Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Zwischen der Verantwortlichen:

im Folgenden „**Auftraggeberin**“ oder „**AG**“

und der Auftragsverarbeiterin:

Technische Hochschule Ostwestfalen-Lippe
Campusallee 12
32657 Lemgo
im folgenden „**Auftragnehmerin**“ oder „**AN**“

werden folgende technisch-organisatorischen Maßnahmen festgelegt:

1. Hinweise

Die Auftraggeberin und die Auftragnehmerin, inklusive ihrer Subauftragnehmer, treffen geeignete technische und organisatorische Sicherheitsmaßnahmen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies geschieht unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowie der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung. Zudem werden die unterschiedliche Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen in Betracht gezogen.
Die Auftragsverarbeiterin und ihre Subauftragnehmer bieten hinreichend Garantien dafür, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Europäischen Datenschutz-Grundverordnung (DS-GVO) erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet.
In der Funktion als Auftragsverarbeiterin werden im Folgenden die bei der Auftragnehmerin getroffenen technischen und organisatorischen Maßnahmen zur Sicherung des geforderten Datenschutzniveaus beschrieben.

2. Festlegung des Schutzbedarfs

Im Rahmen der betriebenen Verfahren werden Daten mit unterschiedlichem, auch hohem, Schutzbedarf verarbeitet.
Nachfolgende Maßnahmen berücksichtigen diese Vorgabe.

3. Auflistung der technisch-organisatorischen Maßnahmen

VERTRAULICHKEIT

A. Zutrittskontrolle

(Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Wachdienst bzw. Pförtner, Alarmanlagen, Videoanlagen.)

I. Zutrittskontrolle zu Gebäuden / allgemeinen Räumen der HS OWL

a. Für den Publikumsverkehr zu definierten Zutrittszeiten geöffnet; darüber hinaus geschlossen. Darüber hinaus Zutritt für geschlossene Gruppen per Zugangsberechtigung (über Chip / RFID-Transponder) möglich.
b. mechanische Schließung mit Sicherheitsschlüsseln oder
c. elektronische Schließung mit einem Chip / RFID-Transponder.

II. Zutrittskontrolle zu den Büroräumen der HS OWL

a. Die Räumlichkeiten, in denen sich die PCs der Administratoren und Sachbearbeiter befinden, sind für die Dauer der Anwesenheit der Beschäftigten in dem Raum unverschlossen. Per Dienstanweisung ist das Verschließen der Räume beim Verlassen angeordnet.
b. Bei Abwesenheit der Beschäftigten sind die Räume verschlossen. Zugang zu diesen Räumlichkeiten erhalten nur autorisierte Beschäftigte mit Hilfe von Sicherheitsschlüsseln oder Chip / RFID-Transpondern.
c. Die Berechtigungsvergabe erfolgt im Rahmen eines genehmigungspflichtigen schriftlichen Antragsverfahrens über den jeweiligen Vorgesetzten. Alle Berechtigungen sind nachvollziehbar im Schlüsselsystem, zusätzlich in einer Tabelle, dokumentiert.

III. Zutrittskontrolle zu den Serverräumen / Rechenzentren der HS OWL

a. Einschränkung des Zutritts zum Serverraum auf durch eingegrenzten Personenkreis mit direktem Aufgabenbezug (ausschließlich Mitarbeiter S(kim)).

b. Externes Personal erhält nur Zutritt in Begleitung von Mitarbeitenden des S(kim).

c. Reinigung dieser Räume findet nur bei Bedarf unter Aufsicht von Mitarbeitenden des S(kim) statt.

d. Elektronische Schließung mit einem CHIP / RFID-Transponder und zusätzliche mechanische Schließung (Notschließung). Die Schlüssel für die Notschließung sind unter Verschluss. Nur ein Begrenzter Personenkreis aus der S(kim) Leitung hat hierauf Zugriff.

Technische Maßnahmen	Organisatorische Maßnahmen
• Alarmanlagen • Zäune, Pforten und andere räumliche Begrenzungen • Sicherheitsverglasung • Sicherung von Gebäudeschächten, Fenstern und Türen • Bewegungsmelder und Lichtschranken • Sicherheitsschlösser • Schließsysteme mit Codesperren • Chipkarten für verschlossene Bereiche • Zugangssperren, die mit biometrischen Merkmalen abgesichert sind • Datenschutzkonforme Videoüberwachung	• Besucheranmeldung • Besucherbücher und Besucherprotokolle • Verpflichtung für Mitarbeiter und Gäste, Ausweise zu tragen • Empfangspersonal zur Personenkontrolle und Pförtner • Sorgfältige Auswahl von Reinigungs- und Wachpersonal

Weitere Maßnahmen:

B. Zugangskontrolle

(Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei- Faktor-Authentifizierung, Verschlüsselung von Datenträgern.)

a. Persönlicher und individueller User-Log-In bei Anmeldung an dem jeweiligen System (Führendes System ist das IDM). Erlischt die Zugangsberechtigung, beispielsweise durch Austritt aus der Organisation, wird die Kennung gesperrt.

