Vereinbarung zur Auftragsverarbeitung (AVV)

gemäß Art 28 DSGVO

Die Republik Österreich, vertreten durch das Bundesministerium für Bildung (BMB)
Minoritenplatz 5
1010 Wien, Österreich

als Betreiber des Bildungsportals und des Marktplatz Lernapps,
nachfolgend als „Auftraggeber“ oder „Verantwortlicher“ bezeichnet

und

<Name des Unternehmens (Firma)>
<Firmenbuchnummer, sofern vorhanden>
<Anschrift>
<Land>

als Anbieter von Lernapps bzw. Bildungsangeboten im Marktplatz Lernapps,

nachfolgend als „Auftragnehmer“ oder „Auftragsverarbeiter“ bezeichnet

schließen die folgende Vereinbarung zur Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter (nachfolgend Auftragsverarbeitervereinbarung, kurz „AVV“):

Der Auftragnehmer erbringt als Auftragsverarbeiter Leistungen für den Auftraggeber, welche in den jeweiligen Hauptverträgen (Partnerschaftsvertrag Marktplatz Lernapps samt Anlagen) detailliert beschrieben sind.

Die vorliegende Vereinbarung stellt die vertragliche Basis für die Auftragsverarbeitung gemäß Artikel 28 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung - DSGVO) dar und regelt die Rechte und Pflichten der Vertragsparteien im Hinblick auf eine datenschutzkonforme Auftragsverarbeitung.

Die vorliegende Vereinbarung konkretisiert somit den zwischen dem Auftraggeber (als Verantwortlichen nach Artikel 4 Abs. 7 DSGVO) und dem Auftragnehmer

(als Auftragsverarbeiter nach Artikel 4 Abs. 8 DSGVO) abgeschlossenen „Hauptvertrag“ bezüglich der Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

Die Kategorien der von der Datenverarbeitung betroffenen Personen, sowie Art, Umfang und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag. Im Zuge der Leistungserbringung durch den Auftragnehmer unter dem Hauptvertrag verpflichtet sich der Auftragnehmer die folgenden datenschutzrechtlichen und datensicherheitstechnischen Bestimmungen einzuhalten:

1. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er bei der Verarbeitung personenbezogener Daten **alle anwendbaren Datenschutz- und Datensicherheitsbestimmungen**, insbesondere jedoch nicht abschließend die Datenschutz-Grundverordnung (DSGVO) und das österreichische Datenschutzgesetz (DSG) einhält.
2. Bei Vorliegen der Voraussetzungen des Artikels 37 DSGVO ist der Auftragsverarbeiter (zumindest) für die Laufzeit dieser Vereinbarung verpflichtet, einen Datenschutzbeauftragten zu bestellen. Der Auftragsverarbeiter hat insbesondere sicherzustellen, dass der **Datenschutzbeauftragte** an allen Angelegenheiten, die den Datenschutz betreffen, ordnungsgemäß und frühzeitig beteiligt ist und dieser seinen Aufgaben gemäß Artikel 39 nachkommen kann. Der Auftragsverarbeiter teilt dem Auftraggeber die nach Artikel 37 Abs. 7 DSGVO veröffentlichten Kontaktdaten des Datenschutzbeauftragten sowie den Link zur Veröffentlichung mit.
3. Der Auftragsverarbeiter führt ein **Verzeichnis aller Verarbeitungstätigkeiten für den Auftraggeber** gemäß Artikel 30 Abs. 2 DSGVO. Der Auftraggeber stellt dem Auftragsverarbeiter auf Anfrage für diesen Zweck die relevanten Auszüge aus seinem Verzeichnis von Verarbeitungstätigkeiten in geeigneter digitaler und möglichst weiterverarbeitbarer Form (z. B. Excel-Format) zur Verfügung. Der Auftragsverarbeiter stellt sein Verzeichnis von Verarbeitungstätigkeiten auf Anfrage der Aufsichtsbehörde (Artikel 30 Abs. 4 DSGVO) sowie die für gegenständliche Verarbeitungen relevanten Auszüge dem Auftraggeber zur Verfügung.
4. Pflichten, die sich nicht bereits aus gesetzlichen Bestimmungen oder dem Hauptvertrag ergeben, hat der Auftraggeber durch gesonderte **„Weisungen zur Datenverarbeitung“ in Anlage 2** auszudrücken, welche vom Auftragsverarbeiter einzuhalten sind. Der Auftraggeber kann alle für die rechtskonforme Verarbeitung notwendigen Weisungen jederzeit durch eine entsprechende Mitteilung ändern oder ersetzen. Falls der Auftraggeber mündlich spezifische Weisungen zur Datenverarbeitung erteilt, müssen diese anschließend in Textform (z.B. per E-Mail) bestätigt werden.

5. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person dürfen Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der **dokumentierten Aufträge und Weisungen** des Auftraggebers verarbeiten und übermitteln, außer es liegt ein Ausnahmefall gemäß Artikel 28 Abs. 3 lit a DSGVO (gesetzliche Verpflichtung des Auftragsverarbeiters) vor. Im letzteren Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt (Artikel 28 Abs. 3 letzter Satz DSGVO).

6. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er **alle mit der Datenverarbeitung beauftragten Personen** vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne des Artikels 28 Abs. 3 lit. b DSGVO und § 6 DSG **nachweislich verpflichtet** hat und diese auf die strafrechtlichen Konsequenzen eines Verstoßes hingewiesen worden sind. Kopien dieser Verpflichtungserklärungen sind auf formloses Ersuchen unverzüglich dem Auftraggeber zu übermitteln. Insbesondere bleibt die **Verschwiegenheitsverpflichtung des Auftragsverarbeiters und der mit der Datenverarbeitung beauftragten Personen** auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht. Der Auftragsverarbeiter ist zudem verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäfts- und Betriebsgeheimnissen sowie Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

7. **Alle dem Auftragsverarbeiter unterstellten Personen**, die mit der Verarbeitung personenbezogener Daten im Verantwortungsbereich des Auftraggebers betraut sind, müssen im Hinblick auf Datenschutz, Datensicherheit und Vertraulichkeit angemessen geschult sein. Der Auftragsverarbeiter hat die erforderlichen Schritte zu unternehmen, um sicherzustellen, dass die ihm unterstellten Personen, die Zugang zu personenbezogenen Daten haben, diese nur gemäß den Weisungen des Auftraggebers verarbeiten, es sei denn, sie sind nach gesetzlichen Normen zur Verarbeitung verpflichtet (Artikel 32 Abs. 4 DSGVO).

8. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er **ausreichende technische und organisatorische Maßnahmen im Sinne der DSGVO, insbesondere nach Art 24, 25 und 32 DSGVO** ergriffen hat, um ein dem Risiko angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten zu erreichen und um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden. Der Auftragsverarbeiter verpflichtet sich, Maßnahmen im Sinne des Datenschutzes durch Technikgestaltung und datenschutzrechtliche Voreinstellungen zu treffen. Zum Beleg der Einhaltung von technischen und organisatorischen Maßnahmen können vorhandene, gültige Zertifizierungen nach ISO 27000, ISO 29134, BSI-Grundschutz, CNIL oder ähnliche dienen, die dem Auftraggeber vor Unterzeichnung der vorliegenden Vereinbarung

vorzulegen und welche als Anlage der Vereinbarung anzuschließen sind. Bei Fehlen entsprechender Zertifikate und Testate sind ausführliche Dokumentationen der getroffenen technischen und organisatorischen Maßnahmen vorzulegen und als Anlage dieser Vereinbarung anzuschließen, welche die Einhaltung eines dem Risiko angemessenen Schutzniveaus belegen. Der Auftragsverarbeiter unterstützt den Auftraggeber bei der regelmäßigen Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung, sowie bei der Beurteilung des angemessenen Schutzniveaus für die vom Auftragsnehmer verarbeiteten Daten.

