Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 DS-GVO

Stand: 02.01.2023 | Version 1.2

Vorwort

Die Auftragnehmerin erhebt, verarbeitet und nutzt personenbezogene Daten von Kunden im Rahmen der Auftragsabwicklung und der beauftragten Geschäftsprozesse. Die vorliegenden technischen und organisatorischen Maßnahmen regeln den Umgang mit den personenbezogenen Daten gem. Art. 32 Abs. 1 DS-GVO zum Schutze der Vertraulichkeit, der Integrität, der Verfügbarkeit und Belastbarkeit sowie die Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Datenschutzmaßnahmen.

Inhalt

1. Gültigkeit

Version 1.2 - Erstellung am 02.01.2023

Cornelsen eCademy & inside GmbH

2. Verantwortliche Stelle

Cornelsen eCademy & inside GmbH

Geschäftsführung **Jan Peter aus dem Moore** E-Mail: jpadmoore@ecademy-learning.com	**Geschäftsführung** **Anja Sixt** E-Mail: asixt@ecademy-learning.com

Externer Datenschutzbeauftragter

datenschutz nord GmbH

Konsul-Smidt-Straße 88

28217 Bremen

Tel.: +49 421 69 66 32 0

Fax: +49 421 69 66 32 11

office@datenschutz-nord.de

www.datenschutz-nord-gruppe.de

3. Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 DS-GVO

3.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

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.

3.1.1 Zutrittskontrolle

Ziel ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.

Maßnahmen

- Die Geschäftsräume des Auftragnehmers sind durch eine Schließanlage gesichert und nur mit entsprechenden Schlüsseln zugänglich. Es besteht eine Schlüsselausgaberegelung. Die Schlüsselausgabe wird protokolliert. Es gibt ein Konzept mit getrennten Sicherheitszonen, welches z.B. auch den Zugang von Externen je Zone regelt.
- Elektronische Zugangskontrollsysteme überwachen, protokollieren und gewährleisten den Zutritt zum Firmengebäude nur für autorisierte Personen.
- Besucher oder Dienstleister müssen sich anmelden und werden beaufsichtigt.
- Außerhalb der Geschäftszeiten sind die Räumlichkeiten abgeschlossen und durch eine Alarmanlage abgesichert, welche mit einem Sicherheitsunternehmen verbunden ist, welches 24/7 mit Personal besetzt ist.
- Im Alarmfall wird automatisch das Sicherheitsunternehmen informiert, welches umgehend das Gebäude überprüft.
- Zutritt zu den Serversystemen ist nur über ein separates Schließsystem möglich. Die Empfänger aller ausgegebenen Schlüssel sind dokumentiert.

3.1.2 Zugangskontrolle

Ziel ist es, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen

- Benutzerkonten werden nur durch gesonderte Administratorenkonten gemäß Berechtigungskonzept vergeben und dokumentiert.
- Es besteht für alle Systeme eine eindeutige Zuordnung von Benutzerkonten zu Benutzern. Das Teilen von Nutzerkonten ist nicht gestattet.
- Alle Systeme sind durch Passwörter entsprechend der Passwort-Gruppenrichtlinie geschützt. Wenn verfügbar, wird Single-Sign-On oder MFA in der jeweiligen Anwendung genutzt.
- Die interne Infrastruktur wird durch Firewalls, Webfilter, Virenscanner und Intrusion Detection Systeme geschützt.
- MitarbeiterInnen sind angewiesen, bei jedem Verlassen des Arbeitsplatzes den Bildschirm bzw. Rechner zu sperren. Dies erfolgt nach 10 Minuten Inaktivität automatisch.
- Der Zugang auf Kundensysteme erfolgt verschlüsselt und sind durch eine 2-Faktor-Authentifizierung abgesichert.
- Der Zugang zu Kundensystemen wird immer nur dem kleinsten erforderlichen Mitarbeiterkreis genehmigt.
- Alle eingesetzten Notebooks im Unternehmen sind verschlüsselt.

3.1.3 Zugriffskontrolle

Ziel ist es zu gewährleisten, dass unerlaubte Tätigkeiten in IT-Systemen außerhalb eingeräumter Berechtigungen verhindert werden, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen

- Es bestehen konkrete Regelungen für den Berechtigungsumfang verschiedener Benutzerrollen. Es ist sichergestellt, dass Benutzer nur die im Rahmen ihrer Aufgabenerfüllung erforderlichen Berechtigungen erhalten.
- Zugriff wird jeweils nur gewährt auf die im Rahmen ihrer Aufgabenerfüllung erforderlichen Systeme und Anwendungen sowie Verzeichnisse und Daten im erforderlichen Umfang für die konkrete Tätigkeit (Need-to-know-Prinzip).
- Die Vergabe von Berechtigungen wird dokumentiert und auch regelmäßig überprüft.
- Es erfolgt eine Protokollierung von Zugriffen.

