Itslearning AS
P.O. Box 2686
5836 Bergen
Norwegen

Tel.: +47 55 23 60 70
E-Mail:
post@itslearning.com

Datenverarbeitungsvereinbarung

ZWISCHEN

[NAME DES KUNDEN EINFÜGEN]_____
ORG-NR. [ORGANISATIONSNUMMER EINFÜGEN]_____
(NACHFOLGEND ALS „DATENVERANTWORTLICHER“ BEZEICHNET)

UND

ITSLEARNING AS, WIE IN DER STANDARDVEREINBARUNG ÜBER DAS DIENSTLEISTUNGS-ABONNEMENT BEZEICHNET
(NACHFOLGEND ALS „DATENVERARBEITER“ BEZEICHNET)

_____

1. Zweck

Der Zweck dieser Vereinbarung besteht darin, die Rechte und Pflichten zu beschreiben, denen der Datenverantwortliche gemäß den Datenschutzgesetzen der Europäischen Union, einschließlich der DSGVO (nachfolgend als „anwendbare Datenschutzverordnung“ bezeichnet) und im Zusammenhang mit der Standardvereinbarung über das Dienstleistungs-Abonnement (nachfolgend als „Abonnement-Vereinbarung“ bezeichnet) unterliegt.

Durch diese Vereinbarung wird sicher gestellt, dass personenbezogene Daten, die gemäß der Abonnement-Vereinbarung (https://itslearning.com/global/terms-and-conditions) verarbeitet werden, nicht gesetzwidrig verwendet werden oder in den Besitz nicht-autorisierter Dritter gelangen.

Bekanntmachungen gemäß dieser Vereinbarung sind an die Kontaktperson zu übermitteln, die im Bestellformular angegeben wurde.

Fragen oder Anfragen des Datenverantwortlichen im Zusammenhang mit den unter dieser Vereinbarung bereit gestellten Diensten sind an den Datenschutzbeauftragten (Data Protection Officer, DPO) des Datenverarbeiters contact-dpo@itslearning.com zu senden.

2. Begriffbestimmungen

„DSGVO“ bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

Die anderen Datenschutzbegriffe und -konzepte, die in dieser Vereinbarung verwendet werden, haben den gleichen Inhalt und die gleiche Bedeutung wie die Begriffe der DSGVO.

3. Verarbeitung und Hauptverantwortung

Die Vereinbarung regelt die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen, einschließlich der Erhebung, Aufzeichnung, Ausrichtung, Speicherung und Offenlegung oder einer Kombination davon. Gegenstand und Einzelheiten der Verarbeitung personenbezogener Daten sind im Anhang 1 ausführlich beschrieben.

Der Datenverarbeiter selbst hat kein Verfügungsrecht über die personenbezogenen Daten und kann personenbezogene Daten nicht für eigene Zwecke verarbeiten. Die personenbezogenen Daten werden ausschließlich dazu verwendet, den Zweck der Abonnement-Vereinbarung innerhalb des vom Datenverantwortlichen festgelegten Rahmens zu erfüllen.

Ist der Datenverarbeiter gesetzlich dazu verpflichtet, personenbezogene Daten auf andere Weise zu verarbeiten als durch den Datenverantwortlichen angewiesen, muss der Datenverarbeiter den Datenverantwortlichen über diese Tatsache informieren, bevor eine solche Verarbeitung stattfindet. Dies trifft nicht zu, wenn geltende Gesetze oder rechtliche Verfahren einer solchen Bekanntmachung durch den Datenverarbeiter entgegen stehen.

4. Rolle und Verantwortlichkeit des Datenverantwortlichen

Der Datenverantwortliche hat sicher zu stellen, dass für die Verarbeitung personenbezogener Daten ein rechtmäßiger Verarbeitungsgrund besteht und dass die tatsächliche Verarbeitung in Übereinstimmung mit den anwendbaren Datenschutzgesetzen erfolgt.

Als Teil dieser Verantwortlichkeit hat der Datenverantwortliche sicher zu stellen, dass Systemadministratoren über die erforderliche Autorisierung verfügen, bevor sie mit der Verarbeitung personenbezogener Daten im Auftrag des Datenverantwortlichen beginnen.

Der Datenverantwortliche hat außerdem alle erforderlichen Datenschutz-Folgeabschätzungen durchzuführen. Das bedeutet, dass vor der Verarbeitung die Auswirkungen dieser beabsichtigten Verarbeitung auf den Schutz personenbezogener Daten abgeschätzt werden.

Der Datenverantwortliche ist für Anfragen von Endbenutzern verantwortlich, die Zugriff auf personenbezogene Daten wünschen, welche vom Datenverantwortlichen oder vom Datenverarbeiter gehalten werden. Erhält der Datenverarbeiter eine solche Anfrage, wird er dem Endbenutzer empfehlen, diese Anfrage an den Datenverantwortlichen weiter zu leiten, da der Datenverantwortliche für die Beantwortung solcher Anfragen zuständig ist.

