Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen dem/der

….

– Verantwortlicher – nachstehend Auftraggeber genannt –

und der

Köln-Bonner Akademie GmbH & Co. KG Robert-Bosch-Str. 4 50354 Hürth

– Auftragsverarbeiter – nachstehend Auftragnehmer genannt –

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand
Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag vom ....., auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind das die Bereitstellung (incl. Hosting), Konfiguration und Support von EASYWIZE LMS zur Durchführung von E-Learnings oder anderer Unterweisungen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- r Personenstammdaten (i.w. Namen, Adresse)
- r Kommunikationsdaten (i.W. Telefon, E-Mail)
- r Lernfortschritt sowie Lernhistorie
- r Planungs- und Steuerungsdaten

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Beschäftigte
- ☐ Kunden
- ☐ Lieferanten
- ☐ Dienstleister
- ☐ Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten (sofern gesetzlich erforderlich), der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
   Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der auf Anlage 2 aufgeführten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
   - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber mindestens 3 Wochen vorab schriftlich oder in Textform anzeigt und
   - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
   - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen 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.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;, 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).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Sonstiges

(1) Die Haftung der Parteien richtet sich nach Art. 82 DS-GVO.

(2) Es gilt deutsches Recht.

(3) Ausschließlicher Gerichtsstand ist das Gericht am Geschäftssitz des Auftraggebers.

(4) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(5) Im Falle eines Widerspruchs zwischen dieser Vereinbarung und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, hat diese Vereinbarung Vorrang.

(6) Änderungen und Ergänzungen dieser Vereinbarungen und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers- bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(7) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. 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 DS-GVO liegen.

_____, den __.__.____ _____, den __.__.____

_____ _____

Unterschrift Auftraggeber Unterschrift Auftragnehmer

Anlage 1 – Technisch-organisatorische Maßnahmen

Der Auftragnehmer 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.

I. Zugangskontrolle

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

a) Rechenzentrum:

- Für den Betrieb des Rechenzentrums wurde ein renommierter Anbieter ausgewählt, der über ein dokumentiertes Informationssicherheitsmanagementsystem verfügt.

- Die eingerichteten technischen und organisatorischen Maßnahmen des externen Rechenzentrumbetreibers 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 des Auftragnehmers 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 ausgegeben 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-Roms, 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.

• Beim Zugang zu EASYWIZE LMS müssen Benutzerpasswörter 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 ein 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.

• Beim Zugang zu EASYWIZE LMS müssen Benutzerpasswörter 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 des AN werden schriftlich auf das Datengeheimnis verpflichtet.

• Alle Mitarbeiter des AN werden schriftlich auf das Fernmeldegeheimnis im Sinne des § 88 TKG verpflichtet.

• Die Mitarbeiter werden regelmäßig zu den Themen Datenschutz und Informationssicherheit sensibilisiert.

• 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 aus- schließlich 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 den AN.
- 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 zu- ständig 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 auf- bewahrt, zu dem nur die Leitungsebene des AN Zutritt hat.

• Die Vernichtung von Datenträgern erfolgt stets bei einem qualifizierten, externen Dienstleister, in dessen Räumlichkeiten.

• Beim Hoster 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 in EASYWIZE LMS 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 ein 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 Ein- gaben 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 auf- bewahrt, 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 wieder hergestellt werden können.

• Es werden regelmäßige Backups erstellt.

• Die Datenbestände werden durch regelmäßige Datensicherungen geschützt und bei Bedarf an eine andere Geolokation, stets in der Bundesrepublik Deutschland, ausgelagert.

• 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 auf- tretende 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 und bei Bedarf an eine andere Geolokation, stets in der Bundesrepublik Deutschland, ausgelagert.

• Lokale Backups erfolgen auf ein Synology-NAS.

• Professionelle Klimatisierung.

• Der Hoster 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. Der Hoster 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 und bei Bedarf an eine andere Geolokation, stets in der Bundesrepublik Deutschland, ausgelagert.

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 regelmäßig zu den Themen Datenschutz und Informationssicherheit sensibilisiert.
- 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 und bei Bedarf an eine andere Geolokation, stets in der Bundesrepublik Deutschland, ausgelagert.
- Lokale Backups erfolgen auf ein Synology-NAS.
- Professionelle Klimatisierung.
- Brandvorkehrungen und -bekämpfungsanlagen im Rechenzentrum werden nach Stand der Technik eingesetzt. (Argon-Löschanlage und Brandfrüherkennungssystem)

XIV. Auftragsverarbeitungsvertrag

• Der Hoster 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. Der Hoster 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 wer- den:

• 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.

Anlage 2 – zum Zeitpunkt des Vertragsabschlusses eingesetzte Unterauftragnehmer

lern.link GmbH

Kirchstraße 4

82211 Herrsching

Hosting und Bereitstellung des LMS