9. Der Auftragsverarbeiter ist im Hinblick auf seine IT-Systeme zur Einhaltung angemessener Sicherheitsstandards nach dem jeweils aktuellen Stand der Technik (etwa laut BSI - Grundschutz, Österreichischem Informationssicherheitshandbuch oder ähnlichen) verpflichtet. So die Daten nicht auf der vom Auftraggeber bereitgestellten Server-Infrastruktur gehostet werden, ist nachzuweisen, dass die für den Betrieb herangezogenen Server-infrastruktur jedenfalls eine gültige Zertifizierung nach ISO 27001 oder gleichwertig besitzen.

10. Der Auftragsverarbeiter verpflichtet sich, bei der **elektronischen Übermittlung** von Daten technische Verfahren mit Authentifikation und Verschlüsselung nach den üblichen Sicherheitsstandards unter besonderer Berücksichtigung der Vorgaben nach Artikel 32 DSGVO anzuwenden. Der Auftragsverarbeiter darf ein anderes Unternehmen als weiteren Auftragsverarbeiter (**„Sub-Auftragsverarbeiter“**) nach Artikel 4 Abs. 8 DSGVO heranziehen, wenn der Auftraggeber dem schriftlich zustimmt (Artikel 28 Abs. 2 DSGVO).

    Im Falle einer Heranziehung eines weiteren Sub-Auftragsverarbeiters durch den Auftragsverarbeiter ohne erfolgte schriftliche Zustimmung des Auftraggebers behält sich der Auftraggeber das Recht vor, den Hauptvertrag binnen angemessener Frist außerordentlich zu kündigen. Der Auftragsverarbeiter muss mit dem Sub-Auftragsverarbeiter einen Vertrag im Sinne des Artikel 28 Abs. 4 DSGVO abschließen. In diesem Vertrag hat der Auftragsverarbeiter sicherzustellen, dass der Sub-Auftragsverarbeiter nachweislich dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund der DSGVO, dem DSG sowie dieser Vereinbarung und der zugrunde liegenden Beauftragung obliegen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Bestimmungen erfolgt. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters (Artikel 28 Abs. 4 letzter Satz DSGVO).

11. Der Auftragsverarbeiter hat dem Auftraggeber unverzüglich alle erforderlichen Informationen zum Nachweis der Einhaltung seiner rechtlichen (insbesondere gem. DSGVO und DSG) und vertraglichen Pflichten zur Verfügung zu stellen. Der Auftragsverarbeiter trägt insbesondere für die technischen und organisatorischen Voraussetzungen Vorsorge, dass der Auftraggeber die **Rechte betroffener Personen gemäß Artikel 12 bis 23 DSGVO** (Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung etc.) gegenüber den betroffenen Personen innerhalb der gesetzlichen Fristen rechtskonform erfüllen kann. Für den Fall, dass sich eine betroffene Person direkt an den Auftragsverarbeiter zwecks Geltendmachung seiner Rechte wendet, hat der Auftragsverarbeiter ihr Begehren unverzüglich an den Datenschutzbeauftragten des Auftraggebers unter datenschutz@bmb.gv.at schriftlich weiterzuleiten. Dem Auftragsverarbeiter ist es untersagt, der betroffenen Person nähere Informationen über die Datenverarbeitung des Auftraggebers zu erteilen, ausgenommen davon ist die Nennung des Namens und der Kontaktdaten des Auftraggebers.

12. Sollte für die Auftragsverarbeitung eine **Datenschutz-Folgenabschätzung (DSFA)** nach Artikel 35 DSGVO nötig sein, verpflichtet sich der Auftragsverarbeiter dem Auftraggeber alle für die Erstellung der DSFA erforderlichen Informationen zeitgerecht zur Verfügung zu stellen. Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber bei der Einhaltung der übrigen in den Artikel 32, 33, 34 und 36 DSGVO genannten Pflichten zu unterstützen und dem Auftraggeber dafür alle erforderlichen Informationen unverzüglich zu übermitteln.

