Gymnasium
„Friedrich Ludwig Jahn"
Dietrich-Bonhoeffer-Platz 1
17489 Greifswald
Haus 1: Tel. 03834 7920 • Fax 792222
Haus 2: Tel. 03834 8533090 • Fax 8533099

FRIEDRICH-LUDWIG-JAHN-GYMNASIUM GREIFSWALD
Dietrich-Bonhoeffer-Platz 1, 17489 Greifswald

[redacted]

Caspar David Friedrich

9037394412
0018684162
Nordkurier Logistik 72031/720085/12 – 05
18.11.2021
01013319842391 30

Friedrich-Ludwig-Jahn-Gymnasium Greifswald

FRIEDRICH-LUDWIG-JAHN-GYMNASIUM GREIFSWALD
Dietrich-Bonhoeffer-Platz 1, 17489 Greifswald

[redacted]

Haus I
Dietrich-Bonhoeffer-Platz 1
17489 Greifswald
Telefon: 03834 792-0 Fax: ... - 222
E-Mail: Kontakt@jahngymnasium.de

Haus II
August-Bebel-Platz 1
17489 Greifswald
Telefon: 03834 853309-0 Fax: ... - 9

Datum: 16.11.2021

Lernplattform itsLearning

Sehr [redacted]

Ihr Begehren auf Information stellten Sie über eine Internetplattform. Nach IFG M-V §10 hätte aber ein schriftlicher oder zur Niederschrift gegebener eigenhändig unterschriebener Antrag gestellt werden müssen.

Nach Aufforderung durch den von Ihnen angerufenen Datenschutzbeauftragten gebe ich Ihnen noch einmal Auskunft zur Datenschutzfolgeabschätzung und Sie erhalten eine Kopie des Verarbeitungsvertrages.

1. Datenschutzfolgeabschätzung bei der Verwendung der Lernplattform itsLearning:

Dazu hatte ich bereits per E-Mail geantwortet und wiederhole:

Wir nutzen in der Lernplattform nur die Namen der Schüler, die im Schulberichtssystem unserer Schule zugeordnet sind und vom Bildungsministerium den Betreibern des LMS bereitgestellt werden. Wir ordnen die Namen der Schüler und Lehrkräfte zu Klassen, Kursen und Gruppen zum Zwecke der Kommunikation. Wir geben darüber hinaus keine personengebundenen Daten ein. Soweit schriftliche Leistungen zu erbringen sind, werden diese zu Kenntnis genommen oder gegebenenfalls auch verbal bewertet und dienen allein der Rückmeldung der Qualität der Bewältigung der Aufgaben. Diese Bewertungen sind nur den betreffenden Schülern und den Kurslehrern zugänglich. Noten werden in der Plattform nicht in Listen gespeichert.
Es werden somit keine sensiblen Daten erhoben, erfasst und verarbeitet. Die personenbezogene Leistungseinschätzung bezieht sich nur auf konkrete Arbeitsergebnisse, über welche eine pädagogische Rückmeldung gegeben wird.

Damit ist eine formale Datenschutzfolgeabschätzung nicht erforderlich, weil über reine Adressdaten hinausgehende Daten nicht erfasst und verarbeitet werden.

2. Datenverarbeitungsvertrag

Auch hier ermangelte es der formal richtigen Anfrage nach §10 des IFG-MV.
Das vermittelnde Schreiben des Datenschutzbeauftragten vom 24.10.2021 nehme ich zum Anlass, um ohne ein formal richtiges Begehren Ihnen eine Kopie des Vertrages zukommen zu lassen.

