Technische und organisatorische Maßnahmen (TOM‘s) zur E-Learning-Umgebung

Die E-Learning-Umgebung wird durch einen deutschen Unterauftragnehmer auf deutschen Servern gehostet. DECD GmbH hat die technischen und organisatorischen Maßnahmen der Unterauftragnehmer sowie deren Unterauftragnehmern geprüft, sofern für die Verarbeitung relevant.

TOM’s des beauftragten Unterauftragnehmers:	https://eledia.de/docs/eLeDia_ADV_DSGVO.pdf
TOM’s des relevanten weiteren Unterauftragnehmers (für Hosting):	https://www.hetzner.com/AV/TOM.pdf

1 Hinweise zur Aktualität und Querverweise

Die aktuellen Versionen der Datenschutzinformationen können auf unserer Webseite abgerufen werden.

Weiterführende Links zum Datenschutz, zur Auftragsverarbeitung sowie Kontaktdaten:
https://decd-health.com/datenschutz/
https://decd-health.com/datenschutz/auftragsverarbeitung-e-learning/

Datenschutzerklärung für die E-Learning-Umgebung:
https://decd-health.com/datenschutz/datenschutz-e-learning/

Auftragsverarbeitungsvertrag (basierend auf den Standardvertragsklauseln SCC 2021 der Europäischen Kommission für Verantwortliche und Auftragsverarbeiter in der EU / im EWR):
https://decd-health.com/wp-content/pdf/AV_Vertrag_e_Learning.pdf

Liste der Unterauftragnehmer:
https://decd-health.com/wp-content/pdf/Liste_UAN_e_Learning.pdf

Technische und organisatorische Maßnahmen (TOM’s):
https://decd-health.com/wp-content/pdf/TOM_e_Learning.pdf

DECD GmbH
Geschäftsführerin
Ines Hartwig-Zaidan
Rosenstr. 18
16278 Angermünde

Tel 03331 30 10 713
Fax 03331 30 11 183
contact@decd-health.com
IBAN: DE75 1004 0000 0641 3355 00
BIC: COBADEFFXXX

Sitz der Gesellschaft: Angermünde,
Registergericht Neuruppin
IK Nr. 501102298
USt-IdNr. 356726690
HRB 14003 NP

2 Pseudonymisierung und Verschlüsselung personenbezogener Daten

- Die Abfrage und Übertragung personenbezogener Daten durch Anwender erfolgt verschlüsselt mittels Webbrowser (https). Passwörter der Nutzer werden in der Datenbank nach Möglichkeit verschlüsselt abgelegt.
- Eine Pseudonymisierung von Nutzer-Accounts kann auf Wunsch gewährleistet werden.

3 Fortdauernde Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

3.1 Vertraulichkeit

- Mitarbeiter sind über die Bedeutung des Datenschutzes aufgeklärt und werden regelmäßig sensibilisiert.

Prüfung bei Unterauftragnehmern:

- Die Vertraulichkeit beim Unterauftragsnehmer und dessen Unterauftragnehmer ist angemessen.

3.2 Zutrittskontrolle

- Ein Schließsystem mit Sicherheitsschlössern ist vorhanden.
- Es erfolgt eine dokumentierte Schlüsselvergabe an eine begrenzte Anzahl und nur berechtige Mitarbeiter.
- Der Zutritt von Besuchern ist nur in Begleitung durch Mitarbeiter zulässig.
- Der Zutritt von Besuchern bei Unterauftragnehmer (z.B. Zutritt zu Servern) erfüllt ein angemessenes Schutzniveau.

Prüfung bei Unterauftragnehmern:

- Die Zutrittskontrolle beim Unterauftragsnehmer und dessen Unterauftragnehmer ist angemessen.

3.3 Zugangskontrolle

- Es erfolgt eine Begrenzung der Zugangsberechtigten.
- Den Benutzern werden Benutzerrechte in Abhängigkeit von den von ihnen ausgeübten Funktionen zugewiesen.
- Eine Authentifizierung erfolgt mit Benutzernamen und Passwort.