3.1.4 Trennungskontrolle

Ziel ist es zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen

- Mittels technischer Maßnahmen wird eine Trennung der Daten zwischen den Mandanten gewährleistet, sodass Benutzer eines Mandanten nur die Daten dieses Mandanten sehen oder ändern bzw. löschen können. Die Berechtigungen sind entsprechend organisiert.
- Es existieren Funktionstrennungen für Produktion und Test.
- Bei pseudonymisierten Daten wird die Aufbewahrung der Zuordnungsdatei auf einem getrennten, abgesicherten IT-System gewährleistet.

3.1.5 Pseudonymisierung

Wo möglich passiert die Verarbeitung personenbezogener Daten, dass die Daten ohne Hinzuziehung zusätzlicher Informationen, die gesondert aufbewahrt werden, nicht mehr einer spezifischen betroffenen Person zugeordnet werden können:

- Datensätzen werden vor der Übermittlung um identifizierende Merkmale gekürzt.
- Der Ausschluss der (Re-)Identifizierung von Merkmalen wird durch Berechtigungen gewährleistet.

3.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Der Auftragnehmer trifft die nachfolgenden technischen und organisatorischen Maßnahmen um sicherzustellen, dass personenbezogene Daten nicht (unbemerkt) geändert werden können. Dazu gehören unter anderem Weitergabe- und Transportkontrolle sowie die Eingabekontrolle.

3.2.1 Weitergabekontrolle

Ziel ist es zu 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.

Maßnahmen

- Der Zugriff auf die Systeme, welche personenbezogene Daten beinhalten, erfolgt über verschlüsselte Verbindungen.
- Der Zugriff ist nur für die erforderlichen Personen über separate Zugangsdaten abgesichert möglich.
- Es erfolgt eine Protokollierung von Zugriffen.
- In Kundensysteme mit personenbezogenen Daten erfolgt die Speicherung und Übertragung (in transit and at rest) verschlüsselt.
- Sofern personenbezogene Daten per E-Mail ausgetauscht werden, findet dieser Austausch nur in Form von verschlüsselten/kennwortgeschützten Dateianhängen oder durch eine durch oben genannte Maßnahmen gesicherte Bereitstellungsplattform statt.
- Der Transport von personenbezogenen Daten auf Wechsel-Datenträgern (USB-Stick, CD-ROM, DVD) findet nicht statt.
- Dokumente mit personenbezogenen Daten werden über einen externen Dienstleister datenschutzgerecht vernichtet.

3.2.2 Eingabekontrolle

Ziel ist es zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert
oder entfernt wurden.

Maßnahmen

- Auf den Kundensystemen werden alle wesentlichen Ein- und Ausgaben, die von den Nutzern und den Administratoren bei der Nutzung der Systeme und Applikationen getätigt werden, protokolliert (geloggt).
- Es werden die Art der Änderungen und die Identität der die Änderungen durchführenden Person gespeichert. Die Protokollierung erfolgt beim Anlegen, Ändern und Löschen von personenbezogenen Daten und Rollenzuweisungen.
- Die Verarbeitung der personenbezogenen Daten von Nutzer:innen erfolgt teilweise direkt durch den Kunden (Admin-Accounts) und dessen Datenverarbeitungsprogramme und ist durch den Kunden dann entsprechend zu regeln.

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

3.3.1 Verfügbarkeitskontrolle

Ziel ist es zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen

- Bei externen Hostings werden die Systeme in zertifizierten Rechenzentren betrieben, welchen aktuellen Standards entsprechen. Von den Betreibern liegen entsprechende Konzepte und Unterlagen vor.
- Die Daten werden täglich gesichert.
- Wir verwenden geeignete Sicherheitsmaßnahmen (z.B. 2-Faktor-Authentifizierung), um den Zugriff auf Backups zu schützen.
- Es wird ein automatisches Patch-Management genutzt um einen aktuellen Patch-Level sicherzustellen
- Interne Server sind in redundant klimatisierten Räumlichkeiten im Firmengebäude untergebracht. Eine Brandmeldeanlage ist vorhanden und überwacht das gesamte Gebäude. Des Weiteren existiert eine Datensicherungslösung und es werden regelmäßig Datenwiederherstellungen simuliert. Es werden Raid-Systeme eingesetzt, um Datenverluste zu verhindern. Alle Server sind vor Überspannungen geschützt. Ein Notfallplan ist vorhanden.

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

3.4.1 Auftragskontrolle

Ziel ist es zu gewährleisten, dass beim Einsatz von Subunternehmern durch den Auftragnehmer die Vorgaben des Auftraggebers umgesetzt werden und personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Maßnahmen

- 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 IT-Sicherheits- und 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. Des Weiteren erfolgt eine Risikobewertung von Dienstleistern im Rahmen der Dienstleistersteuerung.
- 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. Wenn Dienstleister oder Subunternehmer Zugriff auf Systeme erhalten, werden diese unter Sorgfaltsgesichtspunkten hinsichtlich Datensicherheit auf Grundlage einer entsprechenden Gruppenrichtlinie ausgewählt.
- Des Weiteren sind diese gemäß DS-GVO zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet. Zu diesem Zweck erfolgt eine einheitliche und eindeutige Vertragsgestaltung zur Auftragsverarbeitung, sowie eine regelmäßige Kontrolle der Vertragsausführung und Überwachung der Auftragnehmer.
- 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.