Mit freundlichen Grüßen

[redacted]

- Schulleiter -

KOPIE

itslearning GmbH
Erich-Steinfurth-Str. 6
10243 Berlin

t: +49 30 616 74 847
f: +49 30 616 74 967
e: kontakt.de@itslearning.com

Vertrag zur Auftragsverarbeitung

ZWISCHEN

Gymnasium „Friedrich Ludwig Jahn"
75530136
Dietrich-Bonhoeffer-Platz 1
17489 Greifswald

(NACHFOLGEND ALS „VERANTWORTLICHER" BEZEICHNET)

UND

ITSLEARNING GMBH,
wie in dem Vertrag
über die Bereitstellung und den Betrieb einer online-basierten Lernplattform als Software as a Service sowie Funktionssicherungsleistungen bezeichnet

(NACHFOLGEND ALS „AUFTRAGSVERARBEITER" BEZEICHNET)

1. Zweck

Der Zweck dieser Vereinbarung besteht darin, die Rechte und Pflichten zu beschreiben, denen der Verantwortliche gemäß den Datenschutzgesetzen der Europäischen Union, einschließlich der DSGVO (nachfolgend als „anwendbare Datenschutzverordnung" bezeichnet) und im Zusammenhang mit wie in dem Vertrag über die Bereitstellung und den Betrieb einer online-basierten Lernplattform als Software as a Service sowie Funktionssicherungsleistungen (nachfolgend als „geschlossener Vertrag" bezeichnet) unterliegt.

Durch diese Vereinbarung wird sicher gestellt, dass personenbezogene Daten, die gemäß dem mit dem Verantwortlichen geschlossenen Vertrag 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 Verantwortlichen im Zusammenhang mit den unter dieser Vereinbarung bereit gestellten Diensten sind an den Datenschutzbeauftragten (Data Protection Officer, DPO) des Auftragsverarbeiters contact-dpo@itslearning.com zu senden.

2. Begriffsbestimmungen

„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 Auftragsverarbeiter im Auftrag des Verantwortlichen, einschließlich der Erhebung, Aufzeichnung, Abgleich, Speicherung und Offenlegung oder einer Kombination davon. Gegenstand und Einzelheiten der Verarbeitung personenbezogener Daten sind im Anhang 1 ausführlich beschrieben.

Der Auftragsverarbeiter selbst hat kein Recht die Daten für eigene Zwecke zu verarbeiten. Die personenbezogenen Daten werden ausschließlich dazu verwendet, den Zweck des geschlossenen Vertrags innerhalb des vom Verantwortlichen festgelegten Rahmens zu erfüllen.

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

4. Rolle und Verantwortlichkeit des Verantwortlichen

Der Verantwortliche hat sicher zu stellen, dass für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage besteht und dass die tatsächliche Verarbeitung in Übereinstimmung mit den anwendbaren Datenschutzgesetzen erfolgt.

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

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

Gemäß des geschlossenen Vertragskann der Verantwortliche zusätzliche Produkte von externen Drittparteien (einschließlich Erweiterungen) installieren und aktivieren. Wenn der Verantwortliche 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 Verantwortliche kann die Verwendung von Produkten externer Drittparteien aktivieren oder deaktivieren und es ist unter dem geschlossenen Vertrag nicht erforderlich, solche Produkte zu verwenden.

5. Rolle und Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen und nur in jenem Ausmaß, das der Verantwortliche bestimmt hat. Verarbeitet der Auftragsverarbeiter personenbezogene Daten, um die Sicherheit, die operativen Instandhaltung oder die Analyse oder Auswertung der unter dem geschlossenen Vertrag bereit gestellten Dienstleistungen zu gewährleisten, gilt dies nicht als eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters, wenn den Datensubjekten dadurch keine nachteiligen Auswirkungen für den Datenschutz entstehen.

Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen bereit, die erforderlich sind, um die Einhaltung der anwendbaren Datenschutzgesetze zu dokumentieren. Darüber hinaus leistet er dem Verantwortlichen 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 Verantwortliche das Recht, auf personenbezogene Daten, die vom Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet werden, sowie auf alle Systeme zuzugreifen, die zu diesem Zweck verwendet werden. Der Auftragsverarbeiter leistet dem Verantwortlichen in diesem Zusammenhang Hilfe. Der Auftragsverarbeiter ist allerdings nicht verpflichtet, dem Verantwortlichen vertrauliche oder sensible Geschäftsinformationen weiter zu geben. Darüber hinaus hat der Verantwortliche kein Zugriffsrecht, wenn dies ein Risiko für die Sicherheit oder Integrität des Systems bedeutet.