DECD GmbH
Geschäftsführerin
Ines Hartwig-Zaidan
Rosenstr. 18
16278 Angermünde

Tel 03331 30 10 713
Fax 03331 30 11 183
contact@decd-health.com
IBAN: DE75 1004 0000 0641 3355 00
BIC: COBADEFFXXX

Sitz der Gesellschaft: Angermünde,
Registergericht Neuruppin
IK Nr. 501102298
USt-IdNr. 356726690
HRB 14003 NP

- Es existieren technische Vorgaben zur Passwortgestaltung (Mindestlänge, Mindestkomplexität).
- Der Zugang erfolgt über unternehmenseigene Endgeräte.
- Es wird auf allen PCs Antivirensoftware mit automatisierter Aktualisierung eingesetzt.
- Der Zugang bei Unterauftragnehmern (z.B. als Serveradmin) erfolgt zusätzlich durch eine Mehrfaktor-Authentifizierung bzw. Richtlinien zur selbständigen Vergabe und regelmäßigen Erneuerung des Passwortes dem Schutzniveau angemessen.

Prüfung bei Unterauftragnehmern:

- Die Zugangskontrolle beim Unterauftragsnehmer und dessen Unterauftragnehmer ist angemessen.

3.4 Zugriffskontrolle

- Die Zugriffsberechtigungen werden in Abhängigkeit von der Funktion eines Mitarbeiters vergeben.
- Die Anzahl der Administratoren ist begrenzt.
- Die Anzahl der Koordinatoren-Accounts der Kunden-Mitarbeiter ist begrenzt.
- Der Zugriff auf Anwendungen wird protokolliert (Logdaten).
- Für die Vernichtung papiergebundener personenbezogener Daten stehen Aktenvernichter zur Verfügung.
- Sicherheitsupdates werden regelmäßig durchgeführt.

Prüfung bei Unterauftragnehmern:

- Die Zugriffskontrolle beim Unterauftragsnehmer und dessen Unterauftragnehmer ist angemessen.

3.5 Trennungskontrolle

- Pro Kunde (z.B. Klinik, medizinische Einrichtung) wird ein eigener Bereich angelegt.
- Patienten- und Koordinatoren-Zugänge werden dem Kunden zugeordnet.
- Auf Angehörigen-Zugänge hat der Kunde keinen Zugriff.
- Die Unterauftragnehmer stellen u.a. sicher, dass die Datensicherung auf logisch und/oder physisch getrennten Systemen erfolgt.

Prüfung bei Unterauftragnehmern:

- Die Trennungskontrolle beim Unterauftragsnehmer und dessen Unterauftragnehmer ist angemessen.

DECD GmbH
Geschäftsführerin
Ines Hartwig-Zaidan
Rosenstr. 18
16278 Angermünde

Tel 03331 30 10 713
Fax 03331 30 11 183
contact@decd-health.com
IBAN: DE75 1004 0000 0641 3355 00
BIC: COBADEFFXXX

Sitz der Gesellschaft: Angermünde,
Registergericht Neuruppin
IK Nr. 501102298
USt-IdNr. 356726690
HRB 14003 NP

3.6 Verfügbarkeit und Belastbarkeit der Systeme

- Es stehen automatisierte Berichte zur Verfügung, die die Performance, Sicherheit sowie den Systemstatus der E-Learning-Umgebung ausweisen.
- Es erfolgen automatische tägliche Backup-Sicherungen.
- Vor größeren Updates erfolgt zusätzlich eine manuelle Sicherung aller Kurse.
- Bei den Unterauftragnehmern existieren zusätzlich Eskalationsketten zur kurzfristigen Wiederherstellbarkeit von Daten sowie weitere technische Sicherungen.

Prüfung bei Unterauftragnehmern:

- Die Verfügbarkeits- und Belastbarkeitskontrolle der Systeme beim Unterauftragsnehmer und dessen Unterauftragnehmer ist angemessen.

