# DATENSCHUTZ gemäß § 9 BDSG

## Kontrollziele gemäß Anlage § 9 BDSG und Beschreibung der technischen und/oder organisatorischen Sicherungsmaßnahmen

| **Kontrollziele**<br>bezüglich Umgang mit personenbezogenen Daten | **Maßnahmen** |
|---|---|
| **1.**<br>**Zutrittskontrolle**<br>(Räume und Gebäude)<br>*Zielbeschreibung:* Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden. | **Standort Köln, Welserstraße 14**<br>- Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen<br>- Es bestehen Sichtkontrollen und ein Besucherbuch am Empfang<br>- Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes<br>- Im Alarmfall werden die für das Gebäude verantwortlichen Mitarbeiter automatisch alarmiert<br>- Zusätzlich ist das Gebäude 24/7 durch eigenes Personal besetzt. Diesem Personal werden die Alarmmeldungen angezeigt<br>- Es besteht eine restriktive Zutrittsregelung<br><br>**Standort Köln, Hansestraße 109**<br>- Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen<br>- Es bestehen Sichtkontrollen und ein Besucherbuch am Empfang<br>- Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes<br>- Im Alarmfall werden die für das Gebäude verantwortlichen Mitarbeiter automatisch alarmiert<br>- Dem im Hauptgebäude 24/7 befindlichen Personal werden die Alarmmeldungen angezeigt<br>- Es besteht eine restriktive Zutrittsregelung<br><br>**Standort Straßburg:**<br>-Sicherheitsbereich mit Eingangskontrolle<br>-eingezäuntes Gelände inkl. Videoüberwachung<br>-Regelmäßige Kontrollgänge durch das Sicherheitspersonal<br>-Zutrittskontrollsystem mit Chipkarten. |

| Kontrollziele<br>bezüglich Umgang mit personenbezogenen Daten | Maßnahmen |
|---|---|
| **2.**<br>**Zugangskontrolle**<br>(IT-Systeme, Anwendungen)<br>*Zielbeschreibung:* Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. | **Allgemein**<br>- Die Host Europe vermietet die Datenverarbeitungsanlage an den Kunden<br>- Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung<br>- Der Kunde entscheidet allein und ausschließlich darüber, welche personenbezogenen Daten in welcher Weise verarbeitetet werden („Herr der Daten“)<br>- Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Kunden erstellt und eingesetzt<br>- Host Europe sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Buch darüber, welche Anlagen durch den Kunden in welchem Umfang genutzt werden<br>- Die Datenverarbeitung selbst erfolgt durch den Kunden. Host Europe hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge im Sinne des § 3 Abs. 4 BDSG<br><br>**Mass Hosting, unmanaged-Systeme**<br>- Die konkreten Verarbeitungsvorgänge sind Host Europe auch nicht bekannt. Insofern obliegt es dem Kunden durch softwaretechnische Gestaltungen dafür Sorge zu tragen, dass die Datenverarbeitungssysteme von Unbefugten nicht genutzt werden können.<br><br>**Mass Hosting, managed-Systeme**<br>- Bei managed-Produkten haben nur wenige ausgewählte Administratoren Zugang zum Server. Jeder dieser Administratoren hat eine individuelle Benutzerkennung und erhält ausschließlich über das Host Europe-Netzwerk Zugang. Es bestehen Regelungen zum Schutz und zur regelmäßigen Änderung der Zugangspasswörter/-Schlüssel.<br><br>**Managed Hosting, unmanaged-Systeme**<br>- Die konkreten Verarbeitungsvorgänge sind Host Europe auch nicht bekannt. Insofern obliegt es dem Kunden durch softwaretechnische Gestaltungen dafür Sorge zu tragen, dass die Datenverarbeitungssysteme von Unbefugten nicht genutzt werden können.<br><br>**Managed Hosting, managed-Systeme**<br>- Bei managed-Produkten haben nur wenige ausgewählte Administratoren Zugang zum Server. Jeder dieser Administratoren hat eine individuelle Benutzerkennung und erhält ausschließlich über das Host Europe-Netzwerk |