Gemäß der Abonnement-Vereinbarung kann der Datenverantwortliche zusätzliche Produkte von externen Drittparteien (einschließlich Erweiterungen) installieren und aktivieren. Wenn der Datenverantwortliche solche Produkte dritter Parteien installiert, verwendet oder aktiviert, erkennt er an, dass diese Datenverarbeitungsvereinbarung nicht für die Verarbeitung von Daten gilt, die von solchen Produkten dritter Parteien oder an solche Produkte übermittelt werden. Der Datenverantwortliche kann die Verwendung von Produkten externer Drittparteien aktivieren oder deaktivieren und es ist unter der Abonnement-Vereinbarung nicht erforderlich, solche Produkte zu verwenden.

5. Rolle und Pflichten des Datenverarbeiters

Der Datenverarbeiter verarbeitet personenbezogene Daten im Auftrag des Datenverantwortlichen und nur in jenem Ausmaß, das der Datenverantwortliche bestimmt hat. Verarbeitet der Datenverarbeiter personenbezogene Daten, um die Sicherheit, die operativen Instandhaltung oder die Analyse oder Auswertung der unter der Abonnement-Vereinbarung bereit gestellten Dienstleistungen zu gewährlisten, gilt dies nicht als eine Verarbeitung zu eigenen Zwecken des Datenverarbeiters, wenn den Datensubjekten dadurch keine nachteiligen Auswirkungen für den Datenschutz entstehen.

Der Datenverarbeiter stellt dem Datenverantwortlichen alle Informationen bereit, die erforderlich sind, um die Einhaltung der anwendbaren Datenschutzgesetze zu dokumentieren. Darüber hinaus leistet er dem Datenverantwortlichen Hilfe, damit dieser seine Verantwortlichkeiten gemäß den Gesetzen und Verordnungen erfüllen kann.

Sofern nichts anders vereinbart wurde und die gesetzlichen Bestimmungen nichts anderes verlangen, hat der Datenverantwortliche das Recht, auf personenbezogene Daten, die vom Datenverarbeiter im Auftrag des Datenverantwortlichen verarbeitet werden, sowie auf alle Systeme zuzugreifen, die zu diesem Zweck verwendet werden. Der Datenverarbeiter leistet dem Datenverantwortlichen in diesem Zusammenhang Hilfe. Der Datenverarbeiter ist allerdings nicht verpflichtet, dem Datenverantwortlichen vertrauliche oder sensible Geschäftsinformationen weiter zu geben. Darüber hinaus hat der Datenverantwortliche kein Zugriffsrecht, wenn dies ein Risiko für die Sicherheit oder Integrität der relevanten personenbezogenen Daten bedeutet.

Der Datenverarbeiter und seine Mitarbeiter unterliegen hinsichtlich der Dokumentation und der personenbezogenen Daten, auf die der Datenverarbeiter gemäß dieser Vereinbarung Zugriff hat, einer Geheimhaltungspflicht. Diese Bestimmung gilt auch nach Beendigung dieser Vereinbarung. Wenn die Mitarbeiter nicht bereits durch eine gesetzliche Geheimhaltungs-

oder Verschiwegenheitspflicht gebunden sind, werden alle erforderlichen Geheimhaltungsvereinbarungen getroffen. Die Geheimhaltungspflicht umfasst auch Mitarbeiter von Sub-Verarbeitern, die Wartungsarbeiten (oder ähnliche Aufgaben) von Systemen durchführen, die der Datenverarbeiter zur Bereitstellung oder Verwaltung des Dienstes verwendet.

Die internen Datenzugriffsprozesse und -richtlinien des Datenverarbeiters wurden entwickelt, damit keine nicht-autorisierten Personen und/oder Systeme auf die Systeme zugreifen können, die zur Verarbeitung der personenbezogenen Daten verwendet werden. Der Datenverarbeiter gestaltet seine Systeme so, dass ausschließlich autorisierte Personen Zugriff auf Daten haben und gewährleistet wird, dass die personenbezogenen Daten nicht ohne Autorisierung während der Verarbeitung, Verwendung oder nach der Erhebung gelesen, kopiert, verändert oder entfernt werden können. Genehmigungen werden von Workflow-Tools verwaltet, die Überwachungsdatensätze aller Änderungen aufbewahren. Der Zugriff auf Systeme wird protokolliert, um einen Überwachungspfad für die Verantwortlichkeit zu erstellen. Die Protokolle sind vom Datenverarbeiter mindestens 3 Monate aufzubewahren. Dem Datenverantwortlichen ist auf Anfrage Zugang zu diesen Protokollen zu gewähren.

