

## Vertrag

zwischen

**Schule/Einrichtung**

Adresse

Adresse

– **Verantwortlicher**, nachstehend „**Auftraggeber**“ genannt –

und

**aula gGmbH**

Alte Schönhauser Straße 23/24

10119 Berlin

– **Auftragsverarbeiter**, nachstehend „**Auftragnehmer**“ genannt –

– Zusammen die „**Parteien**“ –

## 1. Gegenstand und Dauer des Vertrags

### 1) Gegenstand

Der Gegenstand des Vertrags ergibt sich aus dem Nutzungs- und Servicevertrag zwischen Auftraggeber und Auftragnehmer vom **TT.MM.JJJJ**, auf den hier verwiesen wird (nachstehend „Leistungsvereinbarung“).

### 2) Dauer

Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

Der Vertrag gilt unbeschadet des Vorstehenden jedoch so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich eine andere Regelung.

## 2. Konkretisierung des Vertragsinhalts

### 1) Zweck der vorgesehenen Verarbeitung von Daten

Der Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer sind in der Leistungsvereinbarung konkret beschrieben.

### 2) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen alle Nutzer der durch den Auftragnehmer bereitgestellten Dienste:

- Personal
- Schüler\*innen / Teilnehmende

### 3) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind die Folgenden:

- Name
- Vorname
- Klasse
- Schule
- E-Mail-Adresse
- Benutzername
- Logdateien
- Beiträge

## 3. Technische und organisatorische Maßnahmen

- 1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur

Prüfung (**Anlage**). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

- 2) Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, soll versucht werden, diesen einvernehmlich umzusetzen.
- 3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber zeitnah in Kenntnis zu setzen.

### 4. Betroffenenrechte

Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beaufschaffen, portieren, 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.

### 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

- 1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung der folgenden Vorgaben.
  - a) Der Auftragnehmer wird die Wahrung der Vertraulichkeit gemäß Art. 28 III 2 lit. b), 29, 32 IV DS-GVO gewährleisten. Er 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. Die Verpflichtung zur Vertraulichkeit gilt auch nach Beendigung der Leistungsvereinbarung und dieser Vereinbarung. Der Auftragnehmer und alle dem Auftragnehmer unterstellten Personen 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.
  - b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
  - c) Im Falle von Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde hat der Auftragnehmer den Auftraggeber unverzüglich hierüber zu informieren, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde

im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten beim Auftragnehmer ermittelt. Es gilt jedoch nicht, sofern dem Auftragnehmer eine solche Mitteilung durch die zuständigen Behörden untersagt wird.

- d)** Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- e)** 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.
- f)** Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten nachkommen kann, insbesondere jenen nach Art. 33, 34 DS-GVO. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
- g)** Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zu Verfügung.
- h)** Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.
- 2)** Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

## **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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post- / Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

- 2) Der Auftraggeber stimmt der Beauftragung der auf <https://www.aula.de/unterauftragsverhaeltnisse/> bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 II – IV DS-GVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel der bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten soll, vorab schriftlich oder in Textform anzeigt; und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 II – IV 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. Die Einhaltung und Umsetzung der technischen und organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vor der Verarbeitung personenbezogener Daten kontrolliert. Der Auftragnehmer versucht, vertraglich sicher zu stellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

- 4) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

- 5) In jeglichem Schadensfall haftet der Auftragnehmer gegenüber dem Auftraggeber für das Verschulden der eingesetzten Unterauftragnehmer wie für eigenes Verschulden.

## 7. Internationale Datentransfers

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich innerhalb der EU / des EWR statt.

## 8. 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 während der üblichen Geschäftszeiten zu überzeugen.

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

## **9. Weisungsbefugnis des Auftraggebers**

- 1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn, er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. 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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## **10. Rückgabe und Löschung personenbezogener Daten**

- 1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangte Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung sicherheitskonform zu vernichten sind; diese Vernichtung ist dem Auftraggeber nachzuweisen.
- 2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

## **11. Benachrichtigungspflichten, Haftung, Schriftform, Ausschluss des Zurückbehaltungsrechtes, Verhältnis zur Leistungsvereinbarung, salvatorische Klausel, Rechtswahl und Gerichtsstand**

- 1) In dem Fall, dass die personenbezogenen Daten Gegenstand einer Durchsuchung, Pfändung oder Beschlagnahme während einer Insolvenz oder aus anderem Anlass

oder aufgrund der Maßnahmen Dritter werden, während sie sich im Verfügungsbereich des Auftragnehmers befinden, ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer ist ferner verpflichtet, alle befugten Personen in diesen Verfahren darüber zu informieren, dass es sich bei den betroffenen personenbezogenen Daten um Daten des Auftraggebers handelt, für die der Auftraggeber der Verantwortliche ist.

