Technische und organisatorische Maßnahmen

Zum Schutz der personenbezogenen Daten, die im Auftrag durch die Cornelsen eCademy und inside GmbH im Rahmen der Bereitstellung der eCademy Lernplattfporm verarbeitet werden, wurden folgende Maßnahmen getroffen, die regelmäßig überprüft werden.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Der Auftragnehmer trifft die nachfolgenden technischen und organisatorischen Maßnahmen zur angemessenen Sicherung personenbezogener Daten vor unbefugtem Zugriff und unbefugter Weitergabe.

Es bestehen Berechtigungskonzepte für die Vergabe von Zutritts-, Zugangs- und Zugriffsrechten der Mitarbeiter. Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, durch folgende Maßnahmen verwehrt (Zutrittskontrolle):

- Eine Schließanlage sichert das Gebäude, in dem die Geschäftsräume liegen, vor dem Zutritt Unbefugter. Für den Zutritt zu den Büros werden mechanische Schlösser als Schließmechanismus genutzt. Es besteht eine Schlüsselausgaberegelung. Die Schlüsselausgabe wird protokolliert.
- Außerhalb der Geschäftszeiten sind die Räumlichkeiten abgeschlossen und durch eine Alarmanlage, welche bei einem örtlichen Sicherheitsdienst aufgeschaltet ist, gesichert.
- Unbefugten wird der Zugang zu Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, durch folgende Maßnahmen verwehrt (Zugangskontrolle):
- Der Zugang zu allen Datenverarbeitungssystemen ist durch personenbezogene Zugangskennungen und individuellen Passwörtern geschützt.
- Der Kreis der Personen mit Zugang zu den Systemen und Anwendungen der Datenverarbeitung ist konkret festgelegt. Es bestehen konkrete Regelungen für die Vergabe von Berechtigungen. Bei der Vergabe von Berechtigungen ist sichergestellt, dass Benutzer nur die im Rahmen ihrer Aufgabenerfüllung erforderlichen Berechtigungen erhalten (Minimalprinzip). Berechtigungen werden nach dem Minimalprinzip vergeben. Die Einhaltung des Minimalprinzips stellt sicher, dass die Beschäftigten der Cornelsen eCademy jeweils nur auf die im Rahmen ihrer Aufgabenerfüllung erforderlichen Systeme und Anwendungen Zugriff haben und der Zugriff auf Verzeichnisse und Daten auf den für die konkrete Tätigkeit erforderlichen Umfang beschränkt ist.
- Alle Datenverarbeitungssysteme des Auftragnehmers sind nur nach passwortgestützter Authentifizierung nutzbar.
- Beschäftigte der Cornelsen eCademy, die über einen Arbeitsplatzrechner verfügen, erhalten ein aus Benutzername und Kennwort bestehendes persönliches Benutzerkonto. Benutzer müssen sich bei jeder Anmeldung mit Benutzername und Kennwort gegenüber dem System authentifizieren. Nach einer bestimmten Inaktivität erfolgt eine automatische, passwortgeschützte Bildschirm- bzw. Rechnersperre.
- Die Firewall ist eingerichtet, um den Zugang von Unbefugten zu den Datenverarbeitungssystemen zu verhindern und wird regelmäßig upgedatet.

Unbefugten wird der Zugriff auf personenbezogene Daten durch folgende Maßnahmen verwehrt (Zugriffskontrolle):

- Innerhalb der Berechtigungskonzepte werden Rollen der Mitarbeiter definiert, die mit unterschiedlichen Berechtigungen einhergehen.

- Die Vergabe von Berechtigungen wird dokumentiert.
- Zusätzlich bestimmt das verwendete Rollen- und Rechtemodell, welche Benutzer eines Mandanten die o.g. Funktionen ausführen können.

Trennungskontrolle

- Die für die Anwendung verwendeten Daten sind ausschließlich solche Daten, die zur Nutzung der Anwendung durch den Auftraggeber erforderlich sind.
- Mittels technischer Maßnahmen in der Anwendung wird innerhalb der Anwendung eine logische Trennung der Daten zwischen den Mandanten gewährleistet, sodass Benutzer eines Mandanten nur die Daten dieses Mandanten sehen oder ändern, bzw., löschen können.
- Test- und Produktivdaten liegen in getrennter Infrastruktur.