Der Auftragsverarbeiter und seine Mitarbeiter unterliegen hinsichtlich der Verarbeitung einer Geheimhaltungspflicht. Diese Bestimmung gilt auch nach Beendigung dieser Vereinbarung. Wenn die Mitarbeiter nicht bereits durch eine gesetzliche Geheimhaltungs- oder Verschwiegenheitspflicht 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 Auftragsverarbeiter zur Bereitstellung oder Verwaltung des Dienstes verwendet.

Die internen Datenzugriffsprozesse und -richtlinien des Auftragsverarbeiters wurden entwickelt, damit keine nicht-autorisierten Personen und/oder Systeme auf die Systeme zugreifen können, die zur Verarbeitung der personenbezogenen Daten verwendet werden. Der Auftragsverarbeiter 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 Auftragsverarbeiter mindestens 3 Monate aufzubewahren. Dem Verantwortlichen ist auf Anfrage Zugang zu diesen Protokollen zu gewähren.

Der Verantwortliche hat das Recht, die in Art. 28 Abs. 3 lit. h) DSGVO vorgesehene Auftragskontrolle im Benehmen mit dem Auftragsverarbeiter durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber die im Rahmen der Auftragskontrolle erforderlichen Auskünfte zu geben, Zutritt zu seinem Geschäftsbetrieb zu gewähren und die entsprechenden Nachweise verfügbar zu machen. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) vorlegen.

6. Der Datenschutzbeauftragte

Der Auftragsverarbeiter hat in Übereinstimmung mit den Bestimmungen der anwendbaren Datenschutzgesetze einen Datenschutzbeauftragten ernannt. Der Datenschutzbeauftragte ist unter folgenden Kontaktdaten zu erreichen:

Datenschutzbeauftragter der itslearning AS

John Arthur Berg
Data Protection Officer (DPO)
itslearning AS
Solheimsgaten 7D
5058 Bergen, Norwegen

+ 47 55 23 60 70
contact-dpo@itslearning.com

Bei Änderungen informiert der Auftragsverarbeiter den Verantwortlichen.

7. Einsatz von Sub-Verarbeitern und Export von Daten

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

Die im Anhang 4 angeführten Sub-Verarbeiter werden hiermit vom Verantwortlichen zugelassen. Falls der Verantwortliche detailliertere Informationen zu Verarbeitungsstandorten benötigt, um gesetzliche Anforderungen einzuhalten oder Anfragen von Datenschutzbehörden nachzukommen, unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung dieser Anforderungen, vorausgesetzt, dass der Verantwortliche vor der Bereitstellung solcher Informationen die aus Sicht des Auftragsverarbeiters 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 Verantwortlichen offen zu legen. Dies kann unter anderem durch automatisierte Mitteilungen an den Verantwortlichen oder, wenn erforderlich, auf anderen Wegen geschehen. Innerhalb von vier Wochen nach Erhalt einer solchen Mitteilung kann der Verantwortliche eine solche Änderung oder Ergänzung ablehnen, wobei diese Ablehnung ausschließlich auf nachvollziehbaren Gründen beruhen darf.

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

Der Auftragsverarbeiter und jeder potenzielle Sub-Verarbeiter dürfen die personenbezogenen Daten ohne die vorherige schriftliche Zustimmung des Verantwortlichen 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 Verantwortliche personenbezogene Daten in einem Drittstaat oder greift er aus einem Drittstaat auf diese zu, gilt dieser Vorgang in Bezug auf den Auftragsverarbeiter oder einen Sub-Verarbeiter nicht als Transfer personenbezogener Daten in einen solchen Drittstaat.