- 2) Hinsichtlich der Haftung wird auf Art. 82 DS-GVO verwiesen.
- 3) Alle Änderungen dieser Vereinbarung bedürfen der Schriftform. Das gilt auch für die Aufhebung dieses Schriftformerfordernisses.
- 4) Die Einrede des Zurückbehaltungsrechtes gemäß § 273 BGB an den personenbezogenen Daten des Auftraggebers durch den Auftragnehmer wird ausgeschlossen.
- 5) Diese Vereinbarung regelt die Mindestanforderungen an die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers. Insoweit gehen im Fall abweichender Regelungen die Regelungen dieser Vereinbarung den Regelungen der Leistungsvereinbarung vor. Strengere Pflichten für den Auftragnehmer in Bezug auf die Verarbeitung personenbezogener Daten aus der Leistungsvereinbarung lässt sie unberührt.
- 6) Für den Fall, dass einzelne Regelungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sind oder werden, oder für den Fall, dass diese Vereinbarung unbeabsichtigte Lücken enthält, wird dadurch nicht die Wirksamkeit der übrigen Regelungen berührt. Anstelle der unwirksamen, undurchführbaren oder fehlenden Regelungen werden die Parteien wirksame und durchführbare Regelungen vereinbaren, wie sie sie unter Berücksichtigung des wirtschaftlichen Zwecks dieser Vereinbarung vereinbart hätten, wenn ihnen beim Abschluss dieser Vereinbarung die Unwirksamkeit, Undurchführbarkeit oder das Fehlen der betreffenden Regelungen bewusst gewesen wäre.
- 7) Rechtsstreitigkeiten in Zusammenhang mit Vereinbarung unterliegen dem Recht der Bundesrepublik Deutschland. Gerichtsstandort ist Berlin.

**Für den Auftraggeber**

---

Ort, Datum

---

Unterschrift

**Für den Auftragnehmer**

---

Ort, Datum



---

Alexa Schaefer, aula gGmbH

## Anlage – Technische und organisatorische Maßnahmen zur Datensicherheit gemäß Art. 32 DS-GVO

### Präambel

Die technischen und organisatorischen Maßnahmen zur Datensicherheit der aula gGmbH wurden unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechten und Freiheiten natürlicher Personen getroffen. Es ist der aula gGmbH als Auftragnehmer, stets auch während eines laufenden Vertragsverhältnisses, gestattet, alternative Maßnahmen umzusetzen, sofern diese einen adäquaten Schutz darstellen und das hier beschriebene Sicherheitsniveau nicht unterschreiten. Änderungen der Maßnahmen werden stets dokumentiert.

### § 1 Zutrittskontrolle

Die Zutrittskontrolle regelt die Annäherung und den physischen Zutritt zu Bereichen, in denen sich Systeme befinden und Prozesse ausgeführt werden, mit deren Hilfe personenbezogene Daten verarbeitet werden. Ein unbefugter Zutritt zu solchen Bereichen ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Die Zutrittskontrolle wird durch folgende Maßnahmen gewährleistet:

- 1) Alle Stellen, in denen personenbezogene Daten verarbeitet werden, werden durch ein geeignetes Zutrittskontrollsystem geschützt (Schlüssel, Zahlenschlösser, Kartenlesesystem).
- 2) Die befugten Personen sind festgelegt und mit den entsprechenden Zutrittsmitteln wie Schlüssel und / oder Chipkarten ausgestattet. Die Vergabe von Zutrittsberechtigungen wird dokumentiert. Die Verwaltung der Schlüssel erfolgt durch die Mitarbeiter der Büroleitung.
- 3) Alle Zutrittsrechte werden restriktiv vergeben, dokumentiert und vor Manipulationen geschützt. Dies beinhaltet auch eine regelmäßige Überprüfung der Berechtigungen bezüglich der Aktualität und Notwendigkeit. Nicht mehr benötigte Berechtigungen werden unverzüglich entzogen.

- 4) Veränderungen oder Löschungen von Zutrittsberechtigungen auf Grund des Wechsels oder Ausscheidens eines Mitarbeiters werden sofort umgesetzt und dokumentiert.
- 5) Gäste müssen während ihres Besuchs in den Geschäftsräumen von einem Mitarbeiter der aula gGmbH begleitet werden.
- 6) Türen und Fenster sind außerhalb der Betriebszeiten fest verschlossen.

