

# Vertrag zur Auftragsdatenverarbeitung gemäss § 11 BDSG

zwischen der

**Host Europe GmbH**  
Hansestr. 111  
51149 Köln

vertreten durch die Geschäftsführer Dr. Claus Boyens und Tobias Mohr  
(nachfolgend „die Auftragnehmerin“)

und

Firma: .....
Straße/Nr.: .....
PLZ: .....
Ort: .....

vertreten durch den/die Geschäftsführer/in: .....  
(nachfolgend „die Auftraggeberin“)



1. Gegenstand und Dauer des Auftrags (§ 11 Abs. 2 S. 2 Nr. 1 BDSG).....	3
2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen (§ 11 Abs. 2 S. 2 Nr. 2 BDSG).....	3
3. Technisch-organisatorische Maßnahmen (§ 11 Abs. 2 S. 2 Nr. 3 BDSG) .....	4
4. Berichtigung, Sperrung, Löschung von Daten (§ 11 Abs. 2 S. 2 Nr. 4 BDSG) .....	4
5. Pflichten der Auftragnehmerin (§ 11 Abs. 2 S. 2 Nr. 5 BDSG).....	4
6. Unterauftragsverhältnisse (§ 11 Abs. 2 S. 2 Nr. 6 BDSG) .....	5
7. Kontrollrechte der Auftraggeberin (§ 11 Abs. 2 S. 2 Nr. 7 BDSG) .....	5
8. Mitteilungspflichten bei Verstößen der Auftragnehmerin oder bei ihr beschäftigter Personen gegen Datenschutzvorschriften oder gegen den Auftrag (§ 11 Abs. 2 S. 2 Nr. 8 BDSG).....	6
9. Weisungsbefugnisse der Auftraggeberin (§ 11 Abs. 2 S. 2 Nr. 9 BDSG) .....	6
10. Löschung von Daten und Rückgabe überlassener Datenträger (§ 11 Abs. 2 S. 2 Nr. 10 BDSG)6	

## 1. Gegenstand und Dauer des Auftrags (§ 11 Abs. 2 S. 2 Nr. 1 BDSG)

- 1.1 Gegenstand des Auftrags ist die Bereitstellung von Hosting Lösungen im Rahmen des mit der Auftraggeberin vereinbarten Umfangs.
- 1.2 Gegenstand des Auftrags ist **nicht** die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch die Auftragnehmerin. Im Zuge der Leistungserbringung der Auftragnehmerin als zentraler IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen der Auftraggeberin, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.
- 1.3 Die Dauer dieses Auftrags (Laufzeit) richtet sich nach der Dauer der Erbringung von Hosting-Leistungen der Auftragnehmerin an die Auftraggeberin. Der Auftrag endet, wenn die Auftraggeberin keine Hosting-Leistungen der Auftragnehmerin, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen für Hosting-Leistungen der Auftragnehmerin, mehr in Anspruch nimmt.

## 2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen (§ 11 Abs. 2 S. 2 Nr. 2 BDSG)

- 2.1 Umfang, Art und Zweck der Zugriffsmöglichkeit der Auftragnehmerin auf Daten der Auftraggeberin ergeben sich aus den Leistungsbeschreibungen der einzelnen Auftragsbestätigungen der Auftragnehmerin für die Hosting-Leistungen. Zusammen gefasst entsteht die Zugriffsmöglichkeit:
  - beim Hosting von Server-Systemen und dort betriebenen Anwendungen (Datenbank-, Backup-, Web-Server, SAN-Umgebung)
  - bei der technischen Administration der Server-Systeme
  - bei sonstigen Support-Tätigkeiten für sämtliche Server-Systeme (z.B. im Rahmen des proaktiven Monitorings)
  - im Rahmen der Betreuung, der von der Auftraggeberin betriebenen Firewall (Log-Files)

Zum Zwecke der Vertragserfüllung kann ein Zugriff der Auftragnehmerin, auf die unter 2.2 aufgeführten Daten, nicht ausgeschlossen werden.