Soweit ein solcher Transfer personenbezogener Daten erfolgt, entweder an Auftragsverarbeiter-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 (insbesondere Art. 44 ff. DSGVO) ein adäquates Datenschutzniveau bieten.

8. Sicherheit

a. Sicherheitsmaßnahmen und Dokumentation

Der Auftragsverarbeiter hat die in den anwendbaren Datenschutzgesetzen vorgeschriebenen Anforderungen in Bezug auf Sicherheitsmaßnahmen zu erfüllen. Der Auftragsverarbeiter ist verpflichtet, seine Sicherheitsmaßnahmen als Bestandteil des ISMS-Prozesses gemäß ISO 27001 zu dokumentieren. Anhang 3 enthält eine Übersicht über die Sicherheitsmaßnahmen des Auftragsverarbeiters. Ausführlichere Dokumentationen werden dem Verantwortlichen auf dessen Anfrage zur Verfügung gestellt.

Der Auftragsverarbeiter hat geeignete technische und organisatorische Sicherheitsmaßnahmen einzuführen und aufrecht zu erhalten, um ein Sicherheitsniveau zu gewährleisten, das dem verbundenen Risiko entspricht. Dabei ist unter anderem auch zu prüfen, welche Art von Cloud-Diensten dem Verantwortlichen 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 Auftragsverarbeiter 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 Verantwortliche und der Auftragsverarbeiter stellen sicher, dass ihnen unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind gemäß den anwendbaren Datenschutzgesetzen oder anderen Gesetzen dazu verpflichtet.

b. Übersicht über die Verarbeitungstätigkeiten

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

a) den Namen und die Kontaktdaten des Auftragsverarbeiters und des Datenschutzbeauftragten;
b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen 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 Auftragsverarbeiter 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 dem Verantwortlichen gemeldet werden, der in Abschnitt 1 dieser Vereinbarung angeführt ist. Eine solche Meldung hat unverzüglich und möglichst binnen 72 Stunden, nachdem dem Auftragsverarbeiter 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 Verantwortliche 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 Auftragsverarbeiter 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 anderer physische Dokumente.

Darüber hinaus verfügt der Auftragsverarbeiter 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 Auftragsverarbeiter hat Sicherheitsmaßnahmen einzurichten und aufrecht zu erhalten, die bei der Bewertung von Sicherheits- und Technologierisiken als notwendig erachtet wurden.

9. Aktualisierungen von Verarbeitungstätigkeiten und Sicherheitsüberprüfungen

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

Der Auftragsverarbeiter 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 Verantwortlichen zur Verfügung zu stellen, unter anderem auch für die Verwendung in der Sicherheitsüberprüfung des Verantwortlichen.

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

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

10. Dauer der Vereinbarung

Die Vereinbarung gilt ab dem Zeitpunkt, an dem die Parteien dieser Vereinbarung zugestimmt haben und sie bleibt in Kraft, solange der geschlossene Vertrag aufrecht ist.

Bei Verletzung dieser Vereinbarung oder der anwendbaren Datenschutzgesetze kann der Verantwortliche den Auftragsverarbeiter anweisen, die Weiterverarbeitung personenbezogener Daten zu stoppen und den zugrundeliegenden Vertrag außerordentlich kündigen.

11. Rückgabe und Löschung bei Beendigung dieser Vereinbarung

Nach Beendigung dieser Vereinbarung ist der Auftragsverarbeiter verpflichtet, die Daten zurückzugeben, zu überschreiben und/oder 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. Hierbei sind mögliche Rechte der Betroffenen zu beachten. Der Auftragsverarbeiter hat nach Beendigung dieser Vereinbarung innerhalb eines angemessenen Zeitraums schriftlich zu dokumentieren, dass eine solche Handlung in Übereinstimmung mit dieser Vereinbarung stattgefunden hat.