### § 2 Zugangskontrolle

Die Zugangskontrolle verfolgt das Ziel, Unbefugten den Zugang zu IT-Systemen zu verwehren. Sie bildet die zweite Sicherheitsebene nach der Zutrittskontrolle und regelt damit die Möglichkeit des Einwirkens auf die Datenverarbeitung im IT-System selbst. Das Eindringen Unbefugter in IT-Systeme ist zu verhindern. Die Zugangskontrolle wird durch folgende Maßnahmen gewährleistet:

- 1) Im Rahmen der Auftragsbearbeitung werden technische (Kennwort- / Passwortschutz) und organisatorische (Berechtigungskonzept) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung getroffen.

### § 3 Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung Berechtigten nur auf die ihrer jeweiligen Berechtigung unterliegenden Daten zugreifen können („Need-to-Know-Prinzip“). Sie bildet die dritte Sicherheitsebene. Unerlaubte Tätigkeiten in Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern. Die Zugriffskontrolle wird durch folgende Maßnahmen gewährleistet:

- 1) Es liegt eine IT-Sicherheitsrichtlinie vor.
- 2) Veränderungen oder Löschungen von Zugriffsberechtigungen auf Grund des Wechsels oder Ausscheidens eines Mitarbeiters werden sofort umgesetzt und dokumentiert.

- 3) Es wird geprüft, wann personenbezogene Daten ohne Beeinträchtigung gesetzlicher, vertraglicher oder interner Interessen vernichtet werden können. Hierbei werden die Maximal-Aufbewahrungsfristen, sofern vorhanden, der Entscheidung zugrunde gelegt. Sobald kein Erfordernis zur Aufbewahrung vorliegt, werden die Daten unabhängig von ihrer Form (digital / Papier) vernichtet. Entsprechend der zu löschenden Daten und deren Schutzbedarf wird eine geeignete Löschmethode gewählt:

- a) Löschkommandos
- b) Formatierung
- c) Überschreiben
- d) Zerstörung

## § 4 Weitergabekontrolle

Durch die Weitergabekontrolle soll sichergestellt werden, dass personenbezogene Daten während einer elektronischen Übertragung, eines Transports oder der Speicherung auf mobilen Datenträgern nicht unberechtigt eingesehen, kopiert, verändert oder gelöscht werden können. Die Weitergabekontrolle wird durch folgende Maßnahmen gewährleistet:

- 1) Im Rahmen der Sachbearbeitung werden Maßnahmen für den Transport, die Übertragung und Übermittlung oder die Speicherung auf Datenträgern getroffen (z.B. mittels Passwortschutz).
- 2) Alle Datenübertragungen werden durch das Personal des Auftraggebers initiiert oder werden diesem durch den Auftragnehmer ersichtlich gemacht. Der Auftraggeber kann jederzeit der Datenübertragung widersprechen. Daten, die zum Transfer vom Auftraggeber zum Auftragnehmer auf ein Transportmedium zwischengespeichert werden müssen, werden nach der Übertragung unverzüglich und unwiderruflich von diesem Medium gelöscht, sofern keine anderweitigen Aufbewahrungspflichten bestehen.
- 3) Nicht mehr benötigte Datenträger werden datenschutz-konform und BSI-konform vernichtet.
- 4) Ein Datenaustausch über das Internet oder per E-Mail kann bei Bedarf mittels einer verschlüsselten Verbindung (z. B. https) erfolgen.

## § 5 Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachvollziehbar protokolliert wird, welcher Nutzer einer Anwendung oder eines Systems personenbezogene Daten verarbeitet hat. Ein weiteres Ziel der Eingabekontrolle ist die Nachvollziehbarkeit von Fehleingaben. Diese Nachvollziehbarkeit beziehungsweise Dokumentation der Datenverwaltung und Pflege wird durch folgende Maßnahmen gewährleistet:

- 1) Bezüglich Daten, die zur Leistungserbringung im Rahmen der Auftragsverarbeitung eingegeben, verändert oder gelöscht werden, erfolgt eine Protokollierung der einzelnen Zugriffe.
- 2) Der Auftragnehmer protokolliert wesentliche Veränderungen an Daten in Systemen des Auftraggebers und macht diese über Auswertungen nachvollziehbar.
- 3) Protokolldaten werden nicht nachträglich verändert.
- 4) Ein Zugriff auf Protokolldaten erfolgt nur durch autorisierte Nutzer mit gesonderten Zugriffsrechten.

## § 6 Auftragskontrolle

Die Auftragskontrolle gewährleistet, dass personenbezogene Daten im Rahmen einer Auftragsverarbeitung nur nach den Weisungen des Auftraggebers durch den Auftragnehmer verarbeitet werden. Die Auftragskontrolle wird durch folgende Maßnahmen gewährleistet:

- 1) Die weisungsgemäße Auftragsverarbeitung wird vertraglich abgesichert, etwa durch einen Vertrag gemäß Art. 28 DS-GVO. Die darin enthaltenen Bestimmungen werden durch die Fachabteilungen geprüft und sichergestellt.
- 2) Alle für die Auftragsverarbeitung relevanten Punkte sind im Leistungsvertrag (Hauptvertrag) sowie dessen Anlagen konkretisiert.

