

Auftragsverarbeitungsvertrag

STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

- a. Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der 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 sichergestellt werden.
- b. Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.
- c. Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
- d. Die Anhänge I bis IV sind Bestandteil der Klauseln.
- e. Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.
- f. Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

- a. Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
- b. Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

- a. Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- b. Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.
- c. Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ

Kopplungsklausel

- a. Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
- b. Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
- c. Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1 Weisungen

- a. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
- b. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

- a. Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den

Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

- b. Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Klauseln

- a. Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- b. Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- c. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.
- d. Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- e. Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

- a. Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 30 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.
- b. Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.
- c. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- d. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag

nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

- e. Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

- a. Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.
- b. Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

- a. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
- b. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- c. Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:
1. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
 2. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
 3. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
 4. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
- d. Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seine Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

- a. bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
- b. bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
 1. die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 2. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 3. die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

- c. bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- a. eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- b. Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- c. die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

- a. Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- b. Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 1. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 2. der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;
 3. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.
- c. Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.
- d. Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r):

Name: Musterschule

Anschrift: Musterstraße 1, 55555 Musterstadt

Name der Kontaktperson: Erika Mustermann

Unterschrift und Beitrittsdatum: **Am 01.01.2018 von Erika Mustermann digital akzeptiert und als unveränderliches Dokument im Benutzerkonto hinterlegt (Art. 28 Abs. 9 DSGVO).**

Auftragsverarbeiter:

Name: indibit GmbH

Anschrift: Wittelsbacherring 10, 95444 Bayreuth

Kontakt: kontakt@indibit.eu

Datenschutzbeauftragter des Auftragnehmers:

heyData GmbH

Schützenstraße 5

10117 Berlin

Kontakt: datenschutz@heydata.eu

M u s t e r

Unterschrift und Beitrittsdatum: **Am 01.01.2018 von Dr. Michael Zeising (Geschäftsführer) digital akzeptiert und als unveränderliches Dokument im Benutzerkonto hinterlegt (Art. 28 Abs. 9 DSGVO).**

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- *Schülerinnen und Schüler der Schule*
- *(Fach-) Lehrkräfte der Schule*
- *Nicht unterrichtendes Personal der Schule*
- *Eltern der Schule*

Kategorien personenbezogener Daten, die verarbeitet werden

1. *(Fach-) Lehrkräfte und nicht unterrichtendes Personal*
 - a. *Stammdaten: Name, Geschlecht, E-Mail-Adresse*
 - b. *Benutzerkonto: Benutzername bzw. E-Mail-Adresse, Prüfsuche des Kennworts, Zeitpunkt der letzten E-Mail Verifikation, Zeitpunkt der letzten Kennwortwiederherstellung*
 - c. *Anmeldedaten: Zeitpunkt der letzten Anmeldung, Zeitpunkt der letzten Aktivität, technische Angaben zum Browser und zur Plattform, IP-Adresse der letzten Anmeldung*
 - d. *Änderungshistorie: Zeitpunkt der letzten Änderung von Benutzerkonten, Einstellungen, Schülern, Klassen, Noten, Notensammlungen und Zeugnissen*
2. *Lehrkräfte*
 - a. *alle aus 1.*
 - b. *Klassenleitung, unterrichtete Fächer*
3. *Schülerinnen und Schüler*
 - a. *Stammdaten: Name, Geschlecht, Geburtstag*
 - b. *Unterricht: Klasse, Jahrgangsstufe, besuchte Fächer, Förderkurse und Arbeitsgemeinschaften*
 - c. *Zeugnis bzw. Lernentwicklungsgespräch: Bewertung in den Fächern, (voraussichtliche) Erreichung des Klassenziels*
 - d. *Leistungen: Note, Art, Gewichtung, Prüfung, Datum der Beurteilung*
 - e. *Beobachtungen: Notizen im Freitext (durch die Schulleitung /-verwaltung deaktivierbar)*
 - f. *Abwesenheiten: Zeitraum, Begründung, Zustand, Art*
 - g. *Zahlungsdaten: Art, Zahlungszweck, Summe und Zahlungsweg (bar oder Überweisung).*
4. *Eltern*
 - a. *Stammdaten: Name, E-Mail-Adresse*
 - b. *Benutzerkonto: Benutzername bzw. E-Mail-Adresse, Prüfsuche des Kennworts, Zeitpunkt der letzten E-Mail Verifikation, Zeitpunkt der letzten Kennwortwiederherstellung*
 - c. *Anmeldedaten: Zeitpunkt der letzten Anmeldung, Zeitpunkt der letzten Aktivität, technische Angaben zum Browser und zur Plattform, IP-Adresse der letzten Anmeldung*