### 2.2 Art der Daten

Die von der Auftragstätigkeit betroffenen Datenkategorien von Kunden, Lieferanten, Geschäftspartnern und Beschäftigten der Auftraggeberin lauten wie folgt:

- Stammdaten
- Kontaktdaten
- Vertragsdaten
- Vertragssteuerungsdaten
- Protokolldaten
- Bankdaten

### 2.3 Kreis der Betroffenen

Der Kreis der, durch den Umgang mit ihren Daten im Rahmen dieses Auftrags, Betroffenen umfasst:

- Kunden und potentielle Kunden der Auftraggeberin (Endverbraucher)
- Beschäftigte, Lieferanten und Geschäftspartner der Auftraggeberin

### **3. Technisch-organisatorische Maßnahmen (§ 11 Abs. 2 S. 2 Nr. 3 BDSG)**

- 3.1 Die Auftragnehmerin beachtet die Grundsätze ordnungsgemäßer Speicherbuchführung und gewährleistet die im Rahmen der ordnungsgemäßen Abwicklung des Auftrags erforderlichen technischen und organisatorischen Maßnahmen gem. § 9 BDSG und Anlage. Die erforderlichen Maßnahmen sind im Datenschutz- und IT-Sicherheitskonzept „Datenschutz gemäß § 9 BDSG - Kontrollziele gemäß Anlage § 9 BDSG und Beschreibung der technischen und/oder organisatorischen Sicherungsmaßnahmen“ dokumentiert und sind Bestandteil dieser Vereinbarung. Sie werden der Auftraggeberin vorab zur Prüfung übergeben.
- 3.2 Die Parteien sind sich einig, dass die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen. Insoweit ist es der Auftragnehmerin gestattet, alternative adäquate Maßnahmen umzusetzen. Sie muss die Auftraggeberin hierüber auf Anfrage informieren und sicherstellen, dass das Sicherheitsniveau der festgelegten Maßnahme nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Die Auftragnehmerin hat auf Anforderung die Angaben nach § 4 g Abs. 2, Satz 1 BDSG der Auftraggeberin zur Verfügung zu stellen.
- 3.3 Die Auftragnehmerin ermöglicht und unterstützt die Prüfung der Umsetzung der vereinbarten Maßnahmen vor Beginn, sowie während der Verarbeitung durch die Auftraggeberin. Hierzu gewährt die Auftragnehmerin Einblick in ein im Hinblick auf den Auftrag umfassendes und aktuelles Datenschutz- und IT-Sicherheitskonzept.

### **4. Berichtigung, Sperrung, Löschung von Daten (§ 11 Abs. 2 S. 2 Nr. 4 BDSG)**

- 4.1 Die Rechte der durch den Datenumgang bei der Auftragnehmerin betroffenen Personen insbesondere auf Berichtigung, Löschung und Sperrung sind gegenüber der Auftraggeberin geltend zu machen. Sie ist allein verantwortlich für die Wahrung dieser Rechte.
- 4.2 Die Auftragnehmerin ist verpflichtet, im Rahmen Ihrer Tätigkeit für die Auftraggeberin an sie gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an die Auftraggeberin weiterzuleiten. Sie ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit der Auftraggeberin selbständig zu bescheiden.
- 4.3 Die Auftragnehmerin hat die Auftraggeberin bei der Umsetzung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Sperrung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen ihrer Möglichkeiten zu unterstützen.

### **5. Pflichten der Auftragnehmerin (§ 11 Abs. 2 S. 2 Nr. 5 BDSG)**

Die Auftragnehmerin hat bezogen auf diesen Auftrag insbesondere folgende Pflichten gemäß § 11 Abs. 4 BDSG:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden der Auftraggeberin auf Anforderung, zum Zweck der direkten Kontaktaufnahme, mitgeteilt.

- Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf die unter Punkt 2.2 aufgeführten Daten der Auftraggeberin zugreifen könnten, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten, sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.
- Die unverzügliche Information der Auftraggeberin über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG bei der Auftragnehmerin ermittelt.
- Die Durchführung der Auftragskontrolle mittels Prüfungen durch die Auftragnehmerin im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

## **6. Unterauftragsverhältnisse (§ 11 Abs. 2 S. 2 Nr. 6 BDSG)**

- 6.1 Die Auftraggeberin ist grundsätzlich damit einverstanden, dass die Auftragnehmerin an sorgfältig ausgewählten Drittunternehmen Unteraufträge erteilt, insbesondere, aber nicht ausschließlich, für die Bereiche Wartung und Installation der Rechenzentrumsinfrastruktur, Telekommunikationsdienstleistungen, Benutzerservice, Reinigungskräfte, Prüfer und Entsorgung von Datenträgern.
- 6.2 Die Auftragnehmerin hat bei der Vergabe von Unteraufträgen die Anforderungen des § 11 BDSG zu beachten und die vertragliche Vereinbarung mit dem Unterauftragnehmer so zu gestalten, dass sie den in dieser Vereinbarung festgelegten Datenschutzerfordernissen zwischen Auftragnehmerin und Auftraggeberin entsprechen.