6. Der Datenschutzbeauftragte

Der Datenverarbeiter hat in Übereinstimmung mit den Bestimmungen der anwendbaren Datenschutzgesetze einen Datenschutzbeauftragten ernannt.

7. Einsatz von Sub-Verarbeitern und Export von Daten

Setzt der Datenverarbeiter für die Verarbeitung personenbezogener Daten Sub-Verarbeiter ein, ist dies mit dem Datenverantwortlichen schriftlich zu vereinbaren, bevor der Sub-Verarbeiter mit der Datenverarbeitung beginnt, außer, der Einsatz eines Sub-Verarbeiters ergibt sich bereits aus der Abonnement-Vereinbarung. Der Datenverarbeiter wird sicher stellen, dass alle Sub-Verarbeiter nur in einer solchen Weise auf personenbezogene Daten zugreifen, die den Bestimmungen der Datenverarbeitungsvereinbarung entspricht und dass solche Sub-Verarbeiter durch schriftliche Vereinbarungen gebunden sind, die zumindest jenes Datenschutzniveau bieten, das in den anwendbaren Datenschutzgesetzen vorgeschrieben ist. Der Datenverantwortliche kann die Zulassung neuer Sub-Verarbeiter ablehnen, wenn nachvollziehbare und berechtigte Gründe dafür vorliegen.

Die auf der folgenden Website angeführten Sub-Verarbeiter werden hiermit vom Datenverantwortlichen zugelassen: https://itslearning.com/global/gdpr/subprocessors. Falls der Datenverantwortliche detailliertere Informationen zu Verarbeitungsstandorten benötigt, um gesetzliche Anforderungen einzuhalten oder Anfragen von Datenschutzbehörden nachzukommen, unterstützt der Datenverarbeiter den Datenverantwortlichen bei der Einhaltung dieser Anforderungen, vorausgesetzt, dass der Datenverantwortliche vor der Bereitstellung solcher Informationen die aus Sicht des Datenverarbeiters erforderlichen Geheimhaltungsverpflichtungen eingegangen ist.

Änderungen, bei denen die oben genannte Liste durch eine Einheit ergänzt oder bei denen eine Einheit durch eine andere Einheit ersetzt wird, sind dem Datenverantwortlichen offen zu legen. Dies kann unter anderem durch automatisierte Mitteilungen an den Datenverantwortlichen oder, wenn erforderlich, auf anderen Wegen geschehen. Innerhalb von vier Wochen nach Erhalt einer solchen Mitteilung kann der Datenverantwortliche eine solche Änderung oder Ergänzung ablehnen, wobei diese Ablehnung ausschließlich auf nachvollziehbaren Gründen beruhen darf.

Der Datenverarbeiter ist gegenüber dem Datenverantwortlichen für die Handlungen und Versäumnisse des Sub-Verarbeiters auf die gleiche Weise verantwortlich, als wären es die eigenen Handlungen und Versäumnisse des Datenverarbeiters. Der Datenverarbeiter hat sicher zu stellen, dass der Sub-Verarbeiter mit den vertraglichen und gesetzlichen Verpflichtungen des Datenverarbeiters vertraut ist und dass der Sub-Verarbeiter diese Verpflichtungen gegenüber dem Datenverarbeiter auf ähnliche Weise erfüllt.

Der Datenverarbeiter und jeder potenzielle Sub-Verarbeiter dürfen die personenbezogenen Daten ohne die vorherige schriftliche Zustimmung des Datenverantwortlichen nicht in einen Staat transferieren, der außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums liegt oder der nicht zu im Vorhinein genehmigten Drittstaaten zählt. Verwendet der Datenverantwortliche personenbezogene Daten in einem Drittstaat oder greift er aus einem Drittstaat auf diese zu, gilt dieser Vorgang in Bezug auf den Datenverarbeiter oder einen Sub-Verarbeiter nicht als Transfer personenbezogener Daten in einen solchen Drittstaat.

Soweit ein solcher Transfer personenbezogener Daten erfolgt, entweder an Datenverarbeiter-Einheiten oder an dritte Sub-Verarbeiter außerhalb der EU/des EWR, müssen solche Transfers bindenden und angemessenen Transfermechanismen unterliegen, die in Übereinstimmung mit den anwendbaren Datenschutzgesetzen ein adäquates Datenschutzniveau bieten.

8. Sicherheit

a. Sicherheitsmaßnahmen und Dokumentation

Der Datenverarbeiter hat die in den anwendbaren Datenschutzgesetzen vorgeschriebenen Anforderungen in Bezug auf Sicherheitsmaßnahmen zu erfüllen. Der Datenverarbeiter ist verpflichtet, seine Sicherheitsmaßnahmen zu dokumentieren. Anhang 3 enthält eine Übersicht über die Sicherheitsmaßnahmen der Datenverarbeiter. Ausführlichere Dokumentationen können dem Datenverantwortlichen auf dessen Anfrage zur Verfügung gestellt werden.

