

der Organisation  
InstiKom GmbH

Stand  
01.06.2021

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die oben genannte Organisation erfüllt diesen Anspruch durch nachfolgende Maßnahmen. Um Transparenz hinsichtlich des Unterauftraggebers Hetzner Online GmbH zu schaffen, wurden die vorliegenden TOMs um die technisch organisatorischen Maßnahmen des Rechenzentrums ergänzt.

## 1. VERTRAULICHKEIT GEM. ART. 32 ABS. 1 LIT. DSGVO

### 1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Alarmanlage & Kameraüberwachung	<input checked="" type="checkbox"/> Maßnahmen bei Verlust von Schlüssel / Chip
<input checked="" type="checkbox"/> Token basierte Schließsysteme	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste
<input checked="" type="checkbox"/> Abgeschlossenes Aufbewahrungssystem	
<input checked="" type="checkbox"/> Aufzug mit Schlüsselsystem	
<input checked="" type="checkbox"/> Klingelanlage mit Sprechfunktion	

Darüber hinaus werden im Rechenzentrum in Falkenstein folgende Sicherheitsmaßnahmen erfüllt:

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> elektronisches Zutrittskontrollsystem mit Protokollierung	<input checked="" type="checkbox"/> dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
<input checked="" type="checkbox"/> Hochsicherheitszaun um den gesamten Datacenter-Park	<input checked="" type="checkbox"/> Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
<input checked="" type="checkbox"/> Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen	<input checked="" type="checkbox"/> 24/7 personelle Besetzung der Rechenzentren

	<input checked="" type="checkbox"/> Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
--	--

## 1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Login mit Benutzername + Passwort	<input checked="" type="checkbox"/> Verwalten von Benutzerberechtigungen
<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Verwendung von komplexen Passwörtern: mind. 8-stellig, Buchstaben, Zahlen, Zeichen
<input checked="" type="checkbox"/> Automatische Desktopsperre	<input checked="" type="checkbox"/> automatische Sperrmechanismen
<input checked="" type="checkbox"/> Zutrittsdokumentation (Logging)	<input checked="" type="checkbox"/> Allg. Richtlinie Datenschutz und / oder Sicherheit
<input checked="" type="checkbox"/> Verschlüsselte Speicherung von Passwörtern	
<input checked="" type="checkbox"/> Login über Clients mit OAuth2 Redirect-URLs; keine Übertragung von Zugangsdaten zwischen Clients und Server	

Darüber hinaus werden im Rechenzentrum in Falkenstein folgende Sicherheitsmaßnahmen erfüllt:

Technische Maßnahmen
<input checked="" type="checkbox"/> Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
<input checked="" type="checkbox"/> Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zwei-Faktor-Authentifizierung zur weiteren Absicherung des Accounts.

## 1.3. Zugriffskontrolle

Maßnahmen, die 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.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Physische Löschung von Datenträgern	<input checked="" type="checkbox"/> Bereitstellung eines rollenbasierter Berechtigungskonzepte für Mitarbeiter und Angehörige, zur selbständigen Vergabe durch die Einrichtungsleitung
	<input checked="" type="checkbox"/> bedarfsgerechte Zugriffsrechte: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
	<input checked="" type="checkbox"/> Minimale Anzahl an Administratoren

	<input checked="" type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren
	<input checked="" type="checkbox"/> Reduzierte, differenzierte und dokumentierte Vergabe von Systemberechtigungen für Mitarbeiter

#### 1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Trennung von Produktiv- und Testumgebung	<input checked="" type="checkbox"/> Steuerung über Berechtigungskonzept
<input checked="" type="checkbox"/> Trennung von Anwendungs- und Administrationszugängen	<input checked="" type="checkbox"/> Festlegung von Datenbankrechten

#### 1.5. Pseudonymisierung & Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Daten werden TLS verschlüsselt übertragen	<input checked="" type="checkbox"/> Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe zu anonymisieren (z.B. Weitergabe Geräteerkennung bei Fehlermeldung an Entwickler)
<input checked="" type="checkbox"/> Verschlüsselung von Festplatten und mobilen Datenträgern	
<input checked="" type="checkbox"/> Freie Wahl der Benutzererkennung / des Benutzernamens – Möglichkeit der Systemnutzung über Pseudonyme	

## 2. INTEGRITÄT (ART. 32 ABS. 1 LIT. B DSGVO)

### 1.1. Weitergabekontrolle

Maßnahmen, die 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.