3.7 Dienste im Zusammenhang mit der Verarbeitung

- Zusätzliche Dienste können nur nach aktiver Beauftragung von DECD an den Unterauftragnehmer aktiviert werden.
- Sofern Dienste im Zusammenhang mit der Verarbeitung eingesetzt werden, wird deren Funktionalität im Rahmen von Tests nach Updates / Upgrades bzw. im Rahmen der oben genannten Berichte getestet und beobachtet.
- Unterauftragnehmer informieren regelmäßig über Neuerungen und technische Hinweise, so dass diese ggf. kurzfristig deaktiviert werden können.

4 Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

- Regelmäßige Wiederherstellungstests von Kursen finden nach jedem Update/Upgrade statt.
- Beim Unterauftragnehmer kann bei Bedarf die Wiederherstellung der Daten aus den Backups jederzeit beauftragt werden. Die Wiederherstellbarkeit wird exemplarisch bzw. nach gesonderter Beauftragung durch DECD geprüft.

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

- Diese technischen organisatorischen Maßnahmen werden regelmäßig überprüft und bei Bedarf angepasst. Diese Überprüfung erfolgt in der Regel jährlich. Der Stand der Technik hier hierbei beachtet.
- Die technischen und organisatorischen Maßnahmen des/der Unterauftragnehmer werden ebenfalls regelmäßig überprüft.
- Beim relevanten Unterauftragnehmer, der das Hosting übernimmt ist ein Datenschutz-Informationssicherheits-Management-System sowie ein Incident-Response-Management vorhanden.
- Datenschutzfreundliche Voreinstellungen mit Blick auf den Verarbeitungszweck werden vorgenommen.

Prüfung bei Unterauftragnehmern:

- Die Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen beim Unterauftragsnehmer und dessen Unterauftragnehmer sind angemessen.

6 Identifizierung und Autorisierung der Nutzer

- Nutzer können in der Lernumgebung durch die IP-Adresse, eindeutige System-ID oder durch Kunden vergebene ID sowie hinterlegte Email-Adresse, Klarnamen oder Pseudonym ermittelt werden.
- Eine „Gastnutzung" des Systems ist nicht zulässig.
- Nutzer erhalten den Zugang über den Kunden (z.B. Klinik oder medizinische Einrichtung) oder von DECD direkt.

7 Schutz der Daten während der Übermittlung

(Siehe: 2 Pseudonymisierung und Verschlüsselung personenbezogener Daten, Seite 2)

8 Schutz der Daten während der Speicherung

(Siehe: 2 Pseudonymisierung und Verschlüsselung personenbezogener Daten, Seite 2)

9 Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

(Siehe: 3.2 Zutrittskontrolle, Seite 2)

10 Gewährleistung der Protokollierung von Ereignissen

- Es werden automatisch Logdaten und Fehlerberichte für verschiedene Ereignisse protokolliert, auf die nur die Administratoren Zugriff haben.

11 Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

- Nur eine begrenzte Anzahl der Administratoren darf das System konfigurieren.
- Der Hauptadministrator stimmt zusammen mit der Geschäftsführung die Standardkonfiguration ab.

12 Interne Governance und Verwaltung der IT und der IT-Sicherheit

- Mitarbeiter, insbesondere Administratoren der E-Learning-Umgebung, werden regelmäßig in den Bereichen Datenschutz und Informationssicherheit sensibilisiert.
- Mitarbeiter, insbesondere Administratoren, greifen nur mit firmeneigenen Endgeräten auf die E-Learning-Umgebung zu.
- Datensicherheitsvorfälle werden über die Geschäftsführung eskaliert.
- Bei Einführung neuer Prozesse innerhalb der E-Learning-Umgebung erfolgt eine Risikobetrachtung nach Datenschutzgrundsätzen.
- Sofern DECD im täglichen Betrieb Unregelmäßigkeiten beobachtet, wird der Unterauftragnehmer zur Klärung kontaktiert.