Der Datenverarbeiter hat geeignete technische und organisatorische Sicherheitsmaßnahmen einzuführen und aufrecht erhalten, um ein Sicherheitsniveau zu gewährleisten, das dem verbundenen Risiko entspricht. Dabei ist unter anderem auch zu prüfen, welche Art von Cloud-Diensten dem Datenverantwortlichen zur Verfügung gestellt werden. Durch die Maßnahmen müssen übertragene, gespeicherte oder auf anderem Weg verarbeitete personenbezogene Daten vor zufälligen oder gesetzwidrigen Zerstörungen, Verlusten, Abänderungen sowie vor nicht-autorisierter Offenlegung oder nicht-autorisiertem Zugang geschützt werden. Der Datenverarbeiter hat bei der Errichtung solcher Maßnahmen die

Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Informationen und der Verarbeitungssysteme und -dienste zu berücksichtigen.

Bei der Verarbeitung personenbezogener Daten müssen geeignete Sicherheitsmaßnahmen gegebenenfalls unter anderem Folgendes umfassen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten.
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung;

Der Datenverantwortliche und der Datenverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Datenverantwortlichen verarbeiten, es sei denn, sie sind gemäß den anwendbaren Datenschutzgesetzen oder anderen Gesetzen dazu verpflichtet.

b. Übersicht über die Verarbeitungsaktivitäten

Der Datenverarbeiter und gegebenenfalls der Beauftragte des Datenverarbeiters erarbeiten und verwalten eine Liste aller Kategorien von Verarbeitungstätigkeiten, die im Namen des Datenverantwortlichen durchgeführt werden. Sie muss folgende Informationen enthalten:

a) den Namen und die Kontaktdaten des Datenverarbeiters und des Datenschutzbeauftragten;
b) die Kategorien von Verarbeitungen, die im Auftrag jedes Datenverantwortlichen durchgeführt werden
c) gegebenenfalls Übermittlungen von personenbezogenen Daten an einen Drittstaat außerhalb der EU / des EWR, einschließlich der Bezeichnung dieses Drittstaats und bei Bedarf die Dokumentierung geeigneter Garantien;
d) wenn möglich, eine allgemeine Beschreibung der angewendeten technischen und organisatorischen Sicherheitsmaßnahmen.

Die Liste wird nach Maßgabe der nachstehenden Klausel 9 aktualisiert. Der Datenverarbeiter stellt die Liste auf Verlangen der zuständigen Datenschutzbehörde zur Verfügung.

c. Meldung von Datenschutzverletzungen

Hat eine Datenschutzverletzung die Sicherheit oder den Schutz der personenbezogenen Daten gefährdet, muss dies der Anlaufstelle gemeldet werden, die in Abschnitt 1 dieser Vereinbarung angeführt ist. Eine solche Meldung hat unverzüglich und möglichst binnen 72 Stunden, nachdem dem Datenverarbeiter die Verletzung bekannt wurde, zu erfolgen.

Diese Meldung hat Folgendes zu enthalten:

- Eine Beschreibung der personenbezogenen Daten und, soweit möglich, die Angabe der Kategorien und der Anzahl der betroffenen Datensubjekte sowie die Angabe der Kategorien und der Anzahl der betroffenen personenbezogenen Daten
- Den Namen und die Kontaktdaten jeglicher Datenschutzbeauftragter oder anderer Kontaktpersonen
- Eine Beschreibung der voraussichtlichen Folgen des Vorfalls
- Eine Beschreibung der Maßnahmen, die ergriffen oder vorgeschlagen werden, um mit dem Vorfall umzugehen und gegebenenfalls die Maßnahmen zur Abschwächung möglicher nachteiliger Auswirkungen.

Der Datenverantwortliche ist dafür zuständig, die Datenschutzbehörden sowie gegebenenfalls die von der Datenschutzverletzung betroffenen Personen über die Datenschutzverletzung in Bezug auf die personenbezogenen Daten zu informieren.

d. Zugriffsverwaltung und Ausstattung

Der Datenverarbeiter hat die ordnungsgemäße Sicherheit der Dienste zu gewährleisten, darunter jene der Server, Datenbanken und anderen relevanten Geräte, damit keine nicht-autorisierte Person auf die Daten zugreifen kann. Dasselbe gilt für alle Ausdrucke und anderen physischen Dokumente.

Darüber hinaus verfügt der Datenverarbeiter über ein System für die Sicherheitskontrolle gemäß den anwendbaren Datenschutzgesetzen. Dieses System umfasst unter anderem Routinen für:

- Behandlung von Nichtkonformitäten, darunter die Meldung einer nicht ordnungsgemäßen Benutzung des Informationssystems wie zum Beispiel Sicherheitsverletzungen
- Sicherheitsüberprüfungen

Der Datenverarbeiter hat Sicherheitsmaßnahmen einzurichten und aufrecht zu erhalten, die bei der Bewertung von Sicherheits- und Technologierisiken als notwendig erachtet wurden.