13. Soweit vorliegend, übermittelt der Auftragsverarbeiter dem Auftraggeber vor Beginn der Verarbeitungstätigkeit alle Nachweise über eingehaltene **Verhaltensregeln nach Artikel 40 DSGVO** sowie erlangte **Zertifikate nach Artikel 42 DSGVO**, welche die beauftragte Verarbeitungstätigkeit betreffen, zur Erstellung der Risikoabschätzung gemäß Artikel 32 Abs. 1 DSGVO.

14. Der Auftragsverarbeiter verpflichtet sich, **Verletzungen des Schutzes personenbezogener Daten** gemäß Artikel 33 oder Artikel 34 DSGVO unverzüglich schriftlich an den Auftraggeber sowie per E-Mail an den Datenschutzbeauftragten des Auftraggebers unter datenschutz@bmb.gv.at zu melden.

15. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz, die Einhaltung der zwischen den Vertragsparteien getroffenen vertraglichen Regelungen sowie die Einhaltung der Weisungen des Auftraggebers durch den Auftragsverarbeiter jederzeit im erforderlichen Umfang zu kontrollieren bzw. durch im Einzelfall zu benennende, sachverständige Dritte (mit oder ohne Beisein des Auftraggebers) kontrollieren zu lassen. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht **zur Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen** nach Artikel 28 Abs. 3 lit. h DSGVO eingeräumt.

Der Auftraggeber kann dazu die Kontrolle in der Betriebsstätte des Auftragsverarbeiters nach angemessener Vorankündigung zu den jeweils üblichen Geschäftszeiten vornehmen bzw. vornehmen lassen. Für die Ermöglichung von Kontrollen durch den Auftraggeber oder einem von ihm benannten Prüfer kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Die Nachweise in Form von Zertifikaten werden dem Auftraggeber kostenlos zur Verfügung gestellt. Eine Vor-Ort-Kontrolle ist grundsätzlich nur nach vorheriger Terminvereinbarung möglich. Die Ermöglichung einer einmaligen Vor-Ort-Kontrolle pro Vertragsjahr, welche die Dauer von 8 h nicht überschreitet, ist mit dem vertraglich vereinbarten Leistungsentgelt bereits abgegolten. Ein darüber hinausgehender Zeitaufwand wird dem Auftraggeber mit einem angemessenen Verrechnungssatz in Rechnung gestellt. Dies gilt nicht für Kontrollen, die der Auftraggeber aufgrund eines Verstoßes des Auftragnehmers durchführen muss. Der Auftragnehmer ist berechtigt, die Zustimmung zur Durchführung der Prüfung davon abhängig zu machen, dass sachverständige Dritte (Prüfer) eine angemessene Verschwiegenheitserklärung unterzeichnet. Sollte der vom Verantwortlichen beauftragte sachverständige Dritte in einem Wettbewerbsverhältnis zum Auftragnehmer stehen oder ein anderer berechtigter Grund vorliegen, steht dem Auftragnehmer ein Einspruchsrecht gegen diesen zu.

Solange der Auftragnehmer den Nachweis über die Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere die Umsetzung der technisch organisatorischen Maßnahmen sowie ihrer Wirksamkeit durch geeignete Nachweise erbringt, kann dieser eine anlasslose Vor-Ort-Prüfung diesbezüglich ablehnen. Geeignete Nachweise können insbesondere genehmigte Verhaltensregeln gemäß Artikel 40 DSGVO, ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 DSGVO, gegebenenfalls die Vorlage von Testaten oder Berichten unabhängiger Instanzen, schlüssiger Datensicherheitskonzepte oder geeigneter Zertifizierungen durch IT-Sicherheits- und Datenschutzaudits sein.

16. Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber unverzüglich von jedem **Verstoß des Auftragsverarbeiters, seiner betrauten Mitarbeiter oder Dritter** gegen anwendbare Datenschutzvorschriften oder in dieser Vereinbarung getroffene Pflichten und Weisungen in Kenntnis zu setzen. Der Auftragsverarbeiter trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

17. Der Auftragsverarbeiter ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber gemäß Artikel 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen **Auskünfte an den Auftraggeber** zu erteilen und der jeweils zuständigen **Aufsichtsbehörde eine Vor-Ort-Kontrolle** zu

ermöglichen. Der Auftraggeber ist über entsprechende (geplante) Maßnahmen vom Auftragsverarbeiter zu informieren.

