Auftragsverarbeitungsvertrag

gemäß Art. 28 Abs. 3 DSGVO

zwischen

Unternehmensname

Anschrift

PLZ Ort

als Auftraggeber („AG“) bzw. Verantwortlicher

und

lern.link GmbH

vertreten durch Herrn Guido Hornig (Geschäftsführer)

Kirchstraße 4, 82211 Herrsching

als Auftragnehmer („AN“)

Beide gemeinsam im Folgenden „Parteien“ genannt.

Folgendes, angekreuztes Produkt wird bzw. folgende, angekreuzte Produkte werden genutzt:

☐ Moodle lern.link-LMS

☐ WordPress mit Webshop

☒ BigBlueButton lern.link-Conference

☐ Nextcloud

Entsprechende(r) Hoster, abhängig von Ihrem/Ihren gewählten Produkt(en):

☒ Contabo GmbH

☐ NETWAYS GmbH

☒ Hetzner Online GmbH

1. Begriffsdefinitionen

1.1. **Personenbezogene Daten** sind Informationen im Sinne des Art. 4 Nr. 1 DSGVO.

1.2. **Verarbeitung** ist jeder Vorgang im Sinne des Art. 4 Nr. 2 DSGVO.

1.3. **Weisung** ist eine vom AG erlassene und an den AN gerichtete Anordnung hinsichtlich der Verarbeitung von personenbezogenen Daten. Bestehende Weisungen (z.B. aus diesem Vertrag) können vom AG durch einzelne Weisungen geändert, ergänzt oder ersetzt werden („Einzelweisung").

2. Gegenstand und Dauer des Auftrags

2.1. Dieser Vertrag regelt den Rahmen der datenschutzrechtlichen Rechte und Pflichten bei der Verarbeitung personenbezogener Daten (im Folgenden „AG-Daten") durch den AN für den AG in dessen Auftrag und nach dessen Weisungen im Sinne des Art. 28 DSGVO.

2.2. Der Gegenstand der Verarbeitung geht aus dem Hauptvertrag hervor, dem dieser Verarbeitungsvertrag angefügt ist.

2.3. Der Auftragnehmer nutzt die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

2.4. Der AG, oder der jeweilige AG des AG, ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten.

2.5. Der AN wird AG-Daten entsprechend der Weisungen des AG im Auftrag des AG, unter Einhaltung der organisatorischen und technischen Vorgaben i. S. d. Ziff. 4 verarbeiten. Hierbei verpflichtet sich der AN besonders zu beachten:

- die technischen und organisatorischen Maßnahmen (Ziff. 4)
- die Wahrung der Betroffenenrechte (Ziff. 5)
- die besonderen datenschutzrechtlichen Pflichten (Ziff. 6)
- die Vorgaben zu Unterauftragsverhältnissen (Ziff. 7)
- die Kontrollrechte des AG und eines anderen Verantwortlichen (Ziff. 8)
- die Mitteilungspflichten (Ziff. 9)
- das allgemeine Weisungsrecht des AG (Ziff. 10)
- die Rückgabe- und Löschpflichten (Ziff. 11)

2.6. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages (Ziff. 2.2), sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinaus gehende Verpflichtungen ergeben.

2.7. Die Parteien können diesen Vertrag jederzeit ohne Einhaltung von Kündigungsfristen aus wichtigem Grund kündigen. Ein wichtiger Grund liegt insbesondere vor,

- wenn ein schwerwiegender Verstoß des AN gegen gesetzliche Vorgaben, oder gegen Pflichten aus diesem Vertrag vorliegt,
- wenn der AN eine Weisung des AG missachtet, oder
- wenn der AN den Zugang des AG, eines entsprechenden Beauftragten oder einer Datenschutzaufsichtsbehörde zu den Betriebsräumen, in denen AG-Daten aufgrund dieses Vertrages verarbeitet werden, vertrags- oder weisungswidrig verweigert.
- wenn der AG der Einsetzung eines neuen Subunternehmers durch den AN widerspricht, obwohl das gleiche Datenschutzniveau gegeben ist.

2.8. Dieser Vertrag geht bei Widersprüchen bezüglich der Festlegung der datenschutzrechtlichen Pflichten, der Verantwortlichkeiten und den Konsequenzen allen anderen vertraglichen Regelungen vor, es sei denn, es wird mit ausdrücklichem Bezug auf diesen Vertrag etwas anderes vereinbart. Eine Abweichung von datenschutzrechtlichen Vorgaben gemäß DSGVO bzw. BDSG-neu ist grundsätzlich ausgeschlossen.

3. Zweck, Art und Umfang der vorgesehenen Verarbeitung, Datenarten und Kreis der Betroffenen

3.1. Zweck

Der Verarbeitungszweck bzw. der Gegenstand der Verarbeitung geht aus dem zwischen AG und AN geschlossenen Hauptvertrag hervor.

3.2. Art der Verarbeitung (Art. 4 Nr. 2 DSGVO):

Nutzung BigBlueButton lern.link-Conference

3.3. Art der personenbezogenen Daten (Art. 4 Nr. 1 DSGVO):

Name, Log-Files, Chat-Einträge, Whiteboard-Einträge, Video- und Audioaufzeichnungen, Informationen zur Web-Konferenz.

