf Papier.

e. Eingabekontrolle
Die Dokumentation des Zugriffs auf einzelne Daten unterliegt dem Auftraggeber.

f. Auftragskontrolle
Die Dokumentation des Zugriffs auf die Auftragskontrolle unterliegt dem Auftraggeber.

g. Verfügbarkeitskontrolle
Unsere EDV-Systeme sind durch RAID-Systeme vor Datenverlust geschützt. Tägliche Datensicherungen garantieren, dass bei Verlust der Funktionsfähigkeit von EDV-Systemen keine Daten verloren gehen. Für vom Auftraggeber gemietete EDVSysteme oder vom Auftraggeber eingestellte EDV-Systeme ist der Auftraggeber verantwortlich. Um das Ausmaß möglicher Brandschäden zu minimieren, ist unser Unternehmen mit einer Brandmeldeanlage ausgestattet. Meldungen der Anlage werden durch einen Sicherheitsdienst überwacht und nach einem dokumentierten Interventionsplan verfolgt. Die Klimaanlagen sind N+1 vorhanden und werden durch ein Notstromaggregat versorgt.

h. Getrennte Verarbeitung personenbezogener Daten
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhoben Daten getrennt verarbeitet werden können, obliegt dem Auftraggeber.

i. Löschung personenbezogener Daten Dritter
Eine Regelung zum Löschen personenbezogener Daten und von Zugriffsschlüsseln, mit denen ggf. auf personenbezogene Daten zugegriffen werden kann, ist mit den Auftraggebern auftragsbezogen zu regeln.

j. Unterbeauftragung
Sofern sonstige Dienstleister bzw. Unterauftragsnehmer von HWD beauftragt werden und die Beauftragung den Umgang mit personenbezogenen Daten erforderlich macht, ist es unerlässlich, dass seitens des beauftragten Unternehmens eine unterzeichnete Datenschutzverpflichtungserklärung nach BDSG vorliegt. Sofern die Erteilung solcher Auftragsverhältnisse die Zustimmung eines Dritten erfordert, wird HWD diese Zustimmung über den Auftraggeber einholen.

k. Verpflichtung der Mitarbeiterinnen und Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Bestimmungen
Sämtliche Mitarbeiterinnen und Mitarbeiter werden in jährlichen Schulungen auf ihre Verpflichtungen zur Wahrung des Datengeheimnisses hingewiesen und bezeugen dies durch ihre Unterschrift. Ihnen wird das Merkblatt “Datenschutz” ausgehändigt. Die Unterweisung erfolgt insbesondere zu den Grundsätzen des Datenschutzes nach BDSG (insbesondere die Voraussetzungen der Auftragsdatenverarbeitung), der Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse, dem sorgfältigen Umgang mit Datenträgern und Dateien und dem Fernmeldegeheimnisses.

Hostway Deutschland GmbH

- Die Geschäftsführung -

Hostway Deutschland GmbH
Am Mittelfelde 29
30519 Hannover

Telefon: +49 (0) 511 71260-0
Telefax: +49 (0) 511 71260-199
E-Mail: info@hostway.de

Geschäftsführer
Cord Bansemer
Dr. Achilleas Anastasiadis

Bankverbindung
Commerzbank AG
Konto: 0 111 085 800
BLZ: 250 800 20

Angaben zur Gesellschaft
Sitz: Hannover
HRB 202097
Ust-IdNr.: DE204915504