Art der Verarbeitung

Die Erhebung und Erfassung erfolgt durch die manuelle Eingabe von Daten durch die Nutzer (Lehrkräften/Schulpersonal/Eltern) ins System.

Für die automatisierte Erhebung von Stammdaten (Lehrkräfte, Schüler, Klassen, Kurse) werden durch den Auftragsverarbeiter Import-Schnittstellen bereitgestellt. Der entsprechende Nutzer der jeweiligen Schule hat die Möglichkeit, die benötigten Stammdaten gesamthaft zu importieren.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Verwaltung von Schulnoten, Schülerbeobachtungen und Zeugnissen inkl. Formulare zu Lernentwicklungsgesprächen; Kommunikation mit Eltern; Dokumentation von Zahlungen

Dauer der Verarbeitung

1, 2 Löschung nach Kündigung der Nutzungsvereinbarung mit der Schule, spätestens jedoch am Ende des Schuljahres, in dem die Lehrkraft bzw. die nicht unterrichtende Person die Schule verlässt

3 a, b Löschung nach Kündigung der Nutzungsvereinbarung mit der Schule, spätestens jedoch am Ende des nachfolgenden Schuljahres, in dem die Schülerin/der Schüler von der Schule abgegangen ist

3 c, d, e, f, g Löschung nach Kündigung der Nutzungsvereinbarung mit der Schule, spätestens jedoch am Ende des nachfolgenden Schuljahres, in dem die Daten gespeichert wurden

M u s t e r

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN NACH ART. 32 DSGVO, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

1 Vertraulichkeit

1.1 Zutrittskontrolle

Der Betrieb der technischen Einrichtungen obliegt ausschließlich dem Unterauftragnehmer für das Hosting (siehe Anhang IV). Dieser ist dazu verpflichtet, geeignete Maßnahmen zur Zutrittskontrolle umzusetzen und weist dies unter anderem in Form einer Zertifizierung nach ISO 27001:2013 nach.

1.2 Zugangskontrolle

1.2.1 Sicherung durch Kennwörter

Der Zugang zu edoop.de erfolgt über die Eingabe einer Benutzerkennung und eines Kennworts. Kennwörter werden grundsätzlich nicht im Klartext gespeichert, sondern zugriffssicher mittels Einwegverschlüsselung (Hashfunktion) abgelegt. Dabei kommt ein geeignetes, kollisionsresistentes Verfahren zum Einsatz. Während der Eingabe werden persönliche Kennwörter standardmäßig nicht im Klartext angezeigt. Jeder Benutzer kann sein Kennwort jederzeit ändern. Während der initialen Vergabe und jeder Änderung des Kennworts wird der Benutzer durch eine Entropiemessung (Kennwortgüte) unterstützt. Kennwörter unterhalb geeigneter Grenzen werden dabei vom System abgelehnt.

1.2.2 Zeitbasierte Einmalkennwörter (TOTP) als zweiter Faktor

Zusätzlich zur Sicherung durch Benutzerkennung und Kennwort kann ein zweiter Faktor in Form zeitbasierter Einmalkennwörter eingerichtet werden. Benutzer müssen sich zuerst mit ihrem herkömmlichen Benutzernamen und Passwort authentifizieren. Nach der Einrichtung wird auf neuen Geräten oder spätestens alle 30 Tage ein einmaliges, zeitlich begrenztes Passwort abgefragt, das von einer TOTP-Anwendung auf einem vertrauenswürdigen Endgerät des Benutzers generiert wird. Die Einmalkennwörter werden nur für einen definierten Zeitraum (30 Sekunden) generiert. Eine erneute Eingabe des Codes ist nach Ablauf der Zeit nicht möglich.

