

Anlage 1

Auflistung der personenbezogenen Daten und dem Zweck ihrer Verarbeitung, Art der Daten:

- Personenstammdaten
- Kommunikationsdaten
- Protokolldaten
- Zugehörigkeit zur Bildungseinrichtung/Institution
- Rolle in der TSC
- Gruppenmitgliedschaft (Klassen und Teams)
- Temporäre Daten in Chats und Videokonferenzen
- Passwort
- Erzeugte Pseudonyme, Ort der Verwendung

Kreis der betroffenen Personen:

- Lehrerinnen und Lehrer
- Schülerinnen und Schüler
- Angestellte der Bildungseinrichtung/Institution
- Weitere Personen, zum Beispiel Bildungsexperten oder Eltern
- Mitarbeitende des Auftragnehmers und der Unterauftragnehmer

Anlage 2

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

I. Vertraulichkeit

(a) Zutrittskontrolle

- dokumentierte Schlüsselvergabe an Mitarbeitende
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines ThILLM-Mitarbeitenden.
- gesicherter Serverraum

(b) Zugangskontrolle

- Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeitende vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert.
- Passwortrichtlinie ist vorhanden.

(c) Zugriffskontrolle

- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Revisions-sicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeitende des Auftragnehmers
- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Für übertragene Daten/Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.

(d) Datenträgerkontrolle

- Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht).
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden zerstört (geschreddert).

(e) Trennungskontrolle

- Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

(a) Weitergabekontrolle

- Alle Mitarbeitende sind i. S. d. Art. 32 Abs.4 DSGVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
- Vorliegen eines Löschkonzeptes
- Verschlüsselung mobiler Datenträger

(b) Eingabekontrolle

- Eingabe und Änderungen der Daten werden protokolliert.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

(a) Verfügbarkeitskontrolle

- 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
- Monitoring aller relevanten Server
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage
- Dauerhaft aktiver DDoS-Schutz
- Einsatz von Softwarefirewall und Portreglementierungen
- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DSGVO).
- Die Mitarbeitenden des Auftragnehmers werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.
- Das ThILLM hat einen Datenschutzbeauftragten bestellt.

Anlage 3

Liste der Unterauftragnehmer

Folgende Unterauftragnehmer werden im Rahmen weiterer Auftragsverarbeitung eingesetzt:

- topdev GmbH, Am Seegraben 2, 99099 Erfurt, Dienstleister TSP
- Dataport AöR, Altenholzer Straße 10 – 14, 24161 Altenholz, Dienstleister TSC
- Technische Universität Ilmenau, Ehrenbergstraße 29, 98693 Ilmenau, Bereitstellung Serverräume