13 Zertifizierung/Qualitätssicherung von Prozessen und Produkten

- Derzeit liegen keine Zertifizierungen für die E-Learning-Umgebung der DECD GmbH vor. Eine Zertifizierung als digitale Gesundheitsanwendunge (DiGA) ist in Planung.
- Die Inhalte der E-Learning-Umgebung werden vor Veröffentlichung durch qualifiziertes medizinisches Fachpersonal geprüft.
- Der Unterauftragnehmer ist als „Moodle Partner (Premium Certified Services Provider)“ gelistet. (https://moodle.com/partners/eledia/)
- Der relevante Unterauftragnehmer für das Hosting ist DIN ISO/IEC 27001 zertifiziert. (https://www.hetzner.com/de/unternehmen/zertifizierung/)

DECD GmbH
Geschäftsführerin
Ines Hartwig-Zaidan
Rosenstr. 18
16278 Angermünde

Tel 03331 30 10 713
Fax 03331 30 11 183
contact@decd-health.com
IBAN: DE75 1004 0000 0641 3355 00
BIC: COBADEFFXXX

Sitz der Gesellschaft: Angermünde,
Registergericht Neuruppin
IK Nr. 501102298
USt-IdNr. 356726690
HRB 14003 NP

14 Gewährleistung der Datenminimierung

- Datenschutzfreundliche Voreinstellungen mit Blick auf den Verarbeitungszweck werden vorgenommen.
- Bei Einführung neuer Prozesse innerhalb der E-Learning-Umgebung erfolgt eine Risikobetrachtung nach Datenschutzgrundsätzen.

15 Gewährleistung der Datenqualität

- Korrektheit (sachliche Übereinstimmung mit der Realität):
  - Nach Account-Anlage können Nutzer im eigenen Account bei Bedarf ihren Namen sowie ihre Email-Adresse selbst ändern.
  - Administratoren können diese Daten nach Aufforderung ebenfalls berichtigen.
  - Andere Nutzerdaten können standardmäßig nicht verändert werden.

- Konsistenz (Übereinstimmung von Daten aus verschiedenen Systemen):
  - Derzeit findet keine automatisierte Übertragung aus oder in andere Systeme statt.
  - Sofern Kunden Klarnamen und/oder weitere personenbezogenen Daten an DECD GmbH übermitteln obliegt die Kontrolle dem Kunden.

- Vollständigkeit (notwendige Attribute und Werte):
  - Mit Blick auf Datenminimierung werden nur wenig personenbezogene Daten gesammelt.
  - Für alle in der E-Learning-Umgebung vorhanden Prozessschritte wird auf die Softwaredokumentation in der jeweils gültigen Version verwiesen.

- Einheitlichkeit (Daten liegen im passenden und selben Format vor):
  - Innerhalb der E-Learning-Umgebung werden die Daten im .json-Format abgelegt.

- Redundanzfreiheit (Dubletten innerhalb der Datensätze):
  - Pro Nutzer wird technisch systemweit eine zentrale fortlaufende ID vergeben.
  - Vor der Nutzeranlage wird technisch geprüft, ob gleiche Daten bereits im System sind.
  - Pro Nutzer wird nur ein Account angelegt. Mit diesem Account sind alle weiteren Aktivitäten verbunden.

DECD GmbH
Geschäftsführerin
Ines Hartwig-Zaidan
Rosenstr. 18
16278 Angermünde

Tel 03331 30 10 713
Fax 03331 30 11 183
contact@decd-health.com
IBAN: DE75 1004 0000 0641 3355 00
BIC: COBADEFFXXX

Sitz der Gesellschaft: Angermünde,
Registergericht Neuruppin
IK Nr. 501102298
USt-IdNr. 356726690
HRB 14003 NP

- Genauigkeit und Aktualität (Daten in ausreichender Zahl, aktueller Zustand):
  - Alle Aktivitäten des Nutzers sind mit einem eindeutigen Nutzerkonto verbunden.
  - Die webbasierte E-Learning-Umgebung arbeitet mit LIVE-Daten der Nutzer.