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

Nach Art. 32 Abs. 1 lit b DSGVO ist die Integrität der Datenverarbeitung zu gewährleisten.

Cornelsen eCademy trägt dafür Sorge, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dazu gehören unter anderem Weitergabe- und Transportkontrolle sowie Eingabekontrolle.

Weitergabe- und Transportkontrolle

- Sämtliche Datenübermittlung und Kommunikation zwischen Nutzern (Auftraggeber oder Auftragnehmer) und Anwendung nutzt Transportverschlüsselung (TLS, Transport Layer Security mit AES 128-Verschlüsselung)
- Personenbezogene Daten sind auf den Cloudservern auch bei der Speicherung (at rest) verschlüsselt.
- Dokumente mit personenbezogenen Daten werden über einen externen Dienstleister datenschutzgerecht vernichtet.
- Der Transport von personenbezogenen Daten auf mobilen Datenträgern (USB-Stick, CD-ROM, DVD) findet nicht statt.

Der Auftragnehmer trägt dafür Sorge, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)

- Die Eingabe, Änderung und Löschung von Daten werden protokolliert (Logs).
- Änderungen an persönlichen Daten und Rollenzuweisungen in der Cornelsen eCademy Lernplattform werden protokolliert. Hierbei werden Art der Änderungen und die Identität der die Änderungen durchführenden Person gespeichert. Die Protokollierung erfolgt beim Anlegen, Ändern und Löschen von persönlichen Daten und Rollenzuweisungen.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Der Auftragnehmer trägt dafür Sorge, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

- Die Daten werden täglich gesichert.

- Wir verwenden geeignete Sicherheitsmaßnahmen (z.B. 2-Faktor-Authentifizierung), um den Zugriff auf Backups zu schützen.
- Die IT-Systeme sind technisch vor unbefugten Datenzugriffen mittels aktualisiertem Virenschutz und Spamfilter geschützt.
- Nur die mit der Verwaltung der IT-Systeme beauftragten Personen haben administrativen Zugang zu den IT-Systemen.
- Alarmanlage ist vorhanden.

Der Auftragnehmer trägt dafür Sorge, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle).

- Daten des Auftraggebers werden nur nach dokumentierter Weisung verarbeitet.
- Mitarbeiter, die mit der Auftragsverarbeitung betraut sind, erhalten regelmäßig Schulungen zum Thema Datenschutz und werden sensibilisiert.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Der Auftragnehmer verpflichtet sich der Datenschutzrichtlinie der Franz Cornelsen Bildungsholding GmbH & Co. Kg. Ziel dieser Richtlinie ist es, innerhalb der FCBG ein einheitliches und hohes Niveau für den Schutz personenbezogener Daten und somit des Grundrechts jeder Person auf informationelle Selbstbestimmung zu gewährleisten und die Einhaltung der entsprechenden Datenschutzgesetze sicherzustellen. Hierzu stellt diese Richtlinie grundlegende Regeln für den Umgang mit personenbezogenen Daten auf und legt eine Organisation für den Datenschutz fest.
- Es existiert ein Prozess zur Meldung von Datenschutzverstößen, insbesondere in der Zusammenarbeit mit dem Verantwortlichen (Incident Response Management).
- Mit externen Dienstleistern, die personenbezogene Daten im Auftrag verarbeiten, werden schriftliche Verträge zur Auftragsverarbeitung nach Maßgabe von Art. 28 Abs. 3 DSGVO abgeschlossen.
- Der Auftragnehmer hat schriftlich einen Beauftragten für den Datenschutz bestellt.
- Alle Beschäftigten sind auf das Datengeheimnis bzw. die Vertraulichkeit verpflichtet. Sie werden zu Themen Datenschutz und Datensicherheit durch Schulungen vertraut gemacht und sensibilisiert.