9. Aktualisierungen von Verarbeitungsaktivitäten und Sicherheitsüberprüfungen

Die Liste der Verarbeitungstätigkeiten, vgl. Abschnitt 8b) oben, ist mindestens einmal jährlich oder wenn die Verarbeitungsaktivitäten wesentlich geändert werden, zu überprüfen und zu aktualisieren.

Der Datenverarbeiter führt regelmäßig (mindestens einmal jährlich oder nach wesentlichen Änderungen oder Abweichungen) Sicherheitsüberprüfungen der Systeme und aller anderen Elemente durch, die für die Verarbeitung personenbezogener Daten gemäß dieser Vereinbarung relevant sind. Die Sicherheitsüberprüfung soll gewährleisten, dass die festgelegten technischen, physischen und organisatorischen Sicherheitsmaßnahmen eingehalten werden und wie geplant funktionieren sowie potenzielle Verbesserungsmöglichkeiten feststellen.

Das Ergebnis der Sicherheitsüberprüfung ist zu dokumentieren und dem Datenverantwortlichen zur Verfügung zu stellen, unter anderem auch für die Verwendung in der Sicherheitsüberprüfung des Datenverantwortlichen.

Die Systeme und Prozesse des Datenverarbeiters werden regelmäßig überprüft und zertifiziert. Dem Datenverantwortlichen werden auf Anfrage alle anwendbaren Zertifizierungen zur Verfügung gestellt.

Aufwendungen, die als Folge von durch den Datenverantwortlichen verlangten oder durchgeführten Sonderprüfungen entstehen, sind vom Datenverantwortlichen zu tragen.

10. Dauer der Vereinbarung

Die Vereinbarung gilt ab dem 25. Mai 2018 oder ab dem Zeitpunkt, an dem die Parteien dieser Vereinbarung zugestimmt haben, wenn dieser Zeitpunkt nach dem 25. Mai 2018 liegt, und sie bleibt in Kraft, solange die Abonnement-Vereinbarung aufrecht ist. Sie ersetzt alle vorangegangenen Datenverarbeitungsvereinbarungen der Parteien.

Bei Verletzung dieser Vereinbarung oder der anwendbaren Datenschutzgesetze kann der Datenverantwortliche den Datenverarbeiter anweisen, die Weiterverarbeitung personenbezogener Daten zu stoppen.

11. Rückgabe und Löschung bei Beendigung dieser Vereinbarung

Nach Beendigung dieser Vereinbarung ist der Datenverarbeiter verpflichtet, die Daten zurückzugeben, zu überschreiben zu löschen (vgl. die im Anhang 2 angeführten Löschungsroutinen) und/oder alle Dokumente, Speichermedien und alles andere zu vernichten, was personenbezogene Daten enthält, die in den Geltungsbereich dieses Abkommens fallen. Dies gilt auch für Sicherungskopien. Der Datenverarbeiter hat nach Beendigung dieser Vereinbarung innerhalb eines angemessenen Zeitraums schriftlich zu dokumentieren, dass eine solche Handlung in Übereinstimmung mit dieser Vereinbarung stattgefunden hat.

Der Datenverantwortliche hat alle Kosten im Zusammenhang mit der Erfüllung dieser Klausel zu tragen, sofern die Abonnement-Vereinbarung keine anderen Bestimmungen enthält.

12. Wahl des anzuwendenden Rechts und Gerichtsstand

Die Wahl des anzuwendenden Rechts und des Gerichtsstands wird in der Abonnement-Vereinbarung geregelt oder zwischen den Parteien dieser Vereinbarung vereinbart.

***

Vereinbart für und im Namen von **itslearning** (**DATENVERARBEITER**)	Vereinbart für und im Namen des **Kunden** **(DATENVERANTWORTLICHER)**
Name der itslearning-Organisation:	Name der Kundenorganisation:

_____ _____

Unterzeichnet: DocuSigned by: _____ Unterzeichnet: _____
CB0BBB5AAA6B423...

