Vertrag zur Auftragsverarbeitung zwischen

Kunden der eCademy Plattform

– nachfolgend Verantwortlicher oder Auftraggeber genannt –

und

Cornelsen eCademy & inside GmbH
Vor den Siebenburgen 2
50676 Köln
– nachfolgend Auftragsverarbeiter oder Auftragnehmer genannt –

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Auftragsverarbeiter führt die im Anhang 1 beschriebenen Dienstleistungen für den Verantwortlichen durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Dieser Vertrag tritt - solange keine anderweitigen Regelungen vereinbart wurden - mit Unterzeichnung beider Parteien in Kraft und gilt, solange der Auftragsverarbeiter für den Verantwortlichen personenbezogene Daten verarbeitet.

§ 2 Weisungen des Verantwortlichen

(1) Der Verantwortliche ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Der Auftragsverarbeiter verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen des Verantwortlichen und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Verantwortliche dies anweist.

(3) Die Verarbeitung erfolgt nur auf Weisung des Verantwortlichen, es sei denn, der Auftragsverarbeiter ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von dem Verantwortlichen zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftragsverarbeiter dies verlangt.

(5) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Vorschriften verstößt, hat sie den Verantwortlichen unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und im Anhang 3 dieses Vertrages zu dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Der Auftragsverarbeiter darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss der Auftragsverarbeiter dem Verantwortlichen nur wesentliche Anpassungen mitteilen.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Der Auftragsverarbeiter hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten des Verantwortlichen mitzuwirken. Der Auftragsverarbeiter wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Er hat dem Verantwortlichen alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsverarbeiter bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Der Auftragsverarbeiter darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten des Verantwortlichen zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(6) Der Auftragsverarbeiter darf die ihm zur Verfügung gestellten personenbezogenen Daten im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen von Artt. 44 ff. DSGVO erfüllt sind.

(7) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf

Datenübertragbarkeit und Widerspruch. Der Auftragsverarbeiter benennt einen Ansprechpartner, der den Verantwortlichen bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt dem Verantwortlichen dessen Kontaktdaten unverzüglich mit. Soweit der Verantwortliche besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt der Auftragsverarbeiter den Verantwortlichen hierbei. Auskünfte an die betroffene Person oder Dritte darf der Auftragsverarbeiter nur nach vorheriger Weisung des Verantwortlichen erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber dem Auftragsverarbeiter geltend macht, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragsverarbeiter darf Unterauftragnehmer nur beauftragen, wenn er den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen. Erfolgt kein Widerspruch innerhalb von vier Wochen, gilt die Zustimmung zur Änderung als gegeben.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn der Auftragsverarbeiter weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer sicher, dass Maßnahmen zur Herstellung eines angemessenen Schutzniveaus gemäß Art. 45 ff. DSGVO (z.B. Standarddatenschutzklauseln, Genehmigte Zertifizierungsmechanismus, Angemessenheitsbeschluss der Kommission) vorliegen. Mit externen Dienstleistern, die personenbezogene Daten im Auftrag verarbeiten, werden daher schriftliche Verträge zur Auftragsverarbeitung nach Maßgabe von Art. 28 Abs. 3 DSGVO abgeschlossen.

(4) Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

§ 6 Kontrollrechte des Verantwortlichen

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche oder eine von ihm beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen des Auftragsverarbeiters zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht des Auftragsverarbeiters zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

§ 7 Mitzuteilende Verstöße des Auftragsverarbeiters

Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,

b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind in Textform abzufassen, dies kann schriftlich oder in einem elektronischen Format erfolgen.

