Technische und organisatorische Maßnahmen gemäß Art. 32 Abs. 1 DSGVO

Die beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO gelten für alle durch das KITS eingesetzten bzw. betreuten Verfahren und Systeme.

1. Zutrittskontrolle

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

- ☒ Alarmanlage
- ☐ Automatisches Zugangskontrollsystem
- ☐ Schließsystem mit Codesperre
- ☒ Biometrische Zugangssperren
- ☐ Lichtschranken / Bewegungsmelder
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Sonstige:
- ☐ Absicherung von Gebäudeschächten
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☒ Videoüberwachung der Zugänge
- ☒ Sicherheitsschlösser
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☒ Zuordnung von Benutzerrechten
- ☒ Passwortvergabe
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Erstellen von Benutzerprofilen
- ☐ Authentifikation mit biometrischen Verfahren
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen

- ☐ Gehäuseverriegelungen
- ☒ Einsatz von VPN-Technologie
- ☒ Sperren von externen Schnittstellen (USB etc.)
- ☒ Sicherheitsschlösser
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☐ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Tragepflicht von Berechtigungsausweisen
- ☒ Einsatz von Intrustion-Detection-Systemen
- ☐ Verschlüsselung von mobilen Datenträgern
- ☒ Verschlüsselung von Smartphone-Inhalten
- ☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- ☒ Einsatz von Anti-Viren-Software
- ☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
- ☒ Einsatz einer Hardware-Firewall
- ☒ Einsatz einer Software-Firewall
- ☐ Sonstige:

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.

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Anzahl der Administratoren auf das „Notwendigste" reduziert
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Sichere Aufbewahrung von Datenträgern
- ☒ physische Löschung von Datenträgern vor Wiederverwendung
- ☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☒ Protokollierung der Vernichtung
- ☒ Verschlüsselung von Datenträgern
- ☐ Sonstige:

4. 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

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- ☐ Sonstige:
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen

5. Verfügbarkeitskontrolle

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

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Testen von Datenwiederherstellung
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ In Hochwassergebieten: Serverräume über der Wassergrenze
- ☐ Sonstige:
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☐ Erstellen eines Notfallplans
- ☒ Serverräume nicht unter sanitären Anlagen

6. Trennungsgebot

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

- ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Erstellung eines Berechtigungskonzepts
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☒ Festlegung von Datenbankrechten
- ☐ Sonstige:
- ☒ Logische Mandantentrennung (softwareseitig)
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☐ Trennung von Produktiv- und Testsystem

Ort/Datum: Meiningen, 19.05.2021

Verantwortlicher für die Erstellung: Bettina Schwidder

Unterschrift Verantwortlicher: Bastian Holland-Moritz

KitS Kommunaler IT-Service
Obertshäuser Platz 1, 98617 Meiningen
03693 485 8880 / info@deinrz.de
www.deinrz.de