18. Der Auftragsverarbeiter verpflichtet sich, die Datenverarbeitung im Auftrag **ausschließlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR)** durchzuführen. Jedwede, sei es auch nur eine teilweise, Erbringung der Datenverarbeitung in einem Drittland bedarf der vorherigen ausdrücklichen Zustimmung des Auftraggebers. Sofern der Auftraggeber einer Erbringung der Datenverarbeitung in einem Drittland zugestimmt hat, darf diese nur dann erfolgen, wenn alle gesetzlichen und vertraglichen Voraussetzungen nachweislich erfüllt sind.
19. Der Auftragsverarbeiter ist gemäß Artikel 28 Abs. 3 lit. g DSGVO **nach Beendigung der Verarbeitungsleistungen** verpflichtet, nach Wahl des Auftraggebers alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben bzw. in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren oder nach vorheriger Zustimmung des Auftraggebers zu vernichten, sofern nicht nach den gesetzlichen Normen eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht. Eine weitere Aufbewahrung durch den Auftragnehmer erfolgt dabei kostenfrei, sofern der Hauptvertrag nichts Anderes vorsieht. Das Protokoll der Löschung (Vernichtung) ist auf Anforderung dem Auftraggeber unverzüglich vorzulegen. Wenn der Auftragsverarbeiter die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung seiner Verarbeitungsleistungen entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten erhalten hat oder in einem anderen, gängigen Format (für den Auftraggeber kostenfrei) herauszugeben.
20. Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch **Pfändung oder Beschlagnahme**, durch ein **Insolvenz- oder Vergleichsverfahren** oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren.

Schlussbestimmungen

1. Die Vertragsparteien schließen die Anwendung etwaiger im Hauptvertrag enthaltener Haftungsprivilegierungen bzw.- -beschränkungen zugunsten des Auftragsverarbeiters auf datenschutzrechtliche Verstöße ausdrücklich aus.
2. Änderungen und Ergänzungen zu dieser Vereinbarung bedürfen der Schriftform. Gleiches gilt für die Vereinbarung, vom Erfordernis der Schriftform abzugehen. Die dieser Vereinbarung beigefügten Anhänge bilden einen integrierenden Vertragsbestandteil. Diese Vereinbarung unterliegt dem österreichischen Recht unter Ausschluss der Verweisungsnormen des Internationalen Privatrechts sowie dem sachlich anwendbaren Unionsrecht.
3. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und in Zusammenhang mit dieser Vereinbarung ist Wien, Österreich.
4. Sofern es nicht zu einem bloßen Austausch elektronischer Dokumente (z.B. per E-Mail) kommt, so wird diese Vereinbarung in zwei Originalen ausgefertigt, von welchen jede Vertragspartei ein Original erhält.
5. Diese Vereinbarung tritt mit Unterzeichnung in Kraft und gilt für die gesamte Dauer der aufrechten Vertragsbeziehung zur Erbringung der Leistungen gemäß dem Hauptvertrag/der Hauptverträge, sofern sich aus den gesetzlichen Bestimmungen, aus dem Hauptvertrag selbst oder dieser Auftragsverarbeitervereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

Für das Bundesministerium für Bildung als Auftraggeber:	**Für den Auftragnehmer:**
Name:	Name:
Funktion:	Funktion:
Datum:	Datum:
Unterschrift:	Unterschrift:

Die Felder „Name“, „Funktion“ und „Datum“ sind handschriftlich oder elektronisch auszufüllen.

Die Unterschrift kann eigenhändig oder mittels qualifizierter elektronischer Signatur im Sinne der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) erfolgen, etwa im Wege der ID Austria.