3.4. Kategorien betroffener Personen (Art. 4 Nr. 1 DSGVO):

- Vorstände bzw. Geschäftsführer
- Fachautoren
- Mitarbeiter (Angestellte, Auszubildende, Praktikanten, Werkstudenten)
- Kunden
- externe Dienstleister
- Lieferanten

4. Gewährleistung der technischen und organisatorischen Maßnahmen

4.1. Der AN bietet nach Maßgabe des Art. 28 Abs. 1 und 5 DSGVO hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit der DSGVO und den Rechten der Betroffenen steht.

4.2. Der AN trifft geeignete technische und organisatorische Maßnahmen, wie in diesem Vertrag vereinbart, die den Vorgaben des Art. 32 DSGVO entsprechen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und unterstützt den AG bei der Einhaltung der in Art. 32 DSGVO genannten Pflichten. Der AN wirkt nach Maßgabe des Art. 28 Abs. 3f) DSGVO bei der Erstellung einer Datenschutz-Folgenabschätzung i. S. d. Art. 35 DSGVO mit, sowie bei der ggf. erforderlichen vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO. Er hat dem AG die erforderlichen Angaben und Dokumente auf Anfrage zur Verfügung zu stellen. Der AN hält ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO bereit.

4.3. Sofern die Auftragsvereinbarung vor Ort beim AG, beim Kunden oder per Fernwartung erfolgt, treffen die Pflichten aus dieser Ziffer 4 den AN nur soweit die technischen und organisatorischen Maßnahmen in seinem Machtbereich liegen.

4.4. Die technischen und organisatorischen Maßnahmen unterliegen dem sich fortwährend entwickelnden Stand der Technik. Falls gesetzliche oder vertragliche Regelungen eine Anpassung bzw. Überarbeitung der in der Anlage 1 aufgeführten Maßnahmen des AN erforderlich machen, wird dieser die Maßnahmen auf eigene Kosten unverzüglich anpassen bzw. überarbeiten. Eine Absenkung des hier vereinbarten Datensicherheitsniveaus ist nicht zulässig.

4.5. Kommt trotz entsprechendem Verlangen des AG keine Einigung über die Angemessenheit der technischen und organisatorischen Maßnahmen zustande, kann der AG alle zwischen den Parteien geschlossenen Verträge, die eine Verarbeitung von AG-Daten vorsehen, mit einer Frist von 14 Tagen zum Monatsende kündigen. Die verbleibenden Vertragsbestandteile können gleichermaßen gekündigt werden, wenn das Festhalten an ihnen aufgrund der Kündigung eine unzumutbare Härte für eine Vertragspartei darstellen würde.

5. Betroffenenrechte und -klagen

5.1. Der AN erhält die Weisung, dem AG unverzüglich mitzuteilen, wenn ein Betroffener seine Betroffenenrechte gemäß Art. 15 - 21 DSGVO i.V.m. §§ 34, 35, 36 BDSG geltend macht. Hierzu zählen:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Mitteilungspflicht im Zusammenhang mit Berichtigung oder Löschung (Art. 19 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)

Ebenso wird der AN den AG unverzüglich darüber informieren, wenn ihm eine Klage auf Grundlage des Art. 82 DSGVO zugeht.

5.2. Der AN wird ausschließlich nach Weisung des AG auf Betroffenenanfragen dieser Art reagieren.

5.3. Die Regelungen der Ziffern 5.1 und 5.2 gelten analog bei Anfragen und Prüfungen der Datenschutzaufsichtsbehörden, soweit AG-Daten mindestens mittelbar von solch einer Anfrage oder Prüfung berührt sind.

5.4. Der AN stellt sicher, dass Sperrungen von Daten sowie untersagte Verarbeitungen rechtskonform umgesetzt werden.

6. Besondere datenschutzrechtliche Pflichten des AN

6.1. **Datengeheimnis:** Den mit der Verarbeitung der AG-Daten beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit in geeigneter Weise und nachprüfbar auf das Datengeheimnis gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO zu verpflichten. Das Datengeheimnis muss auch nach Beendigung der Tätigkeit fortbestehen. Soweit andere Geheimhaltungsverpflichtungen (Fernmeldegeheimnis, Sozialgeheimnis, etc.) zu wahren sind, wird der AN seine Beschäftigten entsprechend verpflichten.

Der AN hat bei der Auswahl und dem Einsatz der Beschäftigten sicherzustellen, dass diese die gesetzlichen Bestimmungen über den Datenschutz beachten und die aus der Sphäre des AG erlangten Informationen nicht an Dritte weitergeben oder zu einem anderen Zweck als dem Beauftragten verarbeiten (Art. 29 DSGVO).

Der AN wird auf Anforderung für den AG innerhalb von fünf Werktagen eine vollständige und jeweils aktuelle Liste der Beschäftigten, welche mit der Verarbeitung AG-Daten befasst sind bzw. vormals befasst waren, zur Einsicht bereit halten (Vorname, Name, einschl. eines verifizierbaren Nachweises über die Verpflichtung).

6.2. Der AN hat bei der Erstellung und Aktualisierung der Verarbeitungsübersicht des AG mitzuwirken. Dies umfasst nur Verarbeitungstätigkeiten, die im Rahmen der Auftragsverarbeitung für den AG vorgenommen werden.

