der Organisation
InstiKom GmbH

Stand
01.05.2021

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
☒ Alarmanlage & Kameraüberwachung	☒ Maßnahmen bei Verlust von Schlüssel / Chip
☒ Token basierte Schließsysteme	☒ Besucher in Begleitung durch Mitarbeiter
☒ Sicherheitsschlösser	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Abgeschlossenes Aufbewahrungssystem	
☒ Aufzug mit Schlüsselsystem	
☒ Klingelanlage mit Sprechfunktion	

Darüber hinaus werden im Rechenzentrum in Falkenstein folgende Sicherheitsmaßnahmen erfüllt:

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

	☒ 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
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Firewall	☒ Verwendung von komplexen Passwörtern: mind. 8-stellig, Buchstaben, Zahlen, Zeichen
☒ Automatische Desktopsperre	☒ automatische Sperrmechanismen
☒ Zutrittsdokumentation (Logging)	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Verschlüsselte Speicherung von Passwörtern	
☒ 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
☒ Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
☒ 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
☒ Physische Löschung von Datenträgern	☒ Bereitstellung eines rollenbasierter Berechtigungskonzepte für Erzieher, Elternbeirat, Eltern zur selbständigen Vergabe durch die Einrichtungsleitung
	☒ bedarfsgerechte Zugriffsrechte: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
	☒ Minimale Anzahl an Administratoren

	☒ Verwaltung Benutzerrechte durch Administratoren
	☒ 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
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Trennung von Anwendungs- und Administrationszugängen	☒ 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
☒Daten werden TLS verschlüsselt übertragen	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe zu anonymisieren (z.B. Weitergabe Gerätekennung bei Fehlermeldung an Entwickler)
☒ Verschlüsselung von Festplatten und mobilen Datenträgern	
☒Freie Wahl der Benutzerkennung / 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
☒ Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport Einsatz von Virtual Private Networks (VPN)
☒ Protokollierung der Zugriffe und Abrufe
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https
☒ 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**
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Backend-Nutzern über Server-Logs	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ 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**
☒ Regelmäßige Archivierung / Backup der Daten auf separaten Back-Up Server	☒ Backup-Strategie (online/offline; onsite/off-site)
	☒ Regelmäßige Tests zur Datenwiederherstellung & Protokollierung der Ergebnisse

Darüber hinaus werden im Rechenzentrum in Falkenstein folgende Sicherheitsmaßnahmen erfüllt:

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage	☒ Festgelegte Informationskette, um im Fehlerfall zu informieren und um das System schnellstmöglich wiederherzustellen.
☒ 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
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. einmal pro Jahr im Rahmen eines Audits durch den externen DSB durchgeführt
☒ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet (datenschutzrechtlichen Verhaltenskodex für Mitarbeiter)
☒ Regelmäßige Sensibilisierung der Mitarbeiter
☒ Mit jedem MA wird eine Home Office-Vereinbarungen zum Datenschutz und Datensicherheit abgeschlossen
☒ Interner / externer Informationssicherheits-Beauftragter: Julia Amann, InstiKom GmbH, Geschäftsführerin
☒ 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
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	

1.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Technische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
☒ Direkte datenschutzrechtliche Hinweise beim erstmaligen Öffnen der App und der Registrierung
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen
☒ Einblendung von speziellen datenschutzrechtlichen Hinweisen bei der Eingabe besonderer personenbezogener Daten (z.B. Eingabe von Krankmeldungen) seitens der Eltern
☒ Datenschutzrechtliche Hinweise sind jederzeit schnell und einfach im Hauptmenü der App für den Nutzer nachlesbar
☒ 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.

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

InstiKom GmbH – Alle Rechte vorbehalten