b. Kennwortverfahren (Vorgabe von Kennwort-Parametern hinsichtlich Komplexität und Aktualisierungsintervall).

c. Organisatorische Festlegung und Prüfung, wer für welche Ressourcen Zugangsberechtigungen erhält (Zugangsberechtigungen werden für Beschäftigte, Studierende und Externe vergeben).

d. IT-Systeme, die zur Verarbeitung personenbezogener Daten verwendet werden, sind passwortgeschützt. Benutzer können auf Daten nur zugreifen, sofern sie dazu berechtigt sind.

e. Benutzer sind per Dienstanweisung angewiesen, den PC beim Verlassen des Platzes zu sperren.

f. Dokumentation der Gruppenzugehörigkeit im IDM / AD.

g. Ein Element der Sicherheitsinfrastruktur ist ein mehrschichtiges Firewall-System, nach dem Stand der Technik (inklusive Wartungsvertrag).

Technische Maßnahmen	Organisatorische Maßnahmen
• Sichere VPN-Verbindung • Verschlüsselung von Datenträgern und mobilen Endgeräten • Sichere Firewall • Chipkarten • Anti-Viren-Software • Sperrung von USB-Anschlüssen und anderen externen Schnittstellen • Verriegelung von Gerätegehäusen • Authentifikation mittels Passworteingabe oder biometrischer Scans • Sicherheitsschlösser • Zwei-Faktor Authentifizierung	• Schlüsselregelungen • Passwortregeln inkl. Vorgaben für die Komplexität des Passwortes • Vertrauenswürdiges Personal für die Bereiche Sicherheit und Reinigung • Generierung von Benutzerprofilen • Zuordnung von Benutzerrechten

Weitere Maßnahmen:

C. Zugriffskontrolle

(Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.)

a. Der Zugriff auf personenbezogene Daten ist Berechtigten nur nach Eingabe der persönlichen Benutzerkennung und des Passwortes möglich.
b. Jeder Mitarbeiter erhält nur die Berechtigungen, die für die Erfüllung seiner Tätigkeit erforderlich sind.
c. Der externe Zugriff erfolgt transportverschlüsselt (SSL).
d. Das interne Netzwerk ist gegen unberechtigte Zugriffe aus dem Internet abgesichert.
e. Einsatz eines mehrschichtigen Firewall-Systems, nach dem Stand der Technik (inklusive Wartungsvertrag).
f. Verwaltung von differenzierten Berechtigungen innerhalb jeder Anwendung über Gruppen, soweit von der Anwendung unterstützt (z.B.: Administratoren, S(kim)-Mitarbeiter, Nutzer).
g. Protokollierungen
h. Geschirmtes, strukturiertes Netz.

Technische Maßnahmen	Organisatorische Maßnahmen
• Protokollierung der Zugriffe auf Anwendungen und Prozesse wie z.B. der Datenvernichtung • Datenschutzkonforme Vernichtung von Datenträgern (Akten, Laufwerke etc.) • Verschlüsselung von Datenträgern und mobilen Endgeräten • Identifizierungs- und Authentifizierungssystem • Sichere Aufbewahrung von Datenträgern	• Passwortregeln • Berechtigungskonzepte • Anpassung der Anzahl an Administratoren, die die volle Zugriffsberechtigung haben • Datenvernichtung durch Dienstleister • Datenschutzkonforme Passwortregeln • Protokollierung von Zugriffen • Vier-Augen-Prinzip bei Spezialanwendungen

Weitere Maßnahmen:

D. Trennungskontrolle

(Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit.)

a. Trennung von Anwendungen
b. Trennung von Datenbanken
c. Trennung von VM-Infrastrukturen
d. Multitier-Architektur
e. Wo immer technisch möglich, Einsatz von Mandaten-basierten Systemen.
f. Nutzung von gruppenbasierten Zugangsberechtigungen mit dokumentiertem, nachvollziehbaren, Berechtigungskonzept.

Technische Maßnahmen	Organisatorische Maßnahmen
• Verschlüsselung von Datensätzen, die aus dem selbem Zweck verarbeitet werden • Klare Trennung der für verschiedene Zwecke gespeicherten Daten	• Mandantentrennung • Auf die jeweiligen Datensätze angepasste Datenbankrechte und Berechtigungskonzepte • Steuerung über Berechtigungskonzept

Weitere Maßnahmen:

E. Pseudonymisierung

(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 entsprechenden technischen und organisatorischen Maßnahmen unterliegen.)

a. Für Test- und Entwicklungszwecke wird mit pseudo- oder anonymisierten Daten gearbeitet.
b. Sollten Daten für Zwecke der Statistik benötigt werden, werden diese pseudo- oder anonymisiert.

Technische Maßnahmen	Organisatorische Maßnahmen
• Automatische Verschlüsselung von Datensätzen inkl. Ablage des Entschlüsselung-Schlüssels mit Zugriffsberechtigung	• Manuelle Kürzung von Datensätzen • Manuelle Überschreibung von Datensätzen inkl. Wiederherstellungsprozess mit Berechtigung

Weitere Maßnahmen:

INTEGRITÄT

F. Weitergabekontrolle

(Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.)

a. Transportverschlüsselte Netzzugriffe.
b. Bereitstellung von VPN-Zugängen.