## **7. Kontrollrechte der Auftraggeberin (§ 11 Abs. 2 S. 2 Nr. 7 BDSG)**

- 7.1 Die Auftraggeberin hat das Recht, die in Nr. 8 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit der Auftragnehmerin durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Sie hat das Recht, sich durch Stichprobenkontrollen, nach rechtzeitiger vorheriger Anmeldung (3 Wochen) zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, von der Einhaltung dieser Vereinbarung durch die Auftragnehmerin in ihrem Geschäftsbetrieb zu überzeugen. Die Auftragnehmerin verpflichtet sich, der Auftraggeberin auf Anforderung die, zur Wahrung seiner Verpflichtung zur Auftragskontrolle, erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Kosten, die der Auftragnehmerin durch ihre Unterstützungshandlung entstehen, sind ihr im angemessenen Umfang zu erstatten.
- 7.2 Im Hinblick auf die Kontrollverpflichtungen der Auftraggeberin nach § 11 Abs. 2 S. 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt die Auftragnehmerin sicher, dass die Auftraggeberin sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.
- 7.3 Die Auftragnehmerin verpflichtet sich, der Auftraggeberin auf Anforderung die, zur Wahrung ihrer bei der Verarbeitung der oben genannten Daten bestehende Verpflichtung zur Auftragskontrolle, erforderlichen Auskünfte zu geben und Nachweise zu führen. Dies gilt auch, soweit die Auftragnehmerin die Kontrolle ihrer Unterauftragnehmer für die Auftraggeberin durchführt.

## **8. Mitteilungspflichten bei Verstößen der Auftragnehmerin oder bei ihr beschäftigter Personen gegen Datenschutzvorschriften oder gegen den Auftrag (§ 11 Abs. 2 S. 2 Nr. 8 BDSG).**

- 8.1 Stellt die Auftragnehmerin fest, dass die bei ihr gespeicherten auftragsrelevanten Daten der Auftraggeberin unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat sie dies ohne Ansehen auf die Verursachung unverzüglich der Auftraggeberin mitzuteilen.
- 8.2 Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs (z.B. längerer Ausfall eines Server-Systems), beim Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit den relevanten Daten der Auftraggeberin.
- 8.3 Soweit die Auftraggeberin Pflichten nach § 42a BDSG treffen, z.B. im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten durch Dritte, hat die Auftragnehmerin sie hierbei zu unterstützen.
- 8.4 Die Auftraggeberin informiert die Auftragnehmerin, wenn sie Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

## **9. Weisungsbefugnisse der Auftraggeberin (§ 11 Abs. 2 S. 2 Nr. 9 BDSG)**

- 9.1 Für die Beurteilung der Zulässigkeit der Erhebung, Verarbeitung oder Nutzung sowie für die Wahrung der Rechte der Betroffenen insbesondere nach §§ 6, 7 und 8 BDSG ist allein die Auftraggeberin verantwortlich (§ 11 Abs. 1 BDSG).
- 9.2 Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen. Die Auftraggeberin ist berechtigt, Weisungen über Art und Umfang der Datenverarbeitung im Hinblick auf die Umsetzung von Datenschutzerfordernissen zu erteilen. Die Weisungen bedürfen der Textform.
- 9.3 Ist die Auftragnehmerin der Ansicht, dass eine Weisung gegen das Bundesdatenschutzgesetz oder andere Vorschriften über den Datenschutz verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen. Sie ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Auftraggeberin bestätigt oder geändert wird.
- 9.4 Die Auftragnehmerin verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen der Auftraggeberin nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.
- 9.5 Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen der Auftraggeberin an die Auftragnehmerin entstehen, bleiben unberührt.

## **10. Löschung von Daten und Rückgabe überlassener Datenträger (§ 11 Abs. 2 S. 2 Nr. 10 BDSG)**

- 10.1 Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch die Auftraggeberin – spätestens mit Beendigung der Leistungsvereinbarung – hat die Auftragnehmerin sämtliche in ihrem Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen und einen Personenbezug zulassen könnten, der Auftraggeberin auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

- 10.2 Zu einem Datenträgeraustausch zwischen den Beteiligten dieser Auftragsdatenverarbeitung kommt es nicht. Insoweit ist eine Rückgabe hier nicht zu regeln.
- 10.3 Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Sie kann sie zu ihrer Entlastung bei Vertragsende der Auftraggeberin übergeben.