6.3. Der AN unterstützt den AG gemäß Art. 28 Abs. 3e) DSGVO mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine Pflichten gegenüber den Betroffen i. S. d. Kapitel 3 der DSGVO erfüllen kann.

7. Begründung von Unterauftragsverhältnissen (Subunternehmer)

7.1. Dem AN ist es gestattet Subunternehmer zur Erfüllung seiner vertraglichen Pflichten einzusetzen, sofern er den AG rechtzeitig (grundsätzlich 6 Wochen) vor der Datenverarbeitung hierüber informiert (Art. 28 Abs. 2 DSGVO). Zudem muss der AN dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat (Art. 28 Abs. 1 DSGVO). Zwischen dem Subunternehmer und dem AN ist ebenso ein Auftragsverarbeitungsvertrag zu schließen (Art. 28 Abs. 4 DSGVO).

7.2. Eine Einsetzung von in Drittländern ansässigen Subunternehmern darf nur erfolgen, wenn die Voraussetzungen der Art. 44 – 50 DSGVO erfüllt sind.

7.3. Widerspricht der AG nicht innerhalb von 4 Wochen nach Erhalt der Information, akzeptiert er die Einsetzung als genehmigt im Sinne dieses Vertrages. Der AG kann der Einsetzung eines Subunternehmers widersprechen, jedoch kann der AN dann von seinem Sonderkündigungsrecht (siehe 2.7) Gebrauch machen.

7.4. Der AN stellt sicher, dass der Subunternehmer gegenüber dem AN in entsprechender Weise verpflichtet ist, wie der AN gegenüber dem AG nach dieser Vereinbarung verpflichtet ist. Der AN hat die Einhaltung dieser Pflichten des Subunternehmers, insbesondere die Einhaltung der dort vereinbarten technischen und organisatorischen Maßnahmen, vor Beginn der Datenverarbeitung und sodann regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

7.5. Der AN stellt ferner sicher, dass der AG gegenüber dem Subunternehmer die gleichen Kontrollrechte eingeräumt bekommt, wie der AG sie gegenüber dem AN selbst hat.

7.6. Der AN haftet gegenüber dem AG dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den AN im Einklang mit 7.1, 7.4 sowie 7.5 vertraglich auferlegt wurden.

7.7. Zurzeit verarbeiten folgende Subunternehmer personenbezogene Daten im Auftrag des AN:

Contabo GmbH

Firmensitz:

Aschauer Straße 32a

81549 München

Telefon: +49 89 3564 717 71

E-Mail: info@contabo.de

Ort der Datenverarbeitung/lern.link-Conference-Server:

Grünberger Straße 27

90475 Nürnberg

HETZNER Online GmbH

Industriestraße 25

91710 Gunzenhausen

Telefon: +49 9831 505-0

E-Mail: info@hetzner.com

Zertifiziert: ISO 27001

Der AG gestattet den Einsatz dieser Subunternehmer für sein gewähltes Produkt bzw. seine gewählten Produkte, soweit jeweils die Pflichten aus 7.1, 7.4 sowie 7.5 erfüllt werden.

7.8. Die in 7.7 genannten Subunternehmen (Hoster) haben grundsätzlich keinen Zugriff auf personenbezogene Daten, welche dort im Auftrag des AN verarbeitet werden. Lediglich falls ein Fehler identifiziert wird, darf der AN den Subunternehmer beauftragen, diesen zu beheben, wobei nur in diesem Fall auch ein Zugriff auf personenbezogene Daten erforderlich sein kann und gestattet wird. Der Vorgang ist zu protokollieren.

8. Kontrollrechte des AG, Mitwirkungs- und Duldungspflichten des AN

8.1. Der AG, der Auftraggeber des AG oder dessen schriftlich Beauftragter haben das Recht, die Befolgung sämtlicher Weisungen und Bestimmungen dieser Vereinbarung durch den AN zu verlangen und nach schriftlicher Vorankündigung von vierzehn (14) Werktagen (mit sachlichem Grund - insbesondere nach Beschwerdefällen auch mit einer schriftlichen Vorankündigung von 24 Stunden), zu den üblichen Geschäftszeiten zeitlich und räumlich unbeschränkt, auf dem Grundstück und in den Geschäftsräumen des AN zu kontrollieren.

8.2. Dies umfasst insbesondere die Überprüfung der technischen und organisatorischen Maßnahmen vor Beginn der Datenverarbeitung und weitere regelmäßige Überprüfungen, insbesondere der geforderten Datenschutz- und Sicherheitsmaßnahmen.

8.3. Der AN verpflichtet sich entsprechende Überprüfungen zu dulden, Zugang, Auskunft und Einsicht in alle dazu erforderlichen Unterlagen und Datenverarbeitungssysteme zu gewähren.

8.4. Über die Kontrolle und deren Ergebnisse ist ein Protokoll anzufertigen, das vom AG, dem Auftraggeber des AG und AN bzw. deren Beauftragte zu unterzeichnen ist.

9. Mitteilungspflichten des AN

9.1. Der AN wird den AG unverzüglich von jedem Empfang von Anfragen oder Aufforderungen von einem Betroffenen oder einer Datenschutzaufsichtsbehörde bezüglich des Gegenstandes dieses Vertrages, insbesondere nach Ziff. 5.1, informieren.