Technische Maßnahmen	Organisatorische Maßnahmen
• gesicherte Transportbehälter • Sichere VPN-Technologie • E-Mail-Verschlüsselung • Elektronische Signatur	• Einsatz von vertrauenswürdigem Transportpersonal • Regelmäßige Überprüfung von Abruf- und Übermittlungsvorgängen • Anfertigung eines Verfahrensverzeichnisses • Kontrolle der Datenempfänger und entsprechende Dokumentation dieser Empfänger

Weitere Maßnahmen:

G. Eingabekontrolle

(Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.)

a. Steuerung der Zugriffsrechte (IDM, AD, bzw. im betreffenden System).
b. Systemseitige Protokollierungen und anlassbezogene Auswertungen.
c. funktionelle Verantwortlichkeiten und entsprechende Berechtigungen.
d. Die Authentifizierung der User erfolgt durch Benutzername und Kennwort.

Technische Maßnahmen	Organisatorische Maßnahmen
• Anfertigung eines Protokolls bezüglich der Eingabe, Veränderung und Löschung von Daten • Digitales Berechtigungskonzept (z.B. Active Directory)	• Einrichtung und Verwendung von individuellen Benutzernamen • Vergabe von Zugriffsberechtigungen

Weitere Maßnahmen:

VERFÜGBARKEIT

H. Verfügbarkeitskontrolle

(Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.)

a. Betrieb der Infrastruktur in den beiden getrennten Rechenzentren mit
   i. redundanter Stromversorgung und unterbrechungsfreier Stromversorgung (USV)
   ii. Klimaanlagen
   iii. Monitoring
b. Verwendung von redundanter Server-, Storage- und Netzinfrastruktur
c. Clustering: Server, Storage, Datenbank-Management-System (DBMS)
d. Application Delivery Controller (ADC) für Web-Dienste
e. Einbindung in ein Backup-Verfahren, Prüfung des Restores erfolgt durch Anforderungen im täglichen Betrieb
f. Rasche Wiederherstellbarkeit personenbezogener Daten
g. Vertretungsregelung bei den Administratoren.
h. Virenschutz / Firewall
i. Abschluss von Serviceverträgen

Technische Maßnahmen	Organisatorische Maßnahmen
• Backups • Diebstahlsicherungen • Klimatisierung des Serverraums durch eine Klimaanlage • USV (Unterbrechungsfreie Stromversorgung) • Feuer- und Rauchmelder • Feuerlöscher • Datenschutz-Management-System • Notfall-Management • Virenschutz • Firewall/ IDS	• Alarmanlagen • Schutz des Serverraums vor Risiken, z.B. durch Hochwasser, Brände oder gefährlich platzierte Sanitäranlagen • Erstellung von Backups der Daten • Zyklus der Backups-Anfertigung • Tests für Datenwiederherstellungen

Weitere Maßnahmen:

I. BELASTBARKEIT

a. Einsatz gespiegelter und geclusterter Systeme.

b. Regelmäßige Revision des IT-Verbundes / ggf. Anpassungen

4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

A. Auftragskontrolle

(Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement.)

a. Auftragsverarbeitungsvertrag und dessen regelhafter Prüfung.

B. Dokumentation / Revision

a. Einsatz eines Datenschutz-Management-Systems (im Aufbau)
b. Aufnahme und Aktualisierung im Verzeichnis der Verarbeitungstätigkeiten.
c. Erstellung und Aktualisierung einer Verarbeitungsdokumentation.
d. Regelmäßige Prüfung durch die Datenschutzbeauftragte und den Informationssicherheitsbeauftragten Sicherheitsbeauftragten.

Technische Maßnahmen	Organisatorische Maßnahmen
•	• Sorgfältige Auswahl des Auftragnehmers • Überprüfung der Datenvernichtung nach Auftragsende • Vertragsstrafen • Schriftliche Weisungen an den Auftragnehmer • Vereinbarung von wirksamen Kontrollrechten bezüglich des Auftragnehmers • Dauerhafte Überprüfung des Auftragnehmers

Weitere Maßnahmen:

5. Versionierung

Version	Datum	Wer	Änderung
1.0	22.11.2018	Stock	Übernahme der durch Hrn. Ebert erstellten Vorlage. Umbenennung der Datei. Ergänzung einer Versionierung.
1.1	22.11.2018	Stock	Änderungen, lt. Änderungsnachverfolgung übernommen. Fußzeile angepasst. Einleitung mit Definition Auftraggeber (AG) und Auftragnehmer (AN) eingefügt.
1.2	26.11.2018	Stock	Abstimmung der Inhalte mit Dr. Köller & DSB
1.3	23.03.2023	Meister	Einfügen des TLP. Aufteilung der technischen und organisatorischen Maßnahmen.