(3) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Bereitstellung und Nutzung der Cornelsen eCademy Lernplattform
Art und Zweck der Verarbeitung	Bereitstellung der Cornelsen eCademy Lernplattform, Anlage und Pflege von NutzerInnen, Bereitstellung und Nutzung der Lerninhalte, Bereitstellung und Nutzung der Lernergebnisse, Empfehlung von Lerninhalten. Emails an die Nutzer bzgl. (i) Empfehlung von Lerninhalten und Funktionen der Lernplattform via E-Mail an die Nutzer, (ii) Einladungen zu Webinaren, für Nutzer und (iii) Einladung zu Bewertung und Feedback.
Art der personenbezogenen Daten	Daten zur Person: Username, E-Mail-Adresse, Name, Firma, Rolle, Organisationseinheit, Ausbildungsprofil, Profilbild. Daten zu Lerninhalten: Zugriff und Verwendung von Lerninhalten, Durchführung von Übungen und Tests, Testergebnisse. Daten zur Kommunikation zwischen BenutzerInnen: Inhaltliche Verweise, Empfehlungen, Kommentare. Gerätespezifische Daten: IP-Adresse, Browser, Betriebssystem, Anzeige.
Kategorien betroffener Personen	Schulungsteilnehmende

Name und Kontaktdaten des Datenschutz-beauftragten des Verantwortlichen	
Name und Kontaktdaten des Datenschutz-beauftragten des Auftragsverarbeiters (sofern benannt)	datenschutz nord GmbH E-Mail: office@datenschutz-nord.de Telefon: 0421/6966320

Anhang 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Folgende Unternehmen werden von Cornelsen eCademy & inside GmbH im Rahmen der Bereitstellung der eCademy Lernplattform eingesetzt. Mit Dienstleistern, die Ihren Sitz außerhalb der Europäischen Union haben, wurden die Standardvertragsklauseln abgeschlossen.

Unterauftragnehmer	Ort der Datenverarbeitung/ erbrachte Dienstleistung
Google Cloud EMEA Ltd. 70 Sir John Rogerson's Quay, Dublin 2, Irland	EU Hosting Infrastruktur Unterstützt Datenreports im Rahmen unserer Customer Success Services
Mailjet 13 Rue de l'Aubrac, 75012 Paris Frankreich	EU Automatisierte Mitteilungen per E-Mail für Passwort-Wiederherstellung etc.
Algolia SAS 55 Rue d'Amsterdam 75008 Paris Frankreich	EU Suchfunktion innerhalb der Lernplattform
Intercom, Inc. 55 Second Street, Suite 400 San Francisco, CA 94105 USA	EU / USA Kundenkommunikation, Support und Hilfecenter: Chat-Funktion für den Support sowie Bereitstellung von FAQs und Hilfeartikel
ConfigCat 1032 Budapest Bécsi út 219. 9. em. 47. Ungarn	EU Konfiguration der Lernplattform: Bereitstellung von neuen Features
SatisMeter s.r.o. Česká 1113/1, Prague 5, 158 00 Tschechien	EU Zufriedenheitsumfragen im Rahmen unserer Customer Success Services

Roadmap 551-1231 Pacific Blvd Vancouver, BC V6Z 0E2 Canada	Kanada Nutzerfeedback und Feature Requests: Nutzer können Vorschläge zu neuen Funktionen machen, bestehende Vorschläge bewerten, und über Roadmap Updates dazu erhalten
Contentful GmbH Ritterstr. 12-14 10969 Berlin	EU Content Delivery Networks (CDN): Schnelle und ausfallsichere Auslieferung von Inhalten bei vielen parallelen Nutzer-Sessions. Diese Networks speichern die Inhalte in verschiedenen Rechenzentren zwischen, die ihrerseits in verschiedenen Ländern (z.B. Australien, USA) stehen.
segment.io, inc. 100 California Street, Suite 700 San Francisco, CA 94111 USA	EU Datenminimierung und DSGVO-Compliance: Segment erlaubt uns, Art und Umfang der Daten, die weitere Dienste erhalten, zentral zu managen und bei Bedarf auch zu unterbinden.
Sentry Functional Software, Inc. 132 Hawthorne St San Francisco, CA 94107 USA	USA Fehler-Diagnosetool: Verwaltung und Korrektur von Bugs auf der Lernplattform
Mixpanel, Inc. 405 Howard St., 2nd Floor, San Francisco, CA 94105 USA	EU Verwaltung und Optimierung von Funktionen und Inhalten der Lernplattform
Honeycomb.io Hound Technology, Inc. 945 Bryant St. #300 San Francisco, CA 94103 USA	EU / USA Monitoring der Performance der Lernplattform
Slack Technologies Limited Level 1, Block A, Nova Atria North Sandyford Business District, Dublin 18, Ireland	EU Automatisierte Benachrichtigungen aus anderen Tools zum Monitoring, Betrieb und Weiterentwicklung der Plattform Art der verarbeiteten Daten: ausschließlich pseudonyme Daten
Atlassian Pty Ltd. Level 6, 341 George Street Sydney NSW 2000 Australien	EU Nutzung von Jira (Bugtracker) und Confluence (Dokumentation) zur Bearbeitung von Supportanfragen (2nd Level)
Salesforce.com Germany GmbH Erika-Mann-Str. 31-37 80636 München	EU Kunden- und Leadmanagement; Verwaltung von Teilnahmen an Veranstaltungen; Versand von Mitteilungen an Kunden, Leads oder Kontakte; Durchführung von Marketingaktivitäten und Umfragen; Handhabung von Kontakt- und Benutzersupport-Anfragen; Rechnungsstellung und Kontenverwaltung (einschließlich der Nutzungs- und Lizenzkonformität); Betrieb einer

	Knowledge Base und einer Community für unsere Anwender; Erbringung unserer Dienste und Optimierung unserer Leistungen

V11, gültig ab 05.03.2024

Anhang 3: Technische und organisatorische Maßnahmen

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

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

Die eCademy trifft die nachfolgenden technischen und organisatorischen Maßnahmen zur angemessenen Sicherung personenbezogener Daten unbefugtem Zugriff und unbefugter Weitergabe.

Unbefugten wird der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, durch folgende Maßnahmen verwehrt (Zutrittskontrolle):

- 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.
-

Durch folgende Maßnahmen wird verhindert, dass Datenverarbeitungssysteme genutzt werden können (Zugangskontrolle):

- Der Zugang zu allen IT-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).
- Alle IT-Datenverarbeitungssysteme des Auftragnehmers sind nur nach passwortgestützter Authentifizierung nutzbar.
- Beschäftigte der Cornelsen eCademy & inside, 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. Die Arbeitsplatzrechner der Mitarbeiter der Cornelsen eCademy & inside sind mit Benutzername und Passwort geschützt. Nach einer bestimmten Inaktivität erfolgt eine automatische, passwortgeschützte Bildschirmsperre. - bzw. Rechnersperre.
- Die Firewall ist eingerichtet, um den Zugang von Unbefugten zu den Datenverarbeitungssystemen zu verhindern und wird regelmäßig upgedatat.
- Berechtigungen werden nach dem Minimalprinzip vergeben. Die Einhaltung des Minimalprinzips stellt sicher, dass die Beschäftigten der Cornelsen eCademy & inside 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.
- Zugriff auf Systeme mit Kundendaten finden nur über geschützte und verschlüsselte Verbindungen statt.

- Zugriffe auf die Cornelsen eCademy Lernplattform werden protokolliert.
- Die Datenübertragung zur Cornelsen eCademy Lernplattform erfolgt verschlüsselt.

Zugriffskontrolle

- 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.

Trennungskontrolle

- 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.

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.

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 & inside 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle).

- 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.
-

Cornelsen eCademy & inside gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)

- 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.

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

Die Cornelsen eCademy & inside trägt dafür Sorge, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

- 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.

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

Gemäß Art. 32 Abs. 1 lit. d DSGVO, Art. 28 Abs. 1 DSGVO ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.

- 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.