\_\_\_\_\_  
Ort, Datum


\_\_\_\_\_  
Ort, Datum

  
\_\_\_\_\_  
Auftraggeberin

  
\_\_\_\_\_  
Auftragnehmerin Host Europe GmbH

## DATENSCHUTZ gemäß § 9 BDSG

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

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	Maßnahmen
<p><b>1.</b> <b>Zutrittskontrolle</b> (Räume und Gebäude) <i>Zielbeschreibung:</i> Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.</p>	<p><b>Standort Köln, Welsersstraße 14</b></p> <ul style="list-style-type: none"> <li>- Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen</li> <li>- Es bestehen Sichtkontrollen und ein Besucherbuch am Empfang</li> <li>- Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes</li> <li>- Im Alarmfall werden die für das Gebäude verantwortlichen Mitarbeiter automatisch alarmiert</li> <li>- Zusätzlich ist das Gebäude 24/7 durch eigenes Personal besetzt. Diesem Personal werden die Alarmpmeldungen angezeigt</li> <li>- Es besteht eine restriktive Zutrittsregelung</li> </ul> <p><b>Standort Köln, Hansestraße 109</b></p> <ul style="list-style-type: none"> <li>- Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen</li> <li>- Es bestehen Sichtkontrollen und ein Besucherbuch am Empfang</li> <li>- Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes</li> <li>- Im Alarmfall werden die für das Gebäude verantwortlichen Mitarbeiter automatisch alarmiert</li> <li>- Dem im Hauptgebäude 24/7 befindlichen Personal werden die Alarmpmeldungen angezeigt</li> <li>- Es besteht eine restriktive Zutrittsregelung</li> </ul> <p><b>Standort Straßburg:</b></p> <ul style="list-style-type: none"> <li>- Sicherheitsbereich mit Eingangskontrolle</li> <li>- eingezäuntes Gelände inkl. Videoüberwachung</li> <li>- Regelmäßige Kontrollgänge durch das Sicherheitspersonal</li> <li>- Zutrittskontrollsystem mit Chipkarten.</li> </ul>
<p>Host Europe GmbH Welsersstr. 14 • 51149 Köln www.hosteurope.de • info@hosteurope.de</p>	<p>Bankverbindungen DE: Sparkasse KölnBonn SWIFT-BIC: COLSDE33 IBAN: DE20 3705 0108 1004 1126 32 AT: Oberbank AG • Kto.-Nr. 611-0515.33 • BLZ 15000 SWIFT-BIC: OBKLAT2L • IBAN: AT69 1500 0006 1105 1533 CH: PostFinance Basel/Bern • Kto.-Nr. 91-181312-4 (EUR) IBAN: CH55 0900 0000 9118 1312 4</p> <p>Geschäftsführer: Dr. Claus Boyens Tobias Mohr Amtsgericht Köln: HRB 28495 USt-IdNr.: DE187370678</p>  <p>CO2- neutrales Hosting</p>
<p>Serviceline Festnetz: 0800 467 8387</p>	



<b>Kontrollziele</b> bezüglich Umgang mit personenbezogenen Daten	<b>Maßnahmen</b>
<p><b>2.</b>  <b>Zugangskontrolle</b>            (IT-Systeme, Anwendungen)  <i>Zielbeschreibung:</i> Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.</p>	<p><b>Allgemein</b></p> <ul style="list-style-type: none"> <li>- Die Host Europe vermietet die Datenverarbeitungsanlage an den Kunden</li> <li>- Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung</li> <li>- Der Kunde entscheidet allein und ausschließlich darüber, welche personenbezogenen Daten in welcher Weise verarbeitet werden („Herr der Daten“)</li> <li>- Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Kunden erstellt und eingesetzt</li> <li>- 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</li> <li>- 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</li> </ul> <p><b>Mass Hosting, unmanaged-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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.</li> </ul> <p><b>Mass Hosting, managed-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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.</li> </ul> <p><b>Managed Hosting, unmanaged-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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.</li> </ul> <p><b>Managed Hosting, managed-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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</li> </ul>