1.2.3 Sichere Verwaltung von Sitzungen

Jede Sitzung (session) hat eine begrenzte Gültigkeitsdauer. Die Sitzungskennung ist eine zufällige Zeichenkette mit geeigneter Entropie. Die Sitzungskennung wird ausschließlich in cookies übertragen und nicht in den URLs, sodass sie von beteiligten IT-Systemen nicht gespeichert und nicht von Dritten eingesehen werden kann. Unbekannte Sitzungskennungen werden vom System abgelehnt. Die Sitzung wird zusätzlich durch die IP des Benutzers zugeordnet, um eine unbefugte Nutzung zu erschweren.

1.2.4 Verhinderung von Cross-Site Scripting (XSS)

Zur Verhinderung von Cross-Site Scripting wird der reflexive XSS-Schutz des Browsers durch die HTTP-Direktive X-Xss-Protection aktiviert und mutmaßlich schadhafte Anfragen werden durch den Browser blockiert.

1.2.5 Verhinderung von Cross-Site Request Forgery (CSRF, XSRF, Session Riding)

Ein CSRF-Angriff wird verhindert, indem neben der Sitzungskennung ein zusätzliches geheimes Merkmal (token) für jeden einzelnen Aufruf benötigt wird. Dieses Merkmal wird für jede Sitzung neu erzeugt.

1.2.6 Verhinderung von click jacking

Das click jacking durch nicht sichtbare HTML-Rahmen (frames) wird verhindert, indem durch die HTTP-Direktive X-Frame-Options nur Inhalte der eigenen Domäne erlaubt werden.

1.2.7 Schutz vor SQL injection

Es kommen ausschließlich emulierte stored procedures zum Einsatz, bei denen Sonderzeichen oder schadhafte SQL-Anweisungen in den Parametern automatisch maskiert werden.

1.2.8 Absenderschutz und Signatur von E-Mails

Zusammen mit unserem Partner für den Versand von E-Mails setzen wir die Sicherheitsmechanismen SPF, DKIM und DMARC ein. Damit wird verhindert, dass unberechtigte Dritte E-Mails im Namen von edoop.de senden (Phishing) oder E-Mails auf dem Weg zu Ihnen verändern (Man-in-the-Middle-Angriff).

1.3 Zugriffskontrolle

Der Zugriff auf das System ist durch eine Nutzer- und Rechteverwaltung abgesichert. Es ist dem einzelnen Benutzer nur möglich die für seine Aufgaben erforderlichen Daten einzusehen, zu nutzen, zu verarbeiten oder zu löschen.

1.4 Trennungskontrolle

Die Daten der Mandanten (Schulen) werden strikt logisch durch eine Markierung voneinander getrennt. Durch eine separate Zugriffssicherungskomponente wird sichergestellt, dass ein Benutzer ausschließlich auf die Daten der eigenen Schule zugreifen kann.

Die Identität von edoop.de wird über ein Zertifikat von einem Anbieter sichergestellt, dessen zentraler Geschäftsgegenstand die Ausstellung von Sicherheitszertifikaten ist.

Für Primärdaten werden ausschließlich Datenbanktabellen auf Basis des Speichersystems InnoDB verwendet. Das System für Primärdaten ist transaktionssicher mit der Isolationsebene REPEATABLE READ und die referentielle Integrität wird über Fremdschlüssel-Constraints gewährleistet.

Entwicklungs-, Test- und Produktivumgebungen sind voneinander getrennt.

2 Integrität

M u s t e r

2.1 Weitergabekontrolle

Die Kommunikation zwischen dem Browser des Benutzers und dem Server von edoop.de erfolgt zwingend über das TLS-Protokoll (SSL, HTTPS). Dies wird server-seitig durch eine permanente Umleitung von Netzwerk-Port 80 auf 443 und client-seitig durch HTTP Strict Transport Security (HSTS) sichergestellt.