9.2. Dem AN ist bekannt, dass der AG verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und gegebenenfalls der Datenschutzaufsichtsbehörde bzw. den Betroffenen binnen 72 Stunden zu melden (Art. 33 DSGVO). Sofern es zu solchen Verletzungen gekommen ist, wird der AN den AG bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem AG melden und hierbei zumindest folgende Informationen bereitstellen:

- Eine Beschreibung der Art der Verletzung, der betroffenen Datenkategorien sowie die ungefähre Zahl der Betroffenen und Datensätze.
- Name und Kontaktdaten eines Ansprechpartners für weitere Informationen.
- Eine Beschreibung der wahrscheinlichen Folgen der Verletzung.
- Eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

9.3. Mitteilungen nach Ziff. 9.1 und 9.2 müssen unverzüglich, jedoch nicht später als innerhalb von 24 Stunden, in Textform (z.B. Brief, Telefax oder E-Mail) übermittelt werden.

10. Weisungsrecht des AG, Haftungsfreistellung

10.1. Der AN verarbeitet AG-Daten ausschließlich im Rahmen dieser vertraglichen Vereinbarung und weiterer Weisungen des AG.

10.2. Der AG wird weitere Weisungen (fern-)mündlich, per Brief, Fax oder E-Mail erteilen. (Fern-)mündlich erteilte Weisungen sind vom AN zu dokumentieren.

10.3. Weisungsberechtigt sind die Geschäftsführer des AG sowie die jeweiligen Kontaktpersonen des AN beim AG.

10.4. Ist der AN der Ansicht, dass eine Weisung gegen die DSGVO oder sonstige Datenschutzvorschriften der Europäischen Union bzw. der Bundesrepublik Deutschland verstößt, weist der AN den AG unverzüglich per Brief, Telefax oder E- Mail darauf hin. Der AN ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie vom AG ausdrücklich bestätigt wird.

10.5. Der AN ist gegenüber dem AG verantwortlich für die Einhaltung seiner Verpflichtungen aus diesem Vertrag. Sofern Verstöße des AN gegen die Bestimmungen dieses Vertrags oder Einzelweisungen des AG zu Rechtsverletzungen führen, stellt der AN den AG von Ansprüchen Dritter frei; außerdem übernimmt der AN die erforderlichen Kosten der Rechtsverteidigung.

10.6. Der AN darf Verarbeitungen von AG-Daten nur dann ohne Weisung des AG durchführen, wenn er aufgrund einer Vorschrift der DSGVO oder einer sonstigen Rechtsvorschrift der Europäischen Union bzw. eines Mitgliedsstaates der Europäischen Union, der der AN unterliegt, hierzu verpflichtet ist. Der AN informiert den AG hierüber, bevor er mit der Verarbeitung beginnt, soweit ihm eine solche Mitteilung nicht durch eine anwendbare Rechtsvorschrift untersagt ist.

11. Rückgabe- und Löschungspflichten

11.1. Sofern keine gegenteilige Weisung erteilt wird, hat der AN dem AG bei Beendigung des Auftrags die ihm überlassenen Datenträger und Dokumente herauszugeben.

11.2. Weiterhin sind bei Beendigung des Auftrags vom AN verwendete AG-Daten – wenn nicht bereits zuvor geschehen – zu löschen, zu vernichten oder dem AG zu übergeben.

11.3. Auf Anfrage des AG bestätigt der AN, dass der AN die überlassenen Daten vollständig zurückgegeben, vernichtet bzw. unwiederbringlich gelöscht hat.

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind vom AN für mindestens drei Jahre nach Ende ihrer Geltungsdauer aufzubewahren. Der AN kann bei Vertragsende die Dokumentationen zu seiner Entlastung dem AG übergeben.

11.5. Die Pflicht zur Löschung bzw. Vernichtung besteht nicht, solange eine gesetzliche Aufbewahrungspflicht entgegensteht.

12. Haftung und Schadensersatz

AG und AN haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

13. Schlussbestimmungen

13.1. Sollte Eigentum des AG beim AN durch Maßnahmen Dritter (z.B. Pfändung, Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet sein, so hat der AN den AG unverzüglich hierüber in Kenntnis zu setzen. Ein Zurückbehaltungsrecht in Bezug auf Datenträger oder Datenbestände des AG ist ausgeschlossen. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der Datenschutz-Grundverordnung liegen.

13.2. Die Einrede des Zurückbehaltungsrechts i.S.d. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der dazugehörigen Datenträger ausgeschlossen.

13.3. Änderungen und Ergänzungen dieses Vertrags und all seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Die Änderung bzw. Ergänzung kann auch in einem elektronischen Format (Textform) erfolgen (Art. 28 Abs. 9 DSGVO).

13.4. Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages zum Datenschutz den Regelungen des Hauptvertrages (Ziff. 2.2) vor. Sollte eine der vorliegenden Regelungen unwirksam sein, so berührt dies nicht die Wirksamkeit der übrigen Bestimmungen.

13.5. Die Anlage 1 (Technische und organisatorische Maßnahmen) ist Bestandteil dieses Vertrags.

13.6. Der AG hat sich vergewissert, dass der AN die gesetzlich vorgeschriebenen technischen und organisatorischen Maßnahmen ab Vertragsbeginn zu erfüllen vermag.