- Verständlichkeit und Zuverlässigkeit der Daten
  (eindeutige Interpretierbarkeit und Nachvollziehbarkeit der Daten):
  - Für alle in der E-Learning-Umgebung vorhanden Prozessschritte wird auf die Softwaredokumentation in der jeweils gültigen Version verwiesen.

- Relevanz (Deckung Informationsbedarf):
  - Innerhalb der E-Learning-Umgebung gibt es ein Rollen- und Berechtigungskonzept zur Sicherstellung der Datenminimierung und Informationsverarbeitung.

- Verfügbarkeit (sind Daten für berechtigte Nutzer zugänglich?)
  - Kunden und Nutzer werden im Vorfeld darauf hingewiesen, dass es sich bei der E-Learning-Umgebung um eine webbasierte Lösung handelt und welche technischen Voraussetzungen notwendig sind.
  - Das Rollen- und Berechtigungskonzept stellt sicher, dass die jeweiligen Rollen Zugriff auf relevante Daten haben.
  - Innerhalb der E-Learning-Umgebung ist zusätzlich ein Auskunftsprozess für personenbezogene Daten zum Nutzerkonto integriert. Die Nutzer erhalten nach Freigabe einen Download mit allen gespeicherten Daten bzw. eine Löschbestätigung.
    (Datenanfragen: „Alle über mich gespeicherten Daten exportieren" sowie „Alle über mich gespeicherten Daten löschen").

16 Gewährleistung einer begrenzten Vorratsdatenspeicherung

- Es findet keine Vorratsdatenspeicherung statt.
- Die aktuelle Datenschutzerklärung für die E-Learning-Umgebung mit aktueller Speicherdauer bzw. Löschfristen (teilweise automatisiert) ist hier hinterlegt: https://decd-health.com/datenschutz/datenschutz-e-learning/

17 Gewährleistung der Rechenschaftspflicht

- DECD hat intern einen Zuständigen für Datenschutz bestimmt.
- Die Datenschutzdokumentation wird regelmäßig überprüft und aktualisiert.

DECD GmbH
Geschäftsführerin
Ines Hartwig-Zaidan
Rosenstr. 18
16278 Angermünde

Tel 03331 30 10 713
Fax 03331 30 11 183
contact@decd-health.com
IBAN: DE75 1004 0000 0641 3355 00
BIC: COBADEFFXXX

Sitz der Gesellschaft: Angermünde,
Registergericht Neuruppin
IK Nr. 501102298
USt-IdNr. 356726690
HRB 14003 NP

18 Ermöglichung der Datenübertragbarkeit und Gewährleistung der Löschung

- Die aktuelle Datenschutzerklärung für die E-Learning-Umgebung mit aktueller Speicherdauer bzw. Löschfristen (teilweise automatisiert) ist hier hinterlegt: https://decd-health.com/datenschutz/datenschutz-e-learning/
- Nutzer können in der E-Learning-Umgebung oder Kontaktaufnahme zu DECD ihre personenbezogenen Daten abfragen bzw. löschen lassen.
  (Datenanfragen: „Alle über mich gespeicherten Daten exportieren" sowie „Alle über mich gespeicherten Daten löschen").
- Derzeit findet keine automatisierte Übertragung aus oder in andere Systeme statt. Die Speicherung der Daten im .json-Format ermöglicht allerdings potentielle Datenübertragungen in Zukunft.

Stand: Juli 2024

DECD GmbH
Geschäftsführerin
Ines Hartwig-Zaidan
Rosenstr. 18
16278 Angermünde

Tel 03331 30 10 713
Fax 03331 30 11 183
contact@decd-health.com
IBAN: DE75 1004 0000 0641 3355 00
BIC: COBADEFFXXX

Sitz der Gesellschaft: Angermünde,
Registergericht Neuruppin
IK Nr. 501102298
USt-IdNr. 356726690
HRB 14003 NP