Die Identität von edoop.de wird über ein Zertifikat von einem Anbieter sichergestellt, dessen zentraler Geschäftsgegenstand die Ausstellung von Sicherheitszertifikaten ist.

Zur Verschlüsselung der Kommunikationsverbindung werden ausschließlich die Verfahren TLS 1.2 und 1.3 eingesetzt. Es werden ausschließlich Cipher-Suites genutzt, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen werden (BSI TR-03116-4, Kryptographische Vorgaben für Projekte der Bundesregierung). Der Schutz des privaten Schlüssels beim Server wird vom Dienstleister für das Hosting übernommen. Es werden ausschließlich Sicherheitseinstellungen verwendet, die zu einer grünen Bewertung beim Dienst sslabs.com führen.

2.2 Eingabekontrolle

Alle Vorgänge, die im Zusammenhang mit personenbezogenen Daten stehen, werden im Rahmen eines Audit Logs protokolliert und 90 Tage lang aufbewahrt.

3 Verfügbarkeit und Wiederherstellung

Im Rahmen eines umfassenden Monitorings wird die Betriebsinfrastruktur hinsichtlich ihrer Leistungsdaten durch die Auftragnehmerin selbst und durch die Unterauftragnehmerin für das Hosting rund um die Uhr überwacht.

Die Datenbank von edoop.de wird täglich nachts gesichert. Jede Sicherung (backup) wird maximal 3 Monate lang aufbewahrt. Sicherungen werden auf verschlüsselten Festplatten gespeichert, auf die nur über gesicherte Verbindungen und nur von Befugten zugegriffen werden kann. Die Wiederherstellung der Sicherung (recovery) wird regelmäßig, mindestens aber nach jeder Änderung des Sicherungsprozesses, getestet.

Der Dienstleister für das Hosting sorgt für eine Absicherung gegenüber Festplattendefekten durch die Spiegelung mindestens per RAID 1.

M u s t e r

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Alle Mitarbeitenden des Auftragsverarbeiters, die personenbezogene Daten verarbeiten, werden regelmäßig geschult und auf die Vertraulichkeit/ das Datengeheimnis verpflichtet.

Der Auftragsverarbeiter hat einen zertifizierten Mitarbeitenden zum Informationssicherheitsbeauftragten bestellt.

Der Auftragsverarbeiter setzt eine Software-Lösung für sein Datenschutz-Management ein.

Der Auftragsverarbeiter kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach.

4.2 Incident-Response-Management

Der Auftragsverarbeiter hat einen etablierten Prozess für den Umgang mit Sicherheitsvorfällen, der die Einbindung des DSBs sowie des ISBs vorsieht.

4.3 Datenschutzfreundliche Voreinstellungen

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

4.4 Auftragskontrolle (Outsourcing an Dritte)

Der Auftragsverarbeiter weist einen Prozess zur Auswahl seiner Auftragnehmer unter Sorgfaltsgesichtspunkten, besonders in Bezug auf Datenschutz und Datensicherheit, auf. Der Auftragsverarbeiter schließt mit seinen Auftragnehmern die notwendige Vereinbarung zur Auftragsverarbeitung ab.

M u s t e r

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

ERLÄUTERUNG:

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Name	Anschrift	Kontakt bei Fragen zum Datenschutz:	Beschreibung der Verarbeitung
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	data-protection@hetzner.com	Infrastruktur- und Plattformdienstleistungen, Rechenkapazität, Speicherplatz und Datenbankdienste, Sicherheitsleistungen sowie technische Wartungsleistungen
IONOS SE	Elgendorfer Str. 57 56410 Montabaur	datenschutz@ionos.de	Infrastruktur- und Plattformdienstleistungen, Rechenkapazität, Speicherplatz und Datenbankdienste, Sicherheitsleistungen sowie technische Wartungsleistungen
Sendinblue GmbH	Köpenicker Straße 126 10179 Berlin	datenschutz@brevo.com	Versand von transaktionalen und anlassbezogenen E-Mails
Zammad GmbH	Marienstraße 18 10117 Berlin	support@zammad.com	Helpdesk-System zur Bearbeitung von Anfragen per E-Mail und Telefon