13.7. Es gilt deutsches und europäisches Recht.

Ort

Datum

Herrsching, 10.07.2020

Unterschrift

(Auftraggeber)

Guido Hornig, lern.link GmbH

(Auftragnehmer)

lern.link GmbH
Kirchstr. 4 - D 82211 Herrsching
+49 8152 909090 www.lern.link
Geschäftsleitung: Guido Hornig
HRB 245666 AG München

Anlage 1 - Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO

lern.link GmbH

Die lern.link GmbH (lern.link) als Auftragsverarbeiter trifft die folgenden technischen und organisatorischen Maßnahmen (TOM), eingerichtet nach erfolgter Risikoabschätzung, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau sicherzustellen. Bei der Erstellung der TOM flossen die relevanten technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit und Informationstechnik (BSI) mit ein. Lern.link nutzt insbesondere Pseudonymisierung und Verschlüsselung personenbezogener Daten, um zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von lern.link- Systemen und -Dienstleistungen beizutragen und um die Verfügbarkeit personenbezogener Daten bei unvorhergesehenen Zwischenfällen unmittelbar wiederherstellen zu können. Wiederkehrend intern stattfindende Evaluationen (Systemtests, Prüfung von kundenseitigen Fehlermeldungen, Hinweise von Subunternehmern, Incident Response, etc.) der Wirksamkeit der TOM gewährleisten ein anhaltend hohes Sicherheitsniveau bei der Datenverarbeitung.

Die technischen und organisatorischen Maßnahmen betreffen den Schutz der Datenverarbeitung sowohl in der genutzten IT-Infrastruktur, bei Subunternehmen, als auch im Bürogebäude der lern.link GmbH.

Bei der Erstellung der folgenden Kontrollbereiche wurde auch auf § 64 BDSG-neu zurückgegriffen, auch wenn dieser Paragraf ursprünglich nur für öffentliche Stellen vorgesehen ist. Dadurch kann jedoch ein äußerst umfangreiches Schutzniveau garantiert werden.

I. Zugangskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet werden:

a) Rechenzentrum/Hoster

- Der bzw. die ausgewählten, renommierten Anbieter für den Betrieb des Rechenzentrums (siehe Seite 1, Auftragsverarbeitungsvertrag) verfügt bzw. verfügen über ein dokumentiertes Informationssicherheitsmanagementsystem.
- Die eingerichteten technischen und organisatorischen Maßnahmen des bzw. der Hoster werden regelmäßig durch eine unabhängige dritte Stelle überprüft.
- Die Zutrittskontrollen umfassen dabei: Zutritt nur für autorisierte Mitarbeiter und autorisiertes Fremdpersonal; Einsatz elektronischer Zutrittskontrollsysteme; Sichtkontrolle und Besucherbuch; Videoüberwachung; Alarmanlage; personelle Besetzung 24/7.

b) Geschäftsräume

- Der Haupteingang ist mit einem mechanischen Zylinderschloss gesichert.
- Nur Mitarbeiter von lern.link sind zutrittsberechtigt und erhalten einen passenden Schlüssel, mit dem sie nur Zutritt zu Geschäftsräumen erhalten, die zur Ausübung ihrer Tätigkeit notwendig sind. Über die an Mitarbeiter ausgegebene Schlüssel wird Protokoll geführt.

II. Datenträgerkontrolle

Maßnahmen, die verhindern, dass Unbefugte die Daten auf Datenträgern lesen, kopieren, verändern oder löschen.

- Daten werden nur auf Servern und (externen) Festplatten/Synology NAS gespeichert und verarbeitet oder in Papierform. Somit sind keine Daten auf CD-ROM, USB-Sticks oder sonstigen Medien vorhanden.
- Papier-Dokumente mit personenbezogenen Daten werden bei Abwesenheit in abschließbaren Möbeln weggesperrt.
- Nicht mehr benötigte Dokumente werden datenschutzkonform vernichtet.
- Der administrative Zugang zu Serversystemen ist autorisierten Administratoren vorbehalten. Die Anmeldung an Servern erfolgt über verschlüsselte Verbindungen mit kryptographischen Schlüsseln (SSH mit Passwort), nach aktuellem Stand der Technik.

III. Speicherkontrolle

Maßnahmen, die verhindern, dass Unbefugte personenbezogene Daten eingeben können bzw. personenbezogene Daten verändern oder löschen können bzw. davon Kenntnis nehmen können.

- Der administrative Zugang zu Serversystemen ist autorisierten Administratoren vorbehalten. Die Anmeldung an Servern erfolgt über verschlüsselte Verbindungen mit kryptographischen Schlüsseln (SSH mit Passwort), nach aktuellem Stand der Technik.
- Alle Benutzerkonten und damit auch der Zugang zu Daten auf Servern sind mit individuellen Passwörtern gesichert, die jeweils nur dem Inhaber des Benutzerkontos bekannt sind und auch innerhalb der Organisation anderen Personen nicht mitgeteilt werden dürfen.
- Benutzerpasswörter müssen mindestens acht (8) Zeichen umfassen und jeweils mindestens einen Groß und Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten. Die Verwendung von Trivialpasswörtern (z. B. 123456789, qwertzuiop) ist untersagt. Die Sperrung eines Zugangs nach mehrfacher Falscheingabe ist systemseitig nicht möglich.