ANLAGEN

Anlage 1

Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Die in dieser Anlage enthaltene Kurzanleitung dient dem Auftragsverarbeiter zur eigenständigen Einschätzung des Schutzbedarfs gemäß Artikel 32 DSGVO unter Berücksichtigung der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit.

Die Bewertung erfolgt anhand anerkannter Methoden zur Schutzbedarfsfeststellung wie etwa dem BSI-Standard 200-2 (IT-Grundschutz-Methodik) oder der Vorgaben des Leitfadens der österreichischen Datenschutzbehörde zur Sicherheit der Verarbeitung personenbezogener Daten.

Allgemeine Klassifizierung des Schutzbedarfs:

Gering / kein Schutz erforderlich

- *Auswirkungen bei Eintreten des Schadensfalles sind begrenzt und überschaubar.*

Hoher Schutzbedarf

- *Auswirkungen bei Eintreten des Schadensfalles können beträchtlich sein.*

Sehr hoher Schutzbedarf

- *Auswirkungen bei Eintreten des Schadensfalles können weitreichend und erheblich sein.*

Schutzbedarf nach Auswirkungen:

Im Erwägungsgrund 75 DSGVO werden die folgenden Kategorien zur Einteilung von Schäden festgelegt, die im Zusammenhang mit der Verarbeitung personenbezogener Daten eintreten können:

Physische Schäden
Materielle Schäden
Immaterielle Schäden

Anhand der Tabelle 1 ist der Schutzbedarf für jede Kategorie festzustellen.

Schutzbedarfsklasse	Auswirkung		
	Physisch	Materiell	Immateriell
Kein/Geringer Schutzbedarf	Vernachlässigbar	Vernachlässigbar	Vernachlässigbar
Hoher Schutzbedarf	Eingeschränkt	Eingeschränkt	Eingeschränkt
Sehr hoher Schutzbedarf	Wesentlich und Maximal	Wesentlich und Maximal	Wesentlich und Maximal

Abbildung 1: Tabelle 1 - Unterteilung der Schutzbedarfsklassen nach Auswirkungen

<u>Beispiel:</u>

Physische Auswirkung: Vernachlässigbar

Materielle Auswirkung: Eingeschränkt

Immaterielle Auswirkung: Vernachlässigbar

Ermittelte Schutzbedarfsklasse: Hoher Schutzbedarf

<u>Schutzbedarf für die folgenden Ziele gemäß Art. 32 Abs. 1 lit. b DSGVO:</u>

Vertraulichkeit

Integrität

Verfügbarkeit

Für jedes Schutzziel ist ein Wert (1-3) festzulegen:

Schutzbedarfsklasse	Gesamtwert	Vertraulichkeit	Integrität	Verfügbarkeit
Kein Schutzbedarf	1	1	1	1
Geringer Schutzbedarf	1	1	1	1
Hoher Schutzbedarf	2	2	2	1
Sehr hoher Schutzbedarf	3	3	3	2

1...gering 2...hoch 3...sehr hoch

Abbildung 2: Tabelle 2 – Schutzbedarfsklassen nach Schutzzielen

<u>Beispiel:</u>

Vertraulichkeit: gering

Integrität: hoch

Verfügbarkeit: gering

Ermittelte Schutzbedarfsklasse: Hoher Schutzbedarf

Der gesamte Schutzbedarf ergibt sich aus der oben beschriebenen Schutzbedarfsklasse nach Auswirkungen sowie der Schutzbedarfsklasse nach Schutzzielen.

Der höchste daraus ermittelte Wert ergibt schließlich die erforderliche Schutzbedarfsklasse für personenbezogene Daten im Zusammenhang mit der gegenständlichen Verarbeitungstätigkeit.