| Kontrollziele<br>bezüglich Umgang mit personenbezogenen Daten | Maßnahmen |
|---|---|
| | Zugang. Es bestehen Regelungen zum Schutz und zur regelmäßigen Änderung der Zugangspasswörter/-Schlüssel. |
| **3.**<br>**Zugriffskontrolle**<br>(auf Daten)<br>*Zielbeschreibung:* Es ist zu gewährleisten, 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. | **Allgemein**<br>- Wie bereits oben unter Zugang ausgeführt, erfolgt die Datenverarbeitung durch den Kunden. Die Host Europe hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass der Zugriff auf Daten ausschließlich durch den Kunden geregelt werden kann.<br>- Alle Mitarbeiter der Host Europe sind gemäß BDSG zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet und entsprechend geschult<br><br>**Mass Hosting, unmanaged-Systeme**<br>- Der Kunde hat die Möglichkeit, die Host Europe für bestimmte Administrationsaufgaben zu beauftragen. Dazu stellt der Kunde für alle „unmanaged-Produkte“ der Host Europe GmbH temporär einen Zugang zur Verfügung und sorgt nach Abschluss der Arbeiten für die Deaktivierung des Zugangs.<br><br>**Mass Hosting, managed-Systeme**<br>- Der Kunde hat die Möglichkeit, die Host Europe für bestimmte Administrationsaufgaben zu beauftragen und Host Europe sorgt für das Monitoring und die Wartung der Systeme. Die Administrationszugriffe werden adäquat protokolliert.<br><br>**Managed Hosting, unmanaged-Systeme**<br>- Der Kunde hat die Möglichkeit, die Host Europe für bestimmte Administrationsaufgaben zu beauftragen. Dazu stellt der Kunde für alle „unmanaged-Produkte“ der Host Europe temporär einen Zugang zur Verfügung und sorgt nach Abschluss der Arbeiten für die Deaktivierung des Zugangs.<br><br>**Managed Hosting, managed-Systeme**<br>- Der Kunde hat die Möglichkeit, die Host Europe für bestimmte Administrationsaufgaben zu beauftragen und Host Europe sorgt für das Monitoring und die Wartung der Systeme. Die Administrationszugriffe werden adäquat protokolliert. |
| **4.**<br>**Eingabekontrolle**<br>(in Datenverarbeitungssysteme)<br>*Zielbeschreibung:* Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem | **Mass Hosting, unmanaged-Systeme**<br>- Wie bereits oben ausgeführt, erfolgt die Datenverarbeitung durch den Kunden. Host Europe hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass die |

| Kontrollziele<br>bezüglich Umgang mit personenbezogenen Daten | Maßnahmen |
|---|---|
| personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden. | Eingabekontrolle der Daten ausschließlich durch den Kunden umgesetzt werden kann.<br><br>**Mass Hosting, managed-Systeme**<br>- Wie bereits oben ausgeführt, erfolgt die Datenverarbeitung durch den Kunden. Host Europe hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass die Eingabekontrolle der Daten ausschließlich durch den Kunden umgesetzt werden kann. Bei Änderungen durch Host Europe werden die Administrationszugriffe adäquat protokolliert.<br><br>**Managed Hosting, unmanaged-Systeme**<br>- Wie bereits oben ausgeführt, erfolgt die Datenverarbeitung durch den Kunden. Host Europe hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass die Eingabekontrolle der Daten ausschließlich durch den Kunden umgesetzt werden kann.<br><br>**Managed Hosting, managed-Systeme**<br>- Wie bereits oben ausgeführt, erfolgt die Datenverarbeitung durch den Kunden. Host Europe hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass die Eingabekontrolle der Daten ausschließlich durch den Kunden umgesetzt werden kann. Bei Änderungen durch Host Europe werden die Administrationszugriffe adäquat protokolliert. |
| **5.**<br>**Weitergabekontrolle**<br>(von Daten)<br>*Zielbeschreibung:* Es ist zu gewährleisten, 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. | **Allgemein**<br>- Eine technisch notwendige Zugriffsmöglichkeit auf alle übertragenen Daten besteht im Rahmen der Verwaltung der Netzwerkhardware (Router, Switches). Dieser Zugriff ist auf die Mitarbeiter des Teams Network beschränkt und dient ausschließlich zur Gewährleistung des technischen Betriebes. Eine Selektierung personenbezogener Daten ist dabei nicht möglich. Dem Kunden obliegt es durch eine Verschlüsselung, z.B. SSL dafür zu sorgen, dass die übertragenen Daten nicht lesbar sind.<br><br>**Mass Hosting, unmanaged-Systeme**<br>- Die Host Europe hat bei unmanaged Produkten keinen Zugriff auf durch den Kunden verarbeitete personenbezogene Daten – außer der Kunde beauftragt die Host Europe mit administrativen Aufgaben auf seinen Systemen. Bei Änderungen durch Host Europe werden die Administrationszugriffe adäquat protokolliert. |