IV. Benutzerkontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Jeder Mitarbeiter verfügt über eine eigenes und personalisiertes Benutzerkonto.
- Alle Benutzerkonten sind mit individuellen Passwörtern gesichert, die jeweils nur dem Inhaber des Benutzerkontos bekannt sind und auch innerhalb der Organisation anderen Personen nicht mitgeteilt werden dürfen.
- Benutzerpasswörter müssen mindestens acht (8) Zeichen umfassen und jeweils mindestens einen Groß und Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten. Die Verwendung von Trivialpasswörtern (z. B. 123456789, qwertzuiop) ist untersagt. Die Sperrung eines Zugangs nach mehrfacher Falscheingabe ist systemseitig nicht möglich.
- Alle Mitarbeiter von lern.link werden schriftlich auf das Datengeheimnis verpflichtet.
- Alle Mitarbeiter von lern.link werden schriftlich auf das Fernmeldegeheimnis im Sinne des § 88 TKG verpflichtet.
- Die Mitarbeiter werden mindestens einmal jährlich zu den Themen Datenschutz und Informationssicherheit geschult.

- Nach spätestens 15 Minuten Inaktivität werden Arbeitsplatzcomputer automatisch vom System gesperrt und können nur nach Eingabe des Benutzerpassworts entsperrt werden.
- Der administrative Zugang zu Serversystemen ist autorisierten Administratoren vorbehalten. Die Anmeldung an Servern erfolgt über verschlüsselte Verbindungen mit kryptographischen Schlüsseln (SSH mit Passwort), nach aktuellem Stand der Technik.
- Alle produktiven Serversysteme sind durch Firewalls nach aktuellem Stand der Technik abgesichert, die sowohl ein-, als auch ausgehend nur die intendierten Übertragungsprotokolle zulassen (default-deny).
- Es ist ein betrieblicher Datenschutzbeauftragter bestellt, der im Rahmen seiner Tätigkeit weisungsfrei agiert.

V. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Die Nutzung des Internetzugangs und der E-Mail-Konten ist ausschließlich zu dienstlichen Zwecken zulässig. Mit dieser Maßnahme wird das Risiko für Schadsoftware deutlich reduziert.
- Die Nutzung der IT- und TK-Systeme selbst ist ebenso ausschließlich zu dienstlichen Zwecken gestattet. Fremdpersonen dürfen diese nicht bedienen.
- Das Einbringen von privaten IT- und TK-Systemen, wie zum Beispiel Laptops, Smartphones und USB-Speichern ist nicht gestattet.
- Die Benutzerverwaltung erfolgt rollenbasiert und folgt einem standardisierten Rollen- und Berechtigungskonzept.
- Rechte können stets nur bei einem Verantwortlichen eingestellt werden, so dass eine Verwechslung oder ein Fehleintrag bei einem anderen Verantwortlichen ausgeschlossen sind.
- Es obliegt dem Verantwortlichen selbst, zugewiesene Rechte zu kontrollieren.
- Nur sofern dies vom Verantwortlichen gewünscht und beauftragt ist, ordnet der AN Rechte zu.
- Die Rechteverwaltung wird über Plesk (Serververwaltung), einem Konfigurationstool für Webhosting, und auf Shell-Ebene mittels Public Certificate gesteuert.
- Der Zugang zum Server kann nur über eine vom AN dezidiert vorgegebene IP-Adresse erfolgen.
- Regelmäßige Prüfungen der bestehenden Berechtigungen durch lern.link.
- Durchgeführte Änderungen an Dateien werden dokumentiert.
- Die Benutzerrechte sind auf das Minimum eingeschränkt, das zur Aufgabenerfüllung notwendig ist (Need-to-know Prinzip).

VI. Übertragungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder ihrer Speicherung auf einem Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Die Datenübermittlung wird protokolliert und erfolgt verschlüsselt (HTTPS, SMTP-STARTTLS), stets nach aktuellem Stand der Technik.
- Physische Datenträger werden verschlüsselt, stets nach aktuellem Stand der Technik.
- Der AN beauftragt einen festen Mitarbeiter, der für das Löschen bzw. Vernichten von Datenträgern zuständig ist und die entsprechenden Prozesse überwacht. Hierzu gehören u. a. erforderliche Absprachen zwischen Abteilungen bzw. AN und Subunternehmen moderieren, wie auch die Prüfung, ob sämtliche Voraussetzungen zur Vernichtung bzw. Löschung vorliegen. Der Löschbeauftragte stellt fortlaufend sicher, dass sämtliche Mitarbeiter des AN über die Lösch- und Vernichtungsprozeduren von Daten informiert sind und nutzt hierfür auch eine schriftliche Dokumentation der unternehmensinternen Lösch- bzw. Vernichtungsprozeduren, welche von ihm einmal jährlich angepasst wird.
- Datenträger werden nach Nutzung grundsätzlich vernichtet, nachdem zuvor die Inhalte vollständig gelöscht wurden. Die Löschung erfolgt mittels Nutzung entsprechender Tools nach aktuellem Stand der Technik und an den entsprechenden Datenträger angepasst. Es ist stets sichergestellt, dass Daten auf Datenträgern nicht nur zum Überschreiben freigegeben werden, sondern tatsächlich, unwiederbringlich und mehrfach überschrieben und somit gelöscht werden. Eine innerbetriebliche Weitergabe von Datenträgern ist grundsätzlich nicht gestattet.
- Die aktuell hierzu zu verwendenden Tools sind dem für Löschung und Vernichtung beauftragten Mitarbeiter und der Führungsebene des AN bekannt. Eine Prüfung, ob zwischenzeitlich bessere Tools zur Verfügung stehen erfolgt mehrfach im Jahr.
- Zur Vernichtung bzw. Löschung vorgesehene Datenträger werden an einem abgeschlossenen Ort aufbewahrt, zu dem nur die Leitungsebene des AN Zutritt hat.
- Die Vernichtung von Datenträgern erfolgt stets bei einem qualifizierten, externen Dienstleister, in dessen Räumlichkeiten.
- Beim Subunternehmer Contabo können Daten nur nach dokumentierter Weisung des AN gelöscht werden. Vom AG an den AN gereichte Löschaufträge werden vom AN unmittelbar an den Subunternehmer Contabo weitergeleitet, der die entsprechende Löschung durchführt.
- Im Falle der Beendigung des Haupt- bzw. AV-Vertrages zwischen AG und AN weist der AN Contabo unmittelbar darauf hin, dass sämtliche zum Subunternehmer gelangten Daten datenschutzgerecht vernichtet werden. Hierüber führt das Subunternehmen ein Protokoll, das die rechtskonform erfolgte Datenlöschung bzw. Vernichtung bestätigt. Dieses Protokoll kann vom AG und AN bei Bedarf bei Contabo angefragt werden.
- Beim Subunternehmer Hetzner werden nach Vertragskündigung bzw. Auftragsbeendigung die im Rechenzentrum genutzten Festplatten mittels eines intern definierten Verfahrens mehrfach überschrieben (gelöscht). Es findet eine Prüfung auf vollständige Datenlöschung statt. Nur hierbei positiv geprüfte Festplatten können erneut genutzt werden. Defekte Festplatten, bei denen eine sichere Datenlöschung nicht möglich ist, werden im Rechenzentrum direkt zerstört bzw. geschreddert.

VII. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Die Eingabekontrolle erfolgt über eine ausführliche Protokollierung aller Schreib-, Änderungs- und Löschaktivitäten innerhalb der Anwendungen und Systeme.
- Berechtigungen nach dem Least-privilege-Prinzip stellen sicher, dass unberechtigten Personen die Eingabe, Veränderung, Löschung von Daten nicht möglich ist.
- Jeder Mitarbeiter verfügt über eine eigenes und personalisiertes Benutzerkonto.
- Alle Benutzerkonten sind mit individuellen Passwörtern gesichert, die jeweils nur dem Inhaber des Benutzerkontos bekannt sind und auch innerhalb der Organisation anderen Personen nicht mitgeteilt werden dürfen. Somit kann stets nachvollzogen werden, welcher eingeloggte Mitarbeiter welche Eingaben getätigt hat.

VIII. Transportkontrolle

Maßnahmen, die beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten schützen.

- Nicht mehr benötigte Papierdokumente (auch Notizen, Fehldrucke und -kopien) und Datenträger mit personenbezogen Daten oder anderen vertraulichen Informationen werden unwiederbringlich vernichtet, sofern dem keine gesetzlichen oder vertraglich auferlegten Aufbewahrungsfristen entgegenstehen.
- Papierdokumente werden mit Aktenvernichtern der Sicherheitsstufe P-4 im Kreuzschnittverfahren hausintern vernichtet bzw. von einem qualifizierten, externen Dienstleister zur Vernichtung abgeholt.
- Zur Vernichtung vorgesehene Papierdokumente werden an einem abgeschlossenen Ort aufbewahrt, zu dem nur die Leitungsebene des AN Zutritt hat.
- Zur Vernichtung bzw. Löschung vorgesehene Datenträger werden an einem abgeschlossenen Ort aufbewahrt, zu dem nur die Leitungsebene des AN Zutritt hat.
- Die Vernichtung von Datenträgern erfolgt stets bei einem qualifizierten, externen Dienstleister, in dessen Räumlichkeiten.

IX. Wiederherstellbarkeit

Maßnahmen, die sicherstellen, dass bei auftretenden Störungen die IT-Systeme vollumfänglich wiederhergestellt werden können.

- Es werden regelmäßige Backups erstellt.
- Die Datenbestände werden durch regelmäßige Datensicherungen geschützt. Eine Auslagerung an eine andere Geolokation ist beim Produkt „BigBlueButton lern.link-Conference“ nicht möglich.
- Falls der Kontakt zu einem Server unterbrochen wird, kann auf lokale Backups auf einem Synology-NAS zurückgegriffen werden.

X. Zuverlässigkeit

Maßnahmen, die sicherstellen, dass sämtliche Funktionen der IT-Systeme stets zur Verfügung stehen und auftretende Störungen bzw. Fehler gemeldet werden.