Technische Maßnahmen
<input checked="" type="checkbox"/> Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport Einsatz von Virtual Private Networks (VPN)
<input checked="" type="checkbox"/> Protokollierung der Zugriffe und Abrufe
<input checked="" type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https
<input checked="" type="checkbox"/> Filetransfer ausschließlich über Private Cloud. Es werden keine USB-Sticks oder Festplatten zur Weitergabe von Daten verwendet.

### 1.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Backend-Nutzern über Server-Logs	<input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
<input checked="" type="checkbox"/> Manuelle oder automatisierte Kontrolle der Protokolle	<input checked="" type="checkbox"/> Klare Zuständigkeiten für Löschungen

## 3. VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

### 1.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Regelmäßige Archivierung / Backup der Daten auf separaten Back-Up Server	<input checked="" type="checkbox"/> Backup-Strategie (online/offline; onsite/off-site)
	<input checked="" type="checkbox"/> Regelmäßige Tests zur Datenwiederherstellung & Protokollierung der Ergebnisse

Darüber hinaus werden im Rechenzentrum in Falkenstein folgende Sicherheitsmaßnahmen erfüllt:

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage	<input checked="" type="checkbox"/> Festgelegte Informationskette, um im Fehlerfall zu informieren und um das System schnellstmöglich wiederherzustellen.
<input checked="" type="checkbox"/> Dauerhaft aktiver DDoS-Schutz.	

#### 4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D DSGVO; ART. 25 ABS. 1 DSGVO)

##### 1.1. Datenschutz-Management

Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. einmal pro Jahr im Rahmen eines Audits durch den externen DSB durchgeführt
<input checked="" type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet (datenschutzrechtlichen Verhaltenskodex für Mitarbeiter)
<input checked="" type="checkbox"/> Regelmäßige Sensibilisierung der Mitarbeiter
<input checked="" type="checkbox"/> Mit jedem MA wird eine Home Office-Vereinbarung zum Datenschutz und Datensicherheit abgeschlossen
<input checked="" type="checkbox"/> Interner / externer Informationssicherheits-Beauftragter: Julia Amann, InstiKom GmbH, Geschäftsführerin
<input checked="" type="checkbox"/> Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

##### 1.2. Incident-Response-Management

*Unterstützung bei der Reaktion auf Sicherheitsverletzungen*

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
<input checked="" type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung	
<input checked="" type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung	
	<input checked="" type="checkbox"/> Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

**1.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)***Privacy by design / Privacy by default*

<b>Technische Maßnahmen</b>
<input checked="" type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
<input checked="" type="checkbox"/> Direkte datenschutzrechtliche Hinweise beim erstmaligen Öffnen der App und der Registrierung
<input checked="" type="checkbox"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen
<input checked="" type="checkbox"/> Datenschutzrechtliche Hinweise sind jederzeit schnell und einfach im Hauptmenü der App für den Nutzer nachlesbar
<input checked="" type="checkbox"/> Schutz vor nicht zweckgebundener Verarbeitung

**1.4. Auftragskontrolle (Outsourcing an Dritte)***Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*

<b>Organisatorische Maßnahmen</b>
<input checked="" type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
<input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten, gerade in Bezug auf Datenschutz und Datensicherheit
<input checked="" type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
<input checked="" type="checkbox"/> Schriftliche Weisungen an den Auftragnehmer
<input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
<input checked="" type="checkbox"/> Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellopflicht
<input checked="" type="checkbox"/> Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
<input checked="" type="checkbox"/> Regelung zum Einsatz weiterer Subunternehmer
<input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
<input checked="" type="checkbox"/> Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus