Vereinbarung zur Auftragsverarbeitung

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen der

Musterschule vertreten durch Erika Mustermann
— Verantwortlicher — nachstehend Auftraggeber

und der

indibit GmbH, Wittelsbacherring 10, 95444 Bayreuth vertreten durch Dr. Michael Zeising
— Verarbeiter — nachstehend Auftragnehmer

§ 1 Gegenstand

Im Rahmen der Leistungserbringung nach dem Vertrag vom 01.01.2018 (nachfolgend „Hauptvertrag " genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten" genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

§ 2 Umfang der Beauftragung

1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.
2. Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in **Anlage A** zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.
3. Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet ausschließlich in Mitgliedstaaten der Europäischen Union (EU) oder Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

§ 3 Weisungsbefugnis des Auftraggebers

1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
2. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und bedürfen der Textform.
3. Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für

die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

§ 4 Verantwortlichkeit des Auftraggebers

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.
2. Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.
3. Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.
4. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

§ 5 Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

§ 6 Sicherheit der Verarbeitung

1. Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten. Diese technischen und organisatorischen Maßnahmen sind in **Anlage B** näher beschrieben.
2. 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.

§ 7 Inanspruchnahme weiterer Auftragsverarbeiter

1. Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses bereits hinzugezogenen weiteren Auftragsverarbeiter sind in **Anlage C** aufgeführt.
2. Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.
3. Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes

Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

4. Unter Einhaltung der Anforderungen des § 2 Nr. 3 dieses Vertrags gelten die Regelungen in diesem § 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem weiteren Auftragsverarbeiter einen Vertrag unter Einbeziehung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vom 5.2.2010 zu schließen. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

§ 8 Rechte der betroffenen Person

1. Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.
2. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.
3. Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.
4. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.
5. Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

§ 9 Mitteilungs- und Unterstützungspflichten des Auftragnehmers

1. Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.
2. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

§ 10 Datenlöschung

1. Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht . Näheres wird in **Anlage A** geregelt.
2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

§ 11 Nachweise und Überprüfungen

1. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.
2. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.
3. Zur Durchführung von Inspektionen nach § 11 Abs. 2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 09 bis 17 Uhr) nach rechtzeitiger Vorankündigung gemäß § 11 Abs. 5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.
4. Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.
5. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.
6. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser § 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.
7. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage zusätzlich zu Inspektionen auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit — z.B. nach BSI-Grundschutz — („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

§ 12 Laufzeit und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags.
Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

§ 13 Haftung

1. Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag oder den jeweils geltenden Nutzungsbedingungen. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.
2. Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 14 Datenschutzbeauftragter des Auftragnehmers

Beim Auftragnehmer ist als Beauftragter für den Datenschutz Herr

Dr. Christopher Lieb
Bayreuther Straße 24
91054 Erlangen
christopher.lieb@lieb-online.com

bestellt.

§ 15 Schlussbestimmungen

1. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.
2. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

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

Erika Mustermann	Dr. Michael Zeising (Geschäftsführer)
Auftraggeber	Auftragnehmer

Anlagenverzeichnis
Anlage A: Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO
Anlage B: Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO
Anlage C: Liste der Unterauftragnehmer

Anlage A:
Verzeichnis von Verarbeitungstätigkeiten (Verantwortlicher)

nach Art. 30 Abs. 1 DSGVO

Angaben zum Verantwortlichen

Musterschule
Musterstraße 1
55555 Musterstadt

Angaben zur Person des Datenschutzbeauftragten

Anrede | Titel

Name | Vorname

Straße

Postleitzahl | Ort

Telefon | E-Mail-Adresse

Bezeichnung der Verarbeitungstätigkeit

Datum der Anlegung: 01.01.2018	**Datum der letzten Änderung:** -/-

Ansprechpartner	Erika Mustermann
Bezeichnung der Verarbeitungstätigkeit	edoop.de
Zwecke der Verarbeitung	Verwaltung von Schulnoten, Schülerbeobachtungen und Zeugnissen inkl. Formulare zu Lernentwicklungsgesprächen; Kommunikation mit Eltern
Beschreibung der Kategorien betroffener Personen	• Schülerinnen und Schüler der Schule • (Fach-) Lehrkräfte der Schule • Nicht unterrichtendes Personal der Schule • Eltern der Schule
Beschreibung der Datenkategorien	1. (Fach-) Lehrkräfte und nicht unterrichtendes Personal a. Stammdaten: Name, Geschlecht, E-Mail-Adresse b. Benutzerkonto: Benutzername bzw. E-Mail-Adresse, Prüfsumme 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. 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 4. Eltern a. Stammdaten: Name, E-Mail-Adresse b. Benutzerkonto: Benutzername bzw. E-Mail-Adresse, Prüfsumme 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
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	*Die Liste unserer Unterauftragnehmer inkl. betroffener Datenkategorien entnehmen Sie bitte **Anlage C**.*
Datenübermittlung	-/-
Fristen für die Löschung der verschiedenen Datenkategorien	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 Löschung nach Kündigung der Nutzungsvereinbarung mit der Schule, spätestens jedoch am Ende des nachfolgenden Schuljahres, in dem die Daten gespeichert wurden

Musterstadt, den 01.01.2018

Erika Mustermann

Anlage B:
Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO

1 Vertraulichkeit

1.1 Zutritt zu technischen Einrichtungen

Der Betrieb der technischen Einrichtungen obliegt ausschließlich der Unterauftragnehmerin für das Hosting. Sie setzt die entsprechenden Maßnahmen um und weist dies unter anderem in Form einer Zertifizierung nach ISO 27001:2013 nach.

1.2 Unterbindung des Zugangs durch Unbefugte

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 (Hash-Funktion) abgelegt. Dabei kommt ein geeignetes, kollisionsresistentes Verfahren zum Einsatz. Während der Eingabe werden persönliche Kennwörter nie 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 Grenze werden dabei vom System abgelehnt.

1.2.2 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.

Falls sich Benutzer nicht aktiv vom System abmelden, werden sie beim nächste Anmeldevorgang ausdrücklich darauf hingewiesen.

1.2.3 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.

1.2.4 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.

1.2.5 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.

1.2.6 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.

1.3 Durchsetzung von Zugriffsberechtigungen

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 Schutz während der elektronischen Übertragung

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 vom TeleSec Trust Center der Deutschen Telekom AG geprüft, dessen zentraler Geschäftsgegenstand die Ausstellung von Sicherheitszertifikaten ist. Es gehört weltweit zu den führenden Zertifizierungsstellen und gilt somit als vertrauenswürdige Zertifizierungsstelle.

Zur Verschlüsselung der Kommunikationsverbindung wird ausschließlich das Verfahren TLS 1.2 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) und die eine grüne Bewertung beim Dienst *ssllabs.com* ergeben. Der Schutz des privaten Schlüssels beim Server wird vom Dienstleister für das Hosting übernommen.

1.5 Trennung von Mandanten

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.

2 Integrität und Protokollierung

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 einen Monat 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.

4 Weitere Maßnahmen

4.1 Restriktive Herausgabe sicherheitsrelevanter Informationen

Das System gibt grundsätzlich keine internen Fehlerinformationen wie *stack traces* und Informationen zum *debugging* aus. Die ausgelieferten Artefakte enthalten keine sicherheitsrelevanten Kommentare und die technische Dokumentation zur Entwicklung von edoop.de ist nicht öffentlich einsehbar. Das System gibt außerdem keine Informationen aus, die Rückschlüsse auf verwendete sicherheitsrelevante Software Dritter zulassen.

4.2 Gewährleistung der Datenintegrität

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

Anlage C:
Liste der Unterauftragnehmer

Unsere Dienstleister setzen wir auf Grundlage unserer berechtigten Interessen gem. Art. 6 Abs. 1 lit. f DSGVO und jeweils eines Auftragsverarbeitungsvertrages gem. Art. 28 DSGVO ein.

Name	Adresse	Leistungen
dogado.pro GmbH	Glashütter Straße 53 01309 Dresden	Infrastruktur- und Plattformdienstleistungen, Rechenkapazität, Speicherplatz und Datenbankdienste, Sicherheitsleistungen sowie technische Wartungsleistungen
Sendinblue GmbH	Köpenicker Straße 126 10179 Berlin	Versand von transaktionalen und anlassbezogenen E-Mails
Zammad GmbH	Marienstraße 18 10117 Berlin	Helpdesk-System zur Bearbeitung von Anfragen per E-Mail und Telefon