## § 7 Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle beinhaltet Maßnahmen zum Schutz von personenbezogenen Daten vor einem zufälligen Verlust oder einer Zerstörung (etwa durch Wasserschäden, Brand, Blitzschlag oder Stromausfall). Die Verfügbarkeitskontrolle wird durch folgende Maßnahmen gewährleistet:

- 1) Im Rahmen der Auftragsverarbeitung werden physikalische und logische Maßnahmen zur Datensicherung getroffen. Alle für die Leistungserbringung notwendigen Daten werden durch ein geeignetes Backup-Verfahren vor Verlust und Zerstörung gesichert.
- 2) Jegliche eingesetzte Software wird einmal voll gesichert, entweder mittels der Originaldatenträger oder als selbst erstellte Kopie.
- 3) Die eingesetzten Mitarbeiter sind vertraglich zur Datensicherung verpflichtet.
- 4) Anwendungsdaten werden auf zentralen Servern, die vom Backupkonzept abgedeckt sind, abgelegt. In Fällen, in denen der Mitarbeiter keinen Netzzugang hat, muss der Mitarbeiter die Datensicherung selbst vornehmen.
- 5) Im Rahmen eines Disaster-Recovery-Plans werden alle Datensicherungen bezüglich der Wiederherstellung regelmäßig getestet.
- 7) Die für die Leistungserbringung relevanten Server liegen bei der Hetzner Online GmbH und sind dort durch deren technische und organisatorische Maßnahmen zusätzlich geschützt. Zu finden unter <https://docs.hetzner.com/de/general/others/technical-and-organizational-measures/>

### § 8 Trennungsgebot

Das Trennungsgebot regelt (technisch und organisatorisch) die getrennte Verarbeitung von personenbezogenen Daten je nach dem Zweck ihrer Erhebung. Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten. Das Trennungsgebot wird durch folgende Maßnahmen gewährleistet:

- 1) Die Systeme der aula gGmbH bilden eine interne Mandantenfähigkeit ab. Daten von Auftraggebern werden logisch von Daten anderer Auftraggeber getrennt. Diese Trennung wird zum einen durch entsprechende Berechtigungen realisiert, zum anderen durch physikalisch getrennte Speichermedien oder Dateiseparierung.
- 2) Bei der Durchführung von vertraglichen und rein internen Leistungen erfolgt eine Funktionstrennung von Test- und Produktivdaten.
- 3) Zur Durchführung von Tests werden die Daten, soweit technisch möglich und zumutbar, zuvor pseudonymisiert oder anonymisiert.

### § 9 Organisationskontrolle

Über die technischen Maßnahmen hinaus ist die innerbetriebliche Organisation bei der aula gGmbH durch folgende Maßnahmen so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes und allgemeiner Compliance gerecht wird:

- 1) Anfallende Aufgaben werden funktional verteilt und synergetisch bearbeitet. Es gibt den Datenschutzbeauftragten und den (Informations-) Sicherheitsbeauftragten.
- 2) Für Außenkontakt zuständige Gremien oder Funktionen verfügen über ein Funktionspostfach, um die personenunabhängige Erreichbarkeit zu gewährleisten.
- 3) Sämtliche Mitarbeiter werden zur Wahrung der Vertraulichkeit hinsichtlich personenbezogener Daten und Geschäftsgeheimnisse verpflichtet.
- 4) Das datenschutzrechtliche Fundament wird über interne Richtlinien vorgegeben, etwa über die allgemeine Datenschutzrichtlinie oder die Richtlinie zum Umgang mit Datenschutzverletzungen.
- 5) Die Informationssicherheit wird über entsprechende Richtlinien gewährleistet.
- 6) Sämtliche Mitarbeiter werden in regelmäßigen Abständen über die Anforderungen des Datenschutzes und der Informationssicherheit unterwiesen – auch der Umgang mit Verschlusssachen ist Teil der Schulungen.
- 7) Schriftliche Arbeitsanweisungen und Merkblätter liegen vor. Diese werden regelmäßig an alle Mitarbeiter versendet und sind im Intranet einsehbar.
- 8) Bei der Auswahl von Mitarbeitenden, insbesondere in datenschutzrelevanten Tätigkeitsbereichen, wird auf fachliche Eignung, Zuverlässigkeit und Verantwortungsbewusstsein geachtet.