1.	**Fähigkeit der Vertraulichkeit** Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet? Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.	☐ Elektronisches Zutrittskontrollsystem ☐ Sicherheitstüren und/oder -fenster ☐ Gitter vor Fenstern und Türen ☐ Werkschutz, Pförtner ☐ Alarmanlage ☐ Videoüberwachung ☐ Spezielle Schutzvorkehrungen für den Serverraum ☐ Individueller Log-In und Kennwortverfahren ☐ Zusätzlicher Log-In für bestimmte Anwendungen ☐ Automatische Sperrung der Clients (Zeitablauf) ☐ Verwaltung von Berechtigungen ☐ Dokumentation von Berechtigungen ☐ Verschlüsselung von Systemen ☐ Verschlüsselung der Kommunikation ☐ Verschlüsselung von Datenträgern ☐ VPN (Virtual Private Network) ☐ Gesichertes WLAN ☐ SSL-Verschlüsselung bei Web-Access ☐ Sonstige:
2.	**Fähigkeit der Integrität** Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet? Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.	☐ Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern ☐ Verwendung von Zugriffsrechten ☐ Systemseitige Protokollierungen ☐ Funktionelle Verantwortlichkeiten ☐ Sonstige:
3.	**Fähigkeit der Verfügbarkeit** Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet? Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.	☐ Back-Up Verfahren ☐ Spiegeln von Festplatten ☐ Unterbrechungsfreie Stromversorgung (USV) ☐ Virenschutz /Firewall ☐ Notfallplan ☐ Klimaanlagen ☐ Brand- und Löschwasserschutz ☐ Alarmanlage ☐ Geeignete Archivierungsräumlichkeiten ☐ Sonstige:

4.	**Fähigkeit der Belastbarkeit** Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet? Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.	☐ Penetrationstests ☐ Lasttests ☐ Sonstige:
5.	**Wiederherstellbarkeit der Verfügbarkeit und des Zugangs** Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?	☐ Back-Up Verfahren ☐ Unterbrechungsfreie Stromversorgung (USV) ☐ Notfallplan ☐ Vertretungsregelungen ☐ Sonstige:
6.	**Pseudonymisierung** Wie wird die Pseudonymisierung der Daten gewährleistet? Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.	☐ Personenbezogene Daten werden durch Zufallscodes ersetzt ☐ Data Masking ☐ Keine Pseudonymisierung ☐ Sonstige:
7.	**Verschlüsselung** Wie wird die Verschlüsselung gewährleistet? Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.	☐ Nutzung von kryptografischen Tools ☐ Data Hashing ☐ Verschlüsselung von Speichermedien ☐ Verschlüsselung der Kommunikation ☐ Keine Verschlüsselung ☐ Sonstige:
8.	**Verfahren zur regelmäßigen Überprüfung** Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?	☐ Es existiert eine festgelegte Prüfroutine ☐ Prüfberichte werden evaluiert ☐ Implementierung von Verbesserungsvorschlägen ☐ Sonstige:

9.	**Unrechtmäßiger Zugang zu personenbezogenen Daten** Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?	☐ Individueller Log-In und Kennwortverfahren ☐ Zusätzlicher Log-In für bestimmte Anwendungen ☐ Automatische Sperrung der Clients (Zeitablauf) ☐ Verwaltung von Berechtigungen ☐ Dokumentation von Berechtigungen ☐ Verschlüsselung von Systemen ☐ Sonstige:
10.	**Verarbeitung personenbezogener Daten nur nach Anweisung** Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?	☐ Mitarbeiter sind zu Verhaltensregeln verpflichtet ☐ Implementierung unternehmensinterner Datenschutz-Richtlinien ☐ Verpflichtung der Mitarbeiter auf das Datengeheimnis ☐ Schulungen aller zugriffsberechtigten Mitarbeiter ☐ Bestimmung von Ansprechpartnern für den konkreten Auftrag ☐ Sonstige:

Anlage 2

(allfällige) Weisungen zur Datenverarbeitung

Sollten sich datenschutzrechtliche Pflichten ergeben, die sich nicht bereits aus gesetzlichen Bestimmungen oder dem Hauptvertrag ableiten, kann das Bundesministerium für Bildung (BMB) als Auftraggeber in dieser Anlage entsprechende Weisungen formulieren.

Sollte dies nicht erforderlich sein, ist diese Anlage nicht auszufüllen.