

Die physische Speicherung der Auftragsdaten erfolgt grundsätzlich in einem Rechenzentrum der **Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen**

oder der

domainfactory GmbH, Oskar-Messter-Straße 33, 85737 Ismaning.

the surface new media gmbh hat eine gesonderte Vereinbarung zur Auftragsdatenverarbeitung mit diesen technischen Partnern abgeschlossen.

Die Dokumentation der technischen und organisatorischen Maßnahmen bei der **Hetzner Online GmbH** und der **domainfactory GmbH** liegen als Anlage anbei.

Anlage zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Im Rahmen eines Auftrages kann der the surface new media GmbH jedoch auf Auftragsdaten zugreifen und besitzt Authentifizierungsgeheimnisse, die einen Zugriff auf Auftragsdaten ermöglichen.

1. Zutrittskontrolle

- Zutritt zu den Büroräumen ist durch geeignete Schließsysteme nur Mitarbeitern möglich
- Auftragsdaten befinden sich ausschließlich in einem gesonderten Sicherheitsbereich (Rechenzentrum)
- Gäste und Besucher können IT-Systeme mit Zugang zu Auftragsdaten nicht einsehen oder erreichen.

2. Zugangskontrolle

- IT-Systeme können nur durch personengebundene Zugangskennungen in Betrieb genommen werden
- Mitarbeiter sind angewiesen und sensibilisiert, sich bei Verlassen des Arbeitsplatzes von Auftragssystemen abzumelden, unabhängig davon erfolgt eine technische Abmeldung nach Inaktivität von 10 Minuten
- Zugangskennungen des Auftragssystems werden nicht auf IT-Systemen des Auftragnehmers gespeichert

3. Zugriffskontrolle

- Zugang zu Auftragssystemen erfordert ebenfalls eine personengebundene Authentifizierung
- Das Auftragssystem folgt einem differenzierten Rollen- und Berechtigungskonzept





4. Weitergabekontrolle

- Kommunikation zwischen Auftragssystem und IT-Systemen des Auftragnehmers erfolgt verschlüsselt (SSL-verschlüsselt)
- Transfers von Dateien zwischen IT-Systemen des Auftragnehmers und Auftragssystemen erfolgt ebenfalls verschlüsselt (SFTP, FTPS), Authentifizierungen erfolgen über eine verschlüsselte Verbindung
- Die Nutzung von WLAN-Verbindungen erfolgt ebenfalls verschlüsselt wobei eine wechselseitige Authentifizierung (VPN) erforderlich ist
- Mitarbeiter werden regelmäßig zum Datenschutz und erforderlichen Sicherheitsmaßnahmen geschult und sensibilisiert
- Mitarbeiter sind auf das Datengeheimnis verpflichtet
- Die Übernahme von Auftragsdaten auf Datenträger außerhalb des Auftragssystems ist allen verboten

5. Eingabekontrolle

- Protokollierung der Zugriffe auf Auftragssysteme über alle verfügbaren Kommunikationsprotokolle
- Regelmäßige Analyse der Zugriffsprotokolle

6. Auftragskontrolle

- Vertragsgestaltung und Formerfordernis an Weisungen gewährleisten weisungsgemäße Auftragsdatenverarbeitung
- Kontrolle durch Leistungsnachweise
- Kontrollmöglichkeiten des Auftraggebers

7. Verfügbarkeitskontrolle

- Dem Auftraggeber wird auf Verlangen ein privilegierter Nutzer eingerichtet und die Authentifizierungsdaten zur Verfügung gestellt, der geeignet ist die Verwaltung der Nutzer inklusive aller anderen privilegierten Nutzer zu übernehmen
- aufgrund der dargestellten Systemtrennung sind keine Maßnahmen zur Sicherung der Verfügbarkeit der Auftragsdaten durch den Auftraggeber erforderlich

8. Trennungskontrolle

- das Auftragssystem als Produktivsystem ist getrennt von Testsystemen