12. Wahl des anzuwendenden Rechts und Gerichtsstand

Die Wahl des anzuwendenden Rechts und des Gerichtsstands wird in dem geschlossenen Vertrag geregelt oder zwischen den Parteien dieser Vereinbarung vereinbart.

***

Vereinbart für und im Namen von itslearning (AUFTRAGSVERARBEITER)	Vereinbart für und im Namen des Kunden (VERANTWORTLICHER)
itslearning GmbH	Gymnasium „Friedrich Ludwig Jahn"
[redacted]	[redacted]
Geschäftsführer Deutschland	Schulleiter
Berlin, den 19.05.2020:	Greifswald, den 15.06.2020

Unterschriften [redacted]

itslearning GmbH
Eric[redacted]tr. 6
T. [redacted]847
F. [redacted]967
ww[redacted].de

Gymnasium
„Friedrich Ludwig Jahn"
Dietrich-Bonhoeffer-Platz 1
17489 Greifswald
Haus 1: Tel. 03834 7920 * Fax 792222
Haus 2: Tel. 03834 8533090 * Fax 8533099

2020-06-18

ANHANG 1

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

itslearning verarbeitet als Auftragsverarbeiter im Auftrag des Verantwortlichen 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 dem geschlossenen Vertrag
- Bereitstellung von grundlegendem technischen Support im Zusammenhang mit den Diensten, die gemäß der Datenverarbeitungsvereinbarung und dem geschlossenen Vertrag erbracht werden
- Sicherung der Daten des Verantwortlichen
- Der Auftragsverarbeiter kann Informationen über die Nutzung des Dienstes durch den Verantwortlichen für interne statistische Zwecke und für Fakturierungszwecke erheben. Diese Daten werden aggregiert erhoben und sind in keinerlei Hinsicht auf Einzelne zurückführbar.

Dauer der Verarbeitung

Die Laufzeit des geschlossenen Vertrags zuzüglich des Zeitraums nach Ablauf der Vereinbarung bis zur Löschung sämtlicher Kundendaten, die der Auftragsverarbeiter gemäß der Vereinbarung durchführt.

Kategorien personenbezogener Daten

Der Auftragsverarbeiter verarbeitet personenbezogene Daten, die über den Service durch den Verantwortlichen (oder auf seine Anweisung) übermittelt, gespeichert, importiert, gesendet oder empfangen werden. Der Umfang der zu erfassenden Daten liegt im alleinigen Ermessen der nutzenden Personen. Die Daten umfassen die folgenden Kategorien:

- Kontaktinformationen (Name, Benutzername, Klassen- / Gruppenzugehörigkeit.)
- Kommunikation (Nachrichten zwischen Benutzern, Diskussionen, Kommentare zu Beiträgen, Benachrichtigungen.)
- Kursmaterialien
- Bewertungen (keine Benotung)
- Kalendereinträge und Ereignisdaten
- Dokumente, Präsentationen, Videos, Bilder, Hausaufgaben, Aufgaben, Nachrichten

Betroffene Personen

Die Verarbeitung personenbezogener Daten durch den Dienst im Auftrag des Auftragsverarbeiters 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 Schüler und Eltern/Erziehungsberechtigte.

ANHANG 2 | LÖSCHUNGSROUTINEN

Löschung von Daten nach Beendigung dieser Vereinbarung

Innerhalb von 6 Monaten nach Beendigung der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter werden alle im Auftrag des Verantwortlichen 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 Auftragsverarbeiters zur Wiederverwendung oder zur Vernichtung verlassen. So soll sichergestellt 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.