<b>Kontrollziele</b> bezüglich Umgang mit personenbezogenen Daten	<b>Maßnahmen</b>
	Zugang. Es bestehen Regelungen zum Schutz und zur regelmäßigen Änderung der Zugangspasswörter/-Schlüssel.
<p><b>3.</b>  <b>Zugriffskontrolle</b>            (auf Daten)  <i>Zielbeschreibung:</i> 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.</p>	<p><b>Allgemein</b></p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- Alle Mitarbeiter der Host Europe sind gemäß BDSG zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet und entsprechend geschult</li> </ul> <p><b>Mass Hosting, unmanaged-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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.</li> </ul> <p><b>Mass Hosting, managed-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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.</li> </ul> <p><b>Managed Hosting, unmanaged-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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.</li> </ul> <p><b>Managed Hosting, managed-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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.</li> </ul>
<p><b>4.</b>  <b>Eingabekontrolle</b>            (in Datenverarbeitungssysteme)  <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem</p>	<p><b>Mass Hosting, unmanaged-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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</li> </ul>

<b>Kontrollziele</b> bezüglich Umgang mit personenbezogenen Daten	<b>Maßnahmen</b>
<p>personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.</p>	<p>Eingabekontrolle der Daten ausschließlich durch den Kunden umgesetzt werden kann.</p> <p><b>Mass Hosting, managed-Systeme</b></p> <p>- 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.</p> <p><b>Managed Hosting, unmanaged-Systeme</b></p> <p>- 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.</p> <p><b>Managed Hosting, managed-Systeme</b></p> <p>- 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.</p>
<p><b>5. Weitergabekontrolle</b> (von Daten)</p> <p><i>Zielbeschreibung:</i> 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.</p>	<p><b>Allgemein</b></p> <p>- 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.</p> <p><b>Mass Hosting, unmanaged-Systeme</b></p> <p>- 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.</p>

<b>Kontrollziele</b> bezüglich Umgang mit personenbezogenen Daten	<b>Maßnahmen</b>
	<p>Der Zugriff erfolgt durch geschulte und auf das Datengeheimnis verpflichtete Administratoren. Sämtliche administrative Aufgaben finden über gesicherte Wege, wie bspw. SSL-verschlüsselt, statt.</p> <p><b>Mass Hosting, managed-Systeme</b></p> <p>- 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.</p> <p><b>Managed Hosting, unmanaged-Systeme</b></p> <p>- 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.</p> <p><b>Managed Hosting, managed-Systeme</b></p> <p>- 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.</p>
<p><b>6. Verfügbarkeitskontrolle</b>            (von Daten)  <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.</p>	<p><b>Allgemein</b></p> <p>- Die autonome Stromversorgung der Data Center erfolgt über eine eigene Trafostation. Die Stromversorgung und Netzersatzanlage garantieren höchste Ausfallsicherheit.</p> <p>- Jedes Serverrack wird über mindestens zwei separate Stromzuführungen versorgt, die je einzeln mit mindestens 16 Ampere abgesichert sind.</p>

<b>Kontrollziele</b> bezüglich Umgang mit personenbezogenen Daten	<b>Maßnahmen</b>
	<ul style="list-style-type: none"> <li>- Die unmittelbare Stromversorgung des Servers ist typenabhängig, so dass bei der Verwendung entsprechender Typen zusätzlich eine redundante Stromversorgung über ein redundantes Netzteil (2 Netzteile) gewährleistet ist.</li> <li>- 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.</li> <li>- Eine leistungsstarke Netzersatzanlage (Dieselaggregat) versorgt bei Stromausfall das gesamte jeweilige Data Center und die Kühlsysteme mit konstanter Energie.</li> <li>- Für Backups wird ein dediziertes Backup-LAN oder ein über VLAN logisch getrenntes Netzwerk verwendet.</li> </ul> <p><b>Standort Köln, Welsersstraße 14</b></p> <ul style="list-style-type: none"> <li>- Der Kraftstoffvorrat ist für mindestens 24 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich.</li> <li>- Ein flächendeckendes Wasser- und Brandfrühwarnsystem (VESDA) reagiert bereits bei geringer Überschreitung definierter Grenzwerte, um größere Schäden zu verhindern.</li> <li>- Die Brandmeldeanlage verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr.</li> <li>- Die Gebäudeaußenhaut ist zudem mittels Überspannungsschutz gegen Blitzschlag abgesichert.</li> <li>- 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.</li> <li>- Klimaanlage</li> <li>- Geräte zur Überwachung der Temperatur und Feuchtigkeit in den Data Centern</li> </ul> <p><b>Standort Köln, Hansestraße 109</b></p> <ul style="list-style-type: none"> <li>- Der Kraftstoffvorrat ist für mindestens 16 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich.</li> <li>- Ein flächendeckendes Wasser- und Brandfrühwarnsystem (VESDA) reagiert bereits bei geringer Überschreitung definierter Grenzwerte, um größere Schäden zu verhindern.</li> <li>- Die Brandmeldeanlage verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr.</li> </ul>

<b>Kontrollziele</b> bezüglich Umgang mit personenbezogenen Daten	<b>Maßnahmen</b>
	<ul style="list-style-type: none"> <li>- Die Gebäudeaußenhaut ist zudem mittels Überspannungsschutz gegen Blitzschlag abgesichert.</li> <li>- 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.</li> <li>- Klimaanlage</li> <li>- Geräte zur Überwachung der Temperatur und Feuchtigkeit in den Data Centern</li> </ul> <p><b>Standort Straßburg:</b>            In dem Rechenzentrum in Straßburg besteht eine unterbrechungsfreie Stromversorgung (USV) sowie ein Überspannungsschutz. Ebenso ist ein Branderkennungs- und Frühwarnsystem implementiert. Das Löschesystem ist auf eine möglichst zerstörungsfreie Brandbekämpfung ausgelegt.</p> <p><b>Standort Falkenstein, Am Datacenter Park 1</b></p> <ul style="list-style-type: none"> <li>- Der Kraftstoffvorrat ist für mindestens 24 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich.</li> <li>- Die Brandmeldeanlage verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr.</li> </ul> <p><b>Mass Hosting, managed-Systeme</b></p> <ul style="list-style-type: none"> <li>- Bei managed-Produkten ist die Host Europe GmbH für das gesamte Backup verantwortlich. Die Vorhaltezeit beträgt mindestens 14 Tage.</li> <li>- Host Europe gewährleistet bei Webpack-Produkten ein OffSite-Backup in ein anderes Data Center.</li> <li>- Bei den Produkten ePages, OpenExchange und Webbuilder findet ausschließlich ein lokales Backup im Produktivrechenzentrum statt.</li> </ul> <p><b>Managed Hosting, managed-Systeme</b></p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- Je nach gebuchter Leistung findet das Backup in einem anderen Brandabschnitt oder einem anderen Data Center statt.</li> </ul>

<b>Kontrollziele</b> bezüglich Umgang mit personenbezogenen Daten	<b>Maßnahmen</b>
	<p><b>Mass Hosting, unmanaged-Systeme</b></p> <ul style="list-style-type: none"> <li>- Bezüglich Firewalls können bei unmanaged-Produkten optional Firewalls gebucht werden. Die Verantwortung für die Verwaltung und Überwachung obliegt dem Kunden.</li> <li>- Virenschutz auf Kundensystemen obliegt der Verantwortung des Kunden.</li> <li>- 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.</li> <li>- 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.</li> </ul> <p><b>Managed Hosting, unmanaged-Systeme</b></p> <ul style="list-style-type: none"> <li>- Bezüglich Firewalls können bei unmanaged-Produkten optional Firewalls gebucht werden. Die Verantwortung für die Verwaltung und Überwachung obliegt dem Kunden.</li> <li>- Virenschutz auf Kundensystemen obliegt der Verantwortung des Kunden.</li> <li>- Der Kunde ist für die Erstellung einer Datensicherung verantwortlich. Er kann entsprechende Services bei Host Europe zu buchen.</li> </ul>
<p><b>7. Datentrennungskontrolle</b>            (zweckbezogen)  <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.</p>	<p><b>Allgemein</b></p> <ul style="list-style-type: none"> <li>- Bitte sehen Sie dazu unsere Ausführungen zum Zugang und Zugriff.</li> <li>- Grundsätzlich liegt eine physikalische oder logische Trennung einzelner Kundensysteme vor.</li> <li>- Es existiert ein Berechtigungskonzept auf den Systemen</li> </ul>
<p><b>8. Auftragskontrolle</b>  <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.</p>	<p><b>Allgemein</b></p> <ul style="list-style-type: none"> <li>- Bitte sehen Sie dazu unsere Ausführungen zum Zugang und Zugriff.</li> <li>- Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß §5 BDSG</li> <li>- Die Host Europe GmbH hat einen Datenschutzbeauftragten formal bestellt.</li> <li>- Die Auftraggeber erhalten bei der Host Europe GmbH im Rahmen der Auftragsdatenverarbeitung ein Kontrollrecht.</li> <li>- Sofern die Host Europe GmbH Subunternehmen mit Aufgaben betraut, gelten für diesen die gleichen Regelungen und Bestimmungen wie für die Host Europe GmbH selbst.</li> </ul>