| Kontrollziele<br>bezüglich Umgang mit personenbezogenen Daten | Maßnahmen |
|---|---|
| | Der Zugriff erfolgt durch geschulte und auf das Datengeheimnis verpflichtete Administratoren. Sämtliche administrative Aufgaben finden über gesicherte Wege, wie bspw. SSL-verschlüsselt, statt.<br><br>**Mass Hosting, managed-Systeme**<br>- Bei managed-Produkten verfügt die Host Europe über organisatorische Maßnahmen, welche den Zugriff auf die Systeme regelt um den Systembetrieb sicherzustellen. Sämtliche administrative Aufgaben finden über gesicherte Wege, wie bspw. SSL-verschlüsselt, statt. Der Zugriff erfolgt durch geschulte und auf das Datengeheimnis verpflichtete Administratoren. Die Anzahl der Mitarbeiter, werden von der Host Europe möglichst gering gehalten. Bei Änderungen durch Host Europe werden die Administrationszugriffe adäquat protokolliert.<br><br>**Managed Hosting, unmanaged-Systeme**<br>- Die Host Europe hat bei unmanaged Produkten keinen Zugriff auf durch den Kunden verarbeitete personenbezogene Daten – außer der Kunde beauftragt die Host Europe mit administrativen Aufgaben auf seinen Systemen. Bei Änderungen durch Host Europe werden die Administrationszugriffe adäquat protokolliert. Der Zugriff erfolgt durch geschulte und auf das Datengeheimnis verpflichtete Administratoren. Sämtliche administrative Aufgaben finden über gesicherte Wege, wie bspw. SSL-verschlüsselt, statt.<br><br>**Managed Hosting, managed-Systeme**<br>- Bei managed-Produkten verfügt die Host Europe über organisatorische Maßnahmen, welche den Zugriff auf die Systeme regelt um den Systembetrieb sicherzustellen. Sämtliche administrative Aufgaben finden über gesicherte Wege, wie bspw. SSL-verschlüsselt, statt. Der Zugriff erfolgt durch geschulte und auf das Datengeheimnis verpflichtete Administratoren. Die Anzahl der Mitarbeiter, werden von der Host Europe möglichst gering gehalten. Bei Änderungen durch Host Europe werden die Administrationszugriffe adäquat protokolliert. |
| **6.**<br>**Verfügbarkeitskontrolle**<br>(von Daten)<br>*Zielbeschreibung:* Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. | **Allgemein**<br>- Die autonome Stromversorgung der Data Center erfolgt über eine eigene Trafostation. Die Stromversorgung und Netzersatzanlage garantieren höchste Ausfallsicherheit.<br>- Jedes Serverrack wird über mindestens zwei separate Stromzuführungen versorgt, die je einzeln mit mindestens 16 Ampere abgesichert sind. |

| Kontrollziele<br>bezüglich Umgang mit personenbezogenen Daten | Maßnahmen |
|---|---|
| | - Die unmittelbare Stromversorgung des Servers ist typenabhänig, so dass bei der Verwendung entsprechender Typen zusätzlich eine redundante Stromversorgung über ein redundantes Netzteil (2 Netzteile) gewährleistet ist.<br>- Der gesamte Energieverbrauch der Data Center wird über eine unterbrechungsfreie Stromversorgung (USV) sichergestellt. Im Falle eines Stromausfalls garantiert die USV-Anlage eine unterbrechungsfreie Umschaltung auf eines der Notstrom-Dieselaggregate. Daneben filtert die USV vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes.<br>- Eine leistungsstarke Netzersatzanlage (Dieselaggregat) versorgt bei Stromausfall das gesamte jeweilige Data Center und die Kühlsysteme mit konstanter Energie.<br>- Für Backups wird ein dediziertes Backup-LAN oder ein über VLAN logisch getrenntes Netzwerk verwendet.<br><br>**Standort Köln, Welserstraße 14**<br>- Der Kraftstoffvorrat ist für mindestens 24 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich.<br>- Ein flächendeckendes Wasser- und Brandfrühwarnsystem (VESDA) reagiert bereits bei geringer Überschreitung definierter Grenzwerte, um größere Schäden zu verhindern.<br>- Die Brandmeldeanlage verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr.<br>- Die Gebäudeaußenhaut ist zudem mittels Überspannungsschutz gegen Blitzschlag abgesichert.<br>- Sollte es wider Erwarten zu einer Rauchentwicklung oder gar einem Brand kommen, flutet die aufwendige Feuerbekämpfungsanlage mit 150fachen Luftdruck das Data Center innerhalb von nur 60 Sekunden vollständig mit dem Löschgas Argon. Hierbei bleibt das Equipment im Data Center vollkommen unbeschädigt.<br>- Klimaanlage<br>- Geräte zur Überwachung der Temperatur und Feuchtigkeit in den Data Centern<br><br>**Standort Köln, Hansestraße 109**<br>- Der Kraftstoffvorrat ist für mindestens 16 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich.<br>- Ein flächendeckendes Wasser- und Brandfrühwarnsystem (VESDA) reagiert bereits bei geringer Überschreitung definierter Grenzwerte, um größere Schäden zu verhindern.<br>- Die Brandmeldeanlage verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr. |