Recht auf Löschung ("Recht auf Vergessenwerden")

Das Löschen eines Nutzers und den damit verbundenen personenbezogenen Daten wird dann vollzogen, wenn der Verarbeitungszweck nicht mehr gegeben ist. Gewöhnlich liegt dies darin begründet, dass Schüler, Lehrer oder andere Betroffene die Bildungseinrichtung verlassen haben oder das Vertragsverhältnis mit itslearning beendet wurde. Im ersten Fall empfehlen wir den im LMS implementierten Löschvorgang für Nutzer. Diese werden in den Papierkorb verschoben oder in einem externen System als gelöscht markiert. Der Vorgang wird durch das Leeren des Papierkorbs abgeschlossen, wobei ein Nutzer und seine Daten permanent aus itslearning gelöscht werden.

Das Löschen von Informationen einer betroffenen Person gehörend basiert auf das Recht auf Löschung, wie es in der DSGVO definiert wurde. Mit Hilfe des DSGVO-Tools kann dies Löschung vollzogen werden. Weitere Details dazu können in Artikel 17 der DSGVO nachgelesen werden. Der Löschvorgang entfernt jegliche Informationen im Zusammenhang mit der betroffenen Person.

Zu beachten sind durch die DSGVO definierte Ausnahmen in Artikel 17 Absatz (3). Ein Beispiel: Eine Lehrkraft hat einen Schüler bewertet. Wird die Lehrkraft gelöscht, bleibt dieser Datensatz bestehen, um das Recht des Schülers zu wahren.

Kategorie	Wirkung des Löschvorgangs
Persönliche Informationen	permanent gelöscht
Kommunikation	Permanent gelöscht, wenn alle weiteren betroffenen Personen gelöscht wurden, die Teil der Kommunikation waren. Die Einträge bleiben bestehen, jedoch werden die Einträge der gelöschten betroffenen Person anonymisiert.
Kursmaterial von der betroffenen Person in der Rolle der Lehrkraft erstellt	Anonymisiert, außer das Material war ausschließlich für die betroffene Person verfügbar. In diesem Falle wird das Material permanent gelöscht.

Bewertungen	Wird nicht gelöscht, wenn eine Lehrkraft entfernt wurde, da die Bewertung weiter Bestand hat und das Recht des Schülers auf Erhalt besteht.
Kalendereinträge	Permanent gelöscht, wenn persönliche Termine; anonymisiert wenn geteilt.
Schülerantworten	Permanent gelöscht.
Interne Logik	Permanent gelöscht.

Löschfristen

Für die Einhalten der gesetzlichen Löschfristen ist der Verantwortliche auf Ebene der Systemadministration verantwortlich, Papierkörbe für Kurse, Projekte, Semester und Nutzer permanent zu leeren.

Eine vollständige und unwiderrufbare Löschung ist aufgrund der Backups 6 Monate nach Leerung des Papierkorbs gegeben.

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.

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 und des Datenschutzes 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
- Update- und Patchmanagement

Sicherheitsteam

itslearning verfügt über 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 der Anwendung (interne Penetrationstests und Anwendungsüberprüfungen)
- Überwachung und Protokollierung als regelmäßige Maßnahme und interne Audits
- 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 erforderlich.

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.

Anhang 4 | Sub-Verarbeiter

Stand: 28.03.2020 / Quelle: https://itslearning.com/global/gdpr/subprocessors/

itslearning verwendet die Dienste von Drittanbietern zur Unterstützung der Bereitstellung des angebotenen Dienstes (wie im Vertrag zur Auftragsverarbeitung definiert):

Sub-Verarbeiter	Land	Dienst	Daten und Verarbeitung
Amazon AWS	Germany, Ireland, France	Hosting	Datenbank itslearning LMS sowie Applikationen und Dateien
USIT (University Center for Information Technology)	Norway	Hosting	Datenbank itslearning LMS sowie Applikationen und Dateien
Proact IT Norge AS	Norway	Hosting	Speichermanagement für USIT
Cloudflare	EU	Hosting	DDOS-Schutz
Lunaweb Ltd.	Germany	Hosting	Zur Konvertierung in PDF-Format bei Druckvorgängen aus dem LMS heraus. Temporäre Speicherung während des Konvertierungsprozesses. Dauerhafte Speicherung auf AWS.
Ziggeo	EU	Video recorder/player	Erstellung und Abspielen von Videos. Temporäre Speicherung während des Erstellungsprozesses. Dauerhafte Speicherung auf AWS.

itslearning-Gruppe

Diese Einheiten innerhalb der itslearning-Gruppe erbringen Support- und Dienstleistungen für unsere Kunden.