Name: Martin Lorenz _____ Name: _____

Titel: Geschäftsführer _____ Titel: _____

Datum: 4/13/2018 _____ Datum: _____

ANHANG 1

Gegenstand und Details der personenbezogenen Daten, die verarbeitet werden Ausgangspunkt und Zweck der Verarbeitung

itslearning verarbeitet als Datenverarbeiter im Auftrag des Datenverantwortlichen personenbezogene Daten, die über den Dienst (also über die itslearning-Software, Skoleintra und andere Plattformen), über den gehosteten Dienst für den Kunden sowie über Anwendungen von Partnern und über die Website (http://www.itslearning.com) erhalten wurden für die folgenden Zwecke:

- Bereitstellung von Diensten gemäß der Datenverarbeitungsvereinbarung und der Abonnementvereinbarung
- Bereitstellung von grundlegendem technischen Support im Zusammenhang mit den Diensten, die gemäß der Datenverarbeitungsvereinbarung und der Abonnementvereinbarung erbracht werden
- Sicherung der Daten des Datenverantwortlichen
- Der Datenverarbeiter kann Informationen über die Nutzung des Dienstes durch den Datenverantwortlichen für interne statistische Zwecke und für Fakturierungszwecke erheben

Dauer der Verarbeitung

Die Laufzeit der Abonnementvereinbarung zuzüglich des Zeitraums nach Ablauf der Vereinbarung bis zur Löschung sämtlicher Kundendaten, die der Datenverarbeiter gemäß der Vereinbarung durchführt.

Kategorien personenbezogener Daten

Der Datenverarbeiter verarbeitet personenbezogene Daten, die über den Service durch den Datenverantwortlichen (oder auf seine Anweisung) übermittelt, gespeichert, importiert, gesendet oder empfangen werden. Der Umfang der Daten wird im alleinigen Ermessen dieser Subjekte festgelegt und kontrolliert. Die Daten umfassen die folgenden Kategorien:

- Kontaktinformationen (Name, E-Mail, Telefonnummer, Adresse, Benutzername etc.)
- Kontaktdaten der Eltern oder der Erziehungsberechtigten
- Kommunikation (Nachrichten zwischen Benutzern, Diskussionen, Kommentare zu Beiträgen, Benachrichtigungen usw.)
- Kursmaterialien
- Bewertungen, Bewertungsergebnisse und Noten
- Kalendereinträge und Ereignisdaten
- Dokumente, Präsentationen, Bilder, Hausaufgaben, Aufgaben, etc.

Betroffene Personen

Die Verarbeitung personenbezogener Daten durch den Dienst im Auftrag des Datenverarbeiters kann unter anderem personenbezogene Daten in Bezug auf die folgenden Kategorien von Datensubjekten beinhalten:

- die Mitarbeiter des Kunden einschließlich Lehrer, Verwalter, Dozenten, Mentoren und andere
- andere Mitarbeiter und Auftragnehmer des Kunden sowie alle anderen berechtigten Benutzer des Kunden, die persönliche Daten über den Dienst übermitteln, einschließlich Studenten und Eltern.

ANHANG 2 | LÖSCHUNGSROUTINEN

Löschung von Daten nach Beendigung dieser Vereinbarung

Innerhalb von 6 Monaten nach Beendigung der Vereinbarung zwischen dem Datenverantwortlichen und dem Datenverarbeiter werden alle im Auftrag des Datenverantwortlichen verarbeiteten Daten, einschließlich Backups, endgültig gelöscht.

Löschrichtlinien für außer Betrieb genommene Speichermedien

Speichermedien/Festplatten (einschließlich HDDs, SSDs, Speicher-Sticks und Bänder), die Daten enthalten, können Leistungsprobleme, Fehler oder Hardwareversagen aufweisen, die es erforderlich machen, diese Medien außer Betrieb zu nehmen. Alle außer Betrieb genommenen Speichermedien müssen gemäß unserer „Unternehmensrichtlinie – Entsorgung von Speichermedien" verschiedene Vernichtungsprozesse durchlaufen, bevor Sie die Räumlichkeiten des Datenverarbeiters zur Wiederverwendung oder zur Vernichtung verlassen. So soll sicher gestellt werden, dass alle Daten vollständig und sicher entfernt und vernichtet wurden. Die Löschungsergebnisse sind mit der Seriennummer des Speichermediums zu protokollieren, um diese nachvollziehen zu können.

ANHANG 3 | SICHERHEITSMASSNAHMEN

itslearning hat die in diesem Anhang dargelegten Sicherheitsmaßnahmen (sowohl technischer als auch organisatorischer Natur) in Übereinstimmung mit den Industriestandards eingeführt. itslearning kann solche Sicherheitsmaßnahmen von Zeit zu Zeit aktualisieren oder ändern, sofern solche Aktualisierungen und Änderungen nicht zur Verschlechterung der allgemeinen Sicherheit der Dienste führen. Eine Aktualisierte Version finden Sie unter https://itslearning.com/global/gdpr/secritymeasures.

Organisatorische Maßnahmen

Das itslearning Management-Team hat sich durch ein kontinuierliches Sensibilisierungsprogramm aktiv an der Entwicklung einer Informationssicherheitskultur innerhalb des Unternehmens beteiligt und verfügt über eine Managementstruktur, die die Umsetzung der Informationssicherheit in seinen Diensten mit klaren Rollen und Verantwortlichkeiten innerhalb der Organisation verwaltet.