| Kontrollziele<br>bezüglich Umgang mit personenbezogenen Daten | Maßnahmen |
|---|---|
| | - Die Gebäudeaußenhaut ist zudem mittels Überspannungsschutz gegen Blitzschlag abgesichert.<br>- Sollte es wider Erwarten zu einer Rauchentwicklung oder gar einem Brand kommen, flutet die aufwendige Feuerbekämpfungsanlage mit 150fachen Luftdruck das Data Center innerhalb von nur 60 Sekunden vollständig mit dem Löschgas Argon. Hierbei bleibt das Equipment im Data Center vollkommen unbeschädigt.<br>- Klimaanlage<br>- Geräte zur Überwachung der Temperatur und Feuchtigkeit in den Data Centern<br><br>**Standort Straßburg:**<br>In dem Rechenzentrum in Straßburg besteht eine unterbrechungsfreie Stromversorgung (USV) sowie ein Überspannungsschutz. Ebenso ist ein Branderkennungs- und Frühwarnsystem implementiert. Das Löschsystem ist auf eine möglichst zerstörungsfreie Brandbekämpfung ausgelegt.<br><br>**Standort Falkenstein, Am Datacenter Park 1**<br>- Der Kraftstoffvorrat ist für mindestens 24 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich.<br>- Die Brandmeldeanlage verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr.<br><br>**Mass Hosting, managed-Systeme**<br>- Bei managed-Produkten ist die Host Europe GmbH für das gesamte Backup verantwortlich. Die Vorhaltezeit beträgt mindestens 14 Tage.<br>- Host Europe gewährleistet bei Webpack-Produkten ein OffSite-Backup in ein anderes Data Center.<br>- Bei den Produkten ePages, OpenExchange und Webbuilder findet ausschließlich ein lokales Backup im Produktivrechenzentrum statt.<br><br>**Managed Hosting, managed-Systeme**<br>- Host Europe ist für die Sicherung der Konfigurationsdaten verantwortlich, auf die der Kunde keinen Zugriff hat. Für die Erstellung einer Datensicherung der eigenen Daten ist der Kunde selbst verantwortlich. Host Europe bietet als Option technische Einrichtungen an, mit Hilfe derer der Kunde eine Kopie seiner Daten anlegen und speichern kann.<br>- Je nach gebuchter Leistung findet das Backup in einem anderen Brandabschnitt oder einem anderen Data Center statt. |

| Kontrollziele<br>bezüglich Umgang mit personenbezogenen Daten | Maßnahmen |
|---|---|
| | **Mass Hosting, unmanaged-Systeme**<br>- Bezüglich Firewalls können bei unmanaged-Produkten optional Firewalls gebucht werden. Die Verantwortung für die Verwaltung und Überwachung obliegt dem Kunden.<br>- Virenschutz auf Kundensystemen obliegt der Verantwortung des Kunden.<br>- Außer bei Dedicated Servern (gegen Aufpreis möglich) finden Backups in einen anderen Brandabschnitt oder ein anderes Data Center statt. Die Vorhaltezeit beträgt mindestens sieben Tage.<br>- Bei Dedicated Servern muss der Kunde dies eigenständig im KIS und VPS Windows im PowerPanel einrichten. Bei allen anderen Produkten übernimmt dies automatisch Host Europe.<br><br>**Managed Hosting, unmanaged-Systeme**<br>- Bezüglich Firewalls können bei unmanaged-Produkten optional Firewalls gebucht werden. Die Verantwortung für die Verwaltung und Überwachung obliegt dem Kunden.<br>- Virenschutz auf Kundensystemen obliegt der Verantwortung des Kunden.<br>- Der Kunde ist für die Erstellung einer Datensicherung verantwortlich. Er kann entsprechende Services bei Host Europe zu buchen. |
| **7.**<br>**Datentrennungskontrolle**<br>(zweckbezogen)<br>*Zielbeschreibung:* Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. | **Allgemein**<br>- Bitte sehen Sie dazu unsere Ausführungen zum Zugang und Zugriff.<br>- Grundsätzlich liegt eine physikalische oder logische Trennung einzelner Kundensysteme vor.<br>- Es existiert ein Berechtigungskonzept auf den Systemen |
| **8.**<br>**Auftragskontrolle**<br>*Zielbeschreibung:* Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. | **Allgemein**<br>- Bitte sehen Sie dazu unsere Ausführungen zum Zugang und Zugriff.<br>- Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß §5 BDSG<br>- Die Host Europe GmbH hat einen Datenschutzbeauftragten formal bestellt.<br>- Die Auftraggeber erhalten bei der Host Europe GmbH im Rahmen der Auftragsdatenverarbeitung ein Kontrollrecht.<br>- Sofern die Host Europe GmbH Subunternehmen mit Aufgaben betraut, gelten für diesen die gleichen Regelungen und Bestimmungen wie für die Host Europe GmbH selbst. |