Einheit	Land	Kategorie
itselarning AS	Norwegen	Support- und Dienstleistungen
itslearning GmbH	Deutschland	Support- und Dienstleistungen
itslearning France	Frankreich	Support- und Dienstleistungen
itslearning Nederland BV	Niederlande	Support- und Dienstleistungen
itslearning AB	Schweden	Support- und Dienstleistungen
itslearning A/S	Dänemark	Support- und Dienstleistungen
itslearning Oy	Finnland	Support- und Dienstleistungen
itslearning Ltd	Vereinigtes Königreich	Support- und Dienstleistungen
itslearning Inc.	USA	Support- und Dienstleistungen

Ergänzend:

Zusätzlich ist es dem Verantwortlichen möglich im Rahmen des geschlossenen Vertrages weitere Produkte von Drittanbietern zu installieren und/ oder zu integrieren und diese zu aktivieren/deaktivieren (inklusive Erweiterungen und LTI).

Anhang 4 | Sub-Verarbeiter

Stand: 24.09.2021 / Quelle: https://itslearning.com/global/gdpr/subprocessors/

itslearning verwendet die Dienste von Drittanbietern zur Unterstützung der Bereitstellung des angebotenen Dienstes (wie im Vertrag zur Auftragsverarbeitung definiert):

Sub-Verarbeiter	Land	Dienst	Daten und Verarbeitung
Amazon AWS	Germany, Ireland, France	Hosting	Datenbank itslearning LMS sowie Applikationen und Dateien
Proact IT Norge AS	Norway	Hosting	Speichermanagement für USIT
USIT (University Center for Information Technology)	Norway	Hosting	Datenbank itslearning LMS sowie Applikationen und Dateien
Cloudflare	EU	Hosting	DDOS-Schutz
Lunaweb Ltd.	Germany	Hosting	Zur Konvertierung in PDF-Format bei Druckvorgängen aus dem LMS heraus. Temporäre Speicherung während des Konvertierungsprozesses. Dauerhafte Speicherung auf AWS.
Ziggeo	EU	Video recorder/player	Erstellung und Abspielen von Videos. Temporäre Speicherung während des Erstellungsprozesses. Dauerhafte Speicherung auf AWS.
sdui GmbH	Deutschland	Videokonferenz	Erstellung und Durchführung von Videokonferenzen innerhalb des itslearning LMS.

itslearning-Gruppe

Diese Einheiten innerhalb der itslearning-Gruppe erbringen Support- und Dienstleistungen für unsere Kunden.

Einheit	Land	Kategorie
itselarning AS	Norwegen	Support- und Dienstleistungen
itslearning GmbH	Deutschland	Support- und Dienstleistungen
itslearning France	Frankreich	Support- und Dienstleistungen
itslearning Nederland BV	Niederlande	Support- und Dienstleistungen
itslearning AB	Schweden	Support- und Dienstleistungen
itslearning A/S	Dänemark	Support- und Dienstleistungen
itslearning Oy	Finnland	Support- und Dienstleistungen
itslearning Ltd	Vereinigtes Königreich	Support- und Dienstleistungen
itslearning Inc.	USA	Support- und Dienstleistungen

Ergänzend: Zusätzlich ist es dem Verantwortlichen möglich im Rahmen des geschlossenen Vertrages weitere Produkte von Drittanbietern zu installieren und/ oder zu integrieren und diese zu aktivieren/deaktivieren (inklusive Erweiterungen und LTI).