

Auftragsverarbeitungsvertrag

Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Art. 28

Abs. 7 DSGVO (Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021), ergänzt um die Anhänge I bis IV und ergänzende Vereinbarungen nach Klausel 2 Buchstabe b. Der Wortlaut der Klauseln 1 bis 10 entspricht dem Amtsblatt der EU (ABl. L 199 vom 7.6.2021, S. 18 ff.); Klausel 5 (fakultativ) ist nicht vereinbart, in Klausel 7.7 gilt Option 2. Fassung 2026-09.

zwischen

[Name der Schule], [Straße], [PLZ Ort], vertreten durch [Schulträger / zeichnungsberechtigte Stelle]
– im Folgenden „Verantwortlicher“ –

und

ZeitFürSchule UG (haftungsbeschränkt), Kantstr. 106, 10627 Berlin, vertreten durch Vianney Lancres – im Folgenden „Auftragsverarbeiter“ –

Dieser Vertrag ist Bestandteil des Vertrags über die Nutzung der Software „Zeugnisprogramm“ vom [Datum des Hauptvertrags] mit Vertragsbeginn [Vertragsbeginn] (im Folgenden „Hauptvertrag“) und ersetzt dessen bisherige Anlage 2 mit Wirkung ab Bestätigung durch den Verantwortlichen.

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 (Datenschutz-Grundverordnung) 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 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 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 und/oder der Verordnung (EU) 2018/1725 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 und/oder der Verordnung (EU) 2018/1725 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 bzw. der Verordnung (EU) 2018/1725 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 bzw. der Verordnung (EU) 2018/1725 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 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

Die fakultative Kopplungsklausel wird nicht vereinbart.

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, die Verordnung (EU) 2018/1725 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 personenbezogener 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 und/oder der Verordnung (EU) 2018/1725 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) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: 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 vier Wochen 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) Beauftragte 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 und/oder der Verordnung (EU) 2018/1725 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 oder der Verordnung (EU) 2018/1725 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 seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 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 und/oder der Verordnung (EU) 2018/1725 – 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 und/oder der Verordnung (EU) 2018/1725 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 und/oder der Verordnung (EU) 2018/1725 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.

Ergänzende Vereinbarungen (Klausel 2 Buchstabe b)

E.1 Laufzeit. Dieser Vertrag gilt für die Dauer des Hauptvertrags und darüber hinaus, solange der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen verarbeitet.

E.2 Form. Änderungen und Ergänzungen dieses Vertrags einschließlich der Anhänge sowie Weisungen bedürfen der Textform (Art. 28 Abs. 9 DSGVO); E-Mail genügt. Aktualisierungen der Anhänge III und IV erfolgen nach dem in Ziffer E.5 beschriebenen Verfahren.

E.3 Meldefrist. „Unverzüglich“ im Sinne von Klausel 9.2 bedeutet spätestens 24 Stunden nach Kenntniserlangung des Auftragsverarbeiters von der Verletzung. Die Meldung erfolgt an die in Anhang I benannte Kontaktstelle des Verantwortlichen.

E.4 Kontrollen. Prüfungen nach Klausel 7.6 werden mit einer Vorankündigung von mindestens 14 Tagen während der üblichen Geschäftszeiten des Auftragsverarbeiters durchgeführt. Vorrangig erfüllt der Auftragsverarbeiter seine Nachweispflicht durch Auskünfte, Dokumentation (Anhang III, Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO) und Nachweise seiner Unterauftragsverarbeiter (z. B. Zertifizierungen, Auditberichte des Rechenzentrumsbetreibers). Vor-Ort-Prüfungen sind auf begründete Fälle beschränkt, weil die Verarbeitung ausschließlich in den Rechenzentren des Unterauftragsverarbeiters gemäß Anhang IV stattfindet.

E.5 Aktualisierung der technischen und organisatorischen Maßnahmen und der Unterauftragsverarbeiter. Der Auftragsverarbeiter darf die Maßnahmen nach Anhang III weiterentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird; wesentliche Änderungen teilt er dem Verantwortlichen in Textform mit. Änderungen an Anhang IV erfolgen nach Klausel 7.7 Buchstabe a mit vierwöchiger Vorankündigung. Die jeweils aktuelle Fassung der Anhänge III und IV sowie eine Änderungshistorie stellt der Auftragsverarbeiter unter www.zeitfuerschule.de/datenschutz/avv bereit. Widerspricht der Verantwortliche einer Änderung nach Anhang IV aus wichtigem datenschutzrechtlichem Grund und kann der Auftragsverarbeiter dem nicht abhelfen, kann der Verantwortliche den Hauptvertrag mit Wirkung zum Zeitpunkt des Wirksamwerdens der Änderung kündigen.

E.6 Vergütung. Die Unterstützungsleistungen nach den Klauseln 8 und 9 sowie die Rückgabe der Daten nach Klausel 10 Buchstabe d im Format nach Anhang III Ziffer 9 sind mit der Vergütung des Hauptvertrags abgegolten. Darüber hinausgehender Aufwand, den der Verantwortliche veranlasst (z. B. wiederholte Vor-Ort-Prüfungen, individuelle Exportformate), wird nach dem Preisblatt des Auftragsverarbeiters vergütet.

E.7 Haftung. Für die Haftung der Parteien gilt Art. 82 DSGVO. Die Haftungsregelungen des Hauptvertrags bleiben im Übrigen unberührt, soweit sie Art. 82 DSGVO nicht widersprechen.

E.8 Datenschutzbeauftragte/r. Der Auftragsverarbeiter ist nach Art. 37 DSGVO und § 38 BDSG nicht zur Benennung einer/eines Datenschutzbeauftragten verpflichtet: Er beschäftigt weniger als 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten, seine Kerntätigkeit besteht nicht in einer umfangreichen regelmäßigen und systematischen Überwachung betroffener Personen, und die Verarbeitung besonderer Kategorien personenbezogener Daten ist nicht vorgesehen. Ansprechstelle für den Datenschutz ist die in Anhang I genannte Kontaktstelle.

E.9 Zuständige Aufsichtsbehörden. Für den Verantwortlichen: [Landesbeauftragte/r für Datenschutz des Bundeslands]. Für den Auftragsverarbeiter: Berliner Beauftragte für Datenschutz und Informationsfreiheit, Alt-Moabit 59–61, 10555 Berlin.

E.10 Anwendbares Recht, Gerichtsstand. Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Berlin, soweit der Verantwortliche juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

Anhang I – Liste der Parteien

Verantwortlicher

Name	[Name der Schule]
Anschrift	[Straße], [PLZ Ort], Deutschland