Betriebsmanagement

Es bestehen mehrere branchenspezifische Best-Practice-Prozesse und -Richtlinien, um die bestmögliche Vertraulichkeit, Verfügbarkeit und Integrität der Plattform zu gewährleisten. Diese Richtlinien richten sich nach strengen Anforderungen in einer Reihe von Bereichen, darunter:

- Informationssicherheit
- Sicherheit der Hosting-Umgebung
- Zugriff durch Drittanbieter
- Kapazitätskontrolle
- Change-Management
- Backup und Recovery
- Zugriffskontrolle
- Dokumentation
- Protokollierung und Überwachung
- Reaktion auf Vorfälle
- Freigabe-Management

Sicherheitsteam

itslearning verfügt ein Team von Sicherheitsexperten, die für die allgemeine Informationssicherheit der Organisation verantwortlich sind. Ihre Rolle beinhaltet die Verantwortung für:

- Koordinierung sicherheitsbezogener Aufgaben
- Sichern der Unternehmensumgebung, des Netzwerks und der Geräte
- Sicherheit die Anwendung (interne Penetrationstests und Anwendungsüberprüfungen)
- Überwachung und Protokollierung
- Prozess- und Policy-Management (Notfallwiederherstellung, Path-Management etc.)
- Aus- und Weiterbildung der Mitarbeiter im Bereich der Informationssicherheit

- Koordinierung der Sicherheitsüberprüfungen von Drittanbietern und Follow-up zu allen Ergebnissen
- Überprüfen des Codes für potenzielle Sicherheitslücken.

Rollen und Verantwortlichkeiten

Alle Mitarbeiter haben klare Rollen innerhalb des Unternehmens und erhalten nur Zugriff auf die für ihre jeweilige Rolle erforderlichen Daten. Eine begrenzte Anzahl von Mitarbeitern hat administrativen Zugang zu unserer Produktionsumgebung und ihre Rechte werden in festgelegten Intervallen streng reguliert und überprüft. Jede wesentliche Änderung der Anwendung, Umgebung oder Hardware der Produktionsumgebung wird immer von mindestens zwei Personen überprüft.

Personalsicherheit

Alle itslearning-Mitarbeiter sind verpflichtet, eine strenge Vertraulichkeitsvereinbarung einzugehen. Alle Mitarbeiter sind verpflichtet, Unternehmensrichtlinien in Bezug auf Vertraulichkeit, Geschäftsethik und professionelle Standards zu befolgen. Mitarbeiter, die an der Sicherung, Bearbeitung und Verarbeitung von Kundendaten beteiligt sind, müssen eine für ihre Rolle angemessene Schulung absolvieren.

Zugriffskontrolle

Es bestehen strenge Anforderungen für sämtliche Mitarbeiter, beauftragte Berater oder Dritte, die Zugang zu itslearning-Informationssystemen beantragen. Die Zugriffskontrolle wird durch ein Authentifizierungssystem gesteuert. Der Benutzer muss:

- Über eine Genehmigung des Managements für den geforderten Zugriff verfügen
- Über starke Passwörter in Übereinstimmung mit der Passwortrichtlinie des Unternehmens verfügen
- Seine Passwörter in regelmäßigen Abständen ändern
- Dokumentieren, dass der geforderte Zugriff für seine spezifische Rolle/Aufgabe erforderlich ist
- Sicher stellen, dass das benutzte Gerät (PC, Tablet, Smartphone) angemessen gesichert und gesperrt ist, wenn der Benutzer abwesend ist

Wenn das Benutzer-Terminal inaktiv ist, führt itslearning eine automatische temporäre Sperrung durch.

Die internen Datenzugriffsprozesse und -richtlinien wurden entwickelt, damit keine nicht-autorisierten Personen und/oder Systeme auf die Systeme zugreifen können, die zur Verarbeitung der personenbezogenen Daten verwendet werden. Sämtliche Änderungen der Daten werden protokolliert, um einen Überwachungspfad für die Verantwortlichkeit zu erstellen.

Physische Sicherheit

a. Datenzentren

itslearning betreibt alle seine Kundendienstleistungen von Datenzentren, die von den Arbeitsräumlichkeiten im Unternehmen getrennt sind. Der Zugang zu Datenzentren wird streng kontrolliert und geschützt, um die Wahrscheinlichkeit von unbefugtem Zugriff, Feuer, Überschwemmungen oder anderen Schäden an der physikalischen Umgebung zu verringern. Der physische Zugang zu Rechenzentren ist auf eine kleine Anzahl von Mitarbeitern innerhalb von itslearning und/oder deren Hosting-Center-Provider beschränkt. Es sind strenge Sicherheitsfreigaben erforderlich, die vor dem Zugang zu einem Datenzentrum vom Sicherheitsmanagement genehmigt werden müssen.

b. Büroräumlichkeiten

Die gesamten Büroräumlichkeiten von itslearning werden durch eine Zutrittskontrolle geschützt. Nur eingeladene Besucher und Mitarbeiter haben Zutritt zu den Büroräumlichkeiten von itslearning. Es existieren verschiedene Maßnahmen, um Sicherheitsprobleme aufgrund von Diebstahl oder Verlust der Computerausrüstung zu vermeiden. Dazu zählen Sicherheitsrichtlinien und Richtlinien zur angemessenen Nutzung, Authentifizierungssysteme und die Verschlüsselung von Speichereinheiten, sofern zutreffend.