- Sicherheitsupdates für Betriebssysteme und Software werden über automatische Update-Mechanismen eingespielt. Es wird eine kommerzielle Anti-Malware-Software eingesetzt und automatisch aktualisiert.
- Alle Server sind durch redundante Stromkreise, USV-Anlagen und Dieselgeneratoren gegen Stromausfall gesichert. Server sind mit redundanten Netzteilen ausgestattet.
- Die USV-Anlage filtert vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes.
- Die Datenbestände werden durch regelmäßige Datensicherungen geschützt. Eine Auslagerung an eine andere Geolokation ist beim Produkt „BigBlueButton lern.link-Conference“ nicht möglich.
- Lokale Backups erfolgen auf ein Synology-NAS.
- Professionelle Klimatisierung.
- Der Subunternehmer Contabo hat ein Incident-Response-Management-System implementiert. Dieses beinhaltet ein ausgeklügeltes Schutzsystem, welches u. a. aus einem aktuellen Virenschutzprogramm und einer Firewall besteht. Weiterhin sind für den Fall eines Angriffsversuchs von außerhalb genaue Meldewege und Notfallpläne definiert. Dadurch ist es dem Subunternehmer möglich Angriffe bereits im Anfangsstadium zu identifizieren und umgehend Bekämpfungsmaßnahmen einzuleiten.
- Der Subunternehmer Hetzner hat ein Incident-Response-Management-System implementiert und für sämtliche, internen Systeme eine Eskalationskette definiert, um im Fehlerfall die passenden Stellen schnellstmöglich zu informieren, so dass das System umgehend wieder vollumfänglich hergestellt werden kann. Hetzner hat ein Back-up und Recovery-Konzept mit täglicher Datensicherung, wie auch einer Festplattenspiegelung, implementiert. Weiterhin sind eine Softwarefirewall und Portreglementierungen im Einsatz, ebenso ein ständig aktiver DDoS-Schutz.

XI. Datenintegrität

Um zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden, müssen die technischen Systeme stets auf dem neuesten Stand gehalten werden:

- Sicherheitsupdates für Betriebssysteme und Software werden über automatische Update-Mechanismen eingespielt. Es wird eine kommerzielle Anti-Malware-Software eingesetzt und automatisch aktualisiert.
- Die Datenbestände werden durch regelmäßige Datensicherungen geschützt. Eine Auslagerung an eine andere Geolokation ist beim Produkt „BigBlueButton lern.link-Conference“ nicht möglich.

XII. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Es ist ein betrieblicher Datenschutzbeauftragter bestellt, der angemessen und effektiv in die relevanten betrieblichen Prozesse eingebunden wird.
- Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet.
- Die Mitarbeiter werden mindestens einmal jährlich zu den Themen Datenschutz und Informationssicherheit geschult.
- Verarbeitungen im Auftrag gemäß Art. 28 DSGVO erfolgen auf Grundlage von Auftragsverarbeitungsverträgen i.S.d. Art. 28 Abs. 3 DSGVO.
- Auftragsverarbeitungen erfolgen nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
- Die technischen und organisatorischen Maßnahmen von Auftragnehmern werden geprüft.
- Die Weisungen der Auftraggeber bei Auftragsdatenverarbeitungen werden strikt umgesetzt.

XIII. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Sicherheitsupdates für Betriebssysteme und Software werden über automatische Update-Mechanismen eingespielt. Es wird eine kommerzielle Anti-Malware-Software eingesetzt und automatisch aktualisiert.
- Alle Server sind durch redundante Stromkreise, USV-Anlagen und Dieselgeneratoren gegen Stromausfall gesichert. Server sind mit redundanten Netzteilen ausgestattet.
- Die USV-Anlage filtert vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes.
- Die Datenbestände werden durch regelmäßige Datensicherungen geschützt. Eine Auslagerung an eine andere Geolokation ist beim Produkt „BigBlueButton lern.link-Conference“ nicht möglich.
- Lokale Backups erfolgen auf ein Synology-NAS.
- Professionelle Klimatisierung.
- Brandvorkehrungen und -bekämpfungsanlagen im Rechenzentrum werden nach Stand der Technik eingesetzt. (Argon-Löschanlage und Brandfrüherkennungssystem)
- Der Subunternehmer Contabo hat ein Incident-Response-Management-System implementiert. Dieses beinhaltet ein ausgeklügeltes Schutzsystem, welches u.a. aus einem aktuellen Virenschutzprogramm und einer Firewall besteht. Weiterhin sind für den Fall eines Angriffsversuchs von außerhalb genaue Meldewege und Notfallpläne definiert. Dadurch ist es dem Subunternehmer möglich, Angriffe bereits im Anfangsstadium zu identifizieren und umgehend Bekämpfungsmaßnahmen einzuleiten.
- Der Subunternehmer Hetzner hat ein Incident-Response-Management-System implementiert und für sämtliche, internen Systeme eine Eskalationskette definiert, um im Fehlerfall die passenden Stellen schnellstmöglich zu informieren, so dass das System umgehend wieder vollumfänglich hergestellt werden kann. Hetzner hat ein Back-up und Recovery-Konzept mit täglicher Datensicherung, wie auch einer Festplattenspiegelung, implementiert. Weiterhin sind eine Softwarefirewall und Portreglementierungen im Einsatz, ebenso ein ständig aktiver DDoS-Schutz.

XIV. Trennbarkeit

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Zu unterschiedlichen Zwecken erhobene Daten und Daten unterschiedlicher Auftraggeber werden grundsätzlich durch logische Zugriffskontrolle getrennt aufbewahrt und verarbeitet, insbesondere auch im Rahmen des zuvor beschriebenen Berechtigungskonzepts.
- Zu Testzwecken werden ausschließlich anonymisierte Daten verwendet, die sich nicht aus personenbezogenen Daten von Nutzern ergeben.