

**Anlage 2 zur Vereinbarung nach § 11 BDSG:
Technische und organisatorische
Maßnahmen nach § 9 BDSG und Anlage**

1. Zutrittskontrolle

- elektronisches Zutrittskontrollsystem mit Protokollierung
- dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen

2. Zugangskontrolle

- bei Hauptauftrag „Rootserver“ und „Colocation“
 - Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und die Auftragnehmer nicht bekannt sind
- bei Hauptauftrag „managed-server“
 - Zugang ist passwortgeschützt, Zugriff besteht nur für Mitarbeiter von Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert

3. Zugriffskontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
 - Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
 - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
- bei Hauptauftrag „Rootserver“ und „Colocation“
 - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
- bei Hauptauftrag „managed-server“
 - Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
 - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für

Mitarbeiter des Auftragnehmers

- Für übertragene Daten/Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.

4. Weitergabekontrolle

- Alle Mitarbeiter sind auf das Datengeheimnis nach § 5 BDSG verpflichtet.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselte Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

5. Eingabekontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
 - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
 - Änderungen der Daten werden protokolliert.
- bei Hauptauftrag „Rootserver“ und „Colocation“
 - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
- bei Hauptauftrag „managed-server“
 - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
 - Änderungen der Daten werden protokolliert.

6. Auftragskontrolle

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
- Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betriebliche Prozesse.

7. Verfügbarkeitskontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
 - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
 - Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
 - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
 - Einsatz unterbrechungsfreier Stromversorgung.
- bei Hauptauftrag „Rootserver“ und „Colocation“
 - Datensicherung obliegt dem Auftraggeber.
 - Einsatz unterbrechungsfreier Stromversorgung.
- bei Hauptauftrag „managed-server“
 - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
 - Einsatz von Festplattenspiegelung
 - Einsatz unterbrechungsfreier Stromversorgung.
 - Einsatz von Softwarefirewall und Portreglementierungen

8. Maßnahmen zur Datensicherung (physikalisch / logisch)

- bei internen Verwaltungssysteme des Auftragnehmers
 - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
 - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.
- bei Hauptauftrag „Rootserver“ und „Colocation“
 - Die Trennungskontrolle obliegt dem Auftraggeber.
- bei Hauptauftrag „managed-server“
 - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
 - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.