Technische Maßnahmen

Systemverfügbarkeit

itslearning hat branchenübliche Maßnahmen ergriffen, um sicherzustellen, dass personenbezogene Daten vor versehentlicher Zerstörung oder versehentlichem Verlust geschützt sind, darunter:

- Redundanz der Infrastruktur (einschließlich vollständiger Netzwerk-, Strom-, Kühlungs-, Datenbank-, Server- und Speicherredundanz)
- Backups werden an einem alternativen Standort gespeichert und im Falle eines Fehlers des primären Systems für die Wiederherstellung zur Verfügung gestellt
- Entsprechender Denial-of-Service-Schutz
- Personal steht 365/24/7 zur Überwachung und Fehlerbehebung zur Verfügung

Datenschutz

itslearning hat eine Reihe von branchenüblichen Maßnahmen ergriffen, um zu verhindern, dass personenbezogene Daten während der Übermittlung oder der Aufbewahrung gelesen, kopiert, verändert oder gelöscht werden. Dies wird durch verschiedene branchenübliche Maßnahmen erreicht, darunter:

- Verwendung von mehrschichtigen Firewalls, VPNs und Verschlüsselungstechnologien zum Schutz von Gateways und Pipelines
- HTTPS-Verschlüsselung (auch als SSL-oder TLS-Verbindung bezeichnet) mit sicheren kryptografischen Schlüsseln

- Der Remote-Zugriff auf Datenzentren ist durch verschiedene Netzwerksicherheitsebenen geschützt
- Besonders sensible Kundendaten werden während der Aufbewahrung durch Verschlüsselung und/oder Hashing geschützt (Pseudonymisierung)
- Alle nicht in Betrieb befindlichen Festplatten unterliegen gemäß unserer „Festplattenlöschungs-Richtlinie" einem bestimmten Festplattenlöschungsprozess und die Stilllegung wird anhand der Seriennummer der Festplatte protokolliert
- Regelmäßige Sicherheitsaudits der Drittanbieter (mindestens jährlich), einschließlich Penetrationstests, die den Kunden zur Verfügung gestellt werden

Datenzentren

itslearning nutzt ausschließlich hochmoderne Datenzentren, die 365/24/7 über Sicherheits- und Überwachungsdienste verfügen. Die Daten sind in modernen, feuerbeständigen Einrichtungen untergebracht, die nur mit einer elektronischen Schlüsselkarte betreten werden können sowie über Alarme verfügen, die mit dem Sicherheitsbetrieb vor Ort verbunden sind. Nur autorisierte Angestellte und Auftragnehmer dürfen eine elektronische Schlüsselkarte für den Zutritt zu diesen Einrichtungen verlangen.

Systementwicklung

Die Plattform von itslearning basiert auf branchenüblichen Technologien namhafter Anbieter, darunter Microsoft, Linux, Dell, Fujitsu, Amazon, CloudFlare, F5 und Cisco. Systeme werden regelmäßig auf die neueste Version gepatcht, um sicherzustellen, dass die neuesten Sicherheitsverbesserungen angewendet werden. Die Plattform wird mehrmals pro Quartal allgemein aktualisiert und Bug-Fixes werden nach strengen Qualitätskontrollen rasch veröffentlicht, abhängig von ihrer Priorität.

itslearning verfügt über Maßnahmen, um das Risiko von neuem Code in der Plattform abzuschwächen, der die Sicherheit oder die Integrität der Kundendienste und der verarbeiteten personenbezogenen Daten herabsetzen könnte. Zu diesen Maßnahmen gehören:

- Regelmäßige Schulung des Personals
- Code-Überprüfung durch Sicherheitsarchitekten
- QA-Prozesse, in denen Änderungen vor der Umsetzung streng geprüft werden.

Sicherheit der Sub-Verarbeiter

Vor der Zusammenarbeit mit neuen Sub-Verarbeitern führt itslearning eine Überprüfung der Sicherheits- und Datenschutzpraktiken der Sub-Verarbeiter durch, um sicher zu stellen, dass ihr Sicherheits- und Datenschutzniveau für ihren Datenzugriff sowie für den von ihnen bereit gestellten Dienstumfang angemessen ist. itslearning führt auch für bestehende Sub-Verarbeiter regelmäßige Sicherheitsüberprüfungen der Praktiken und der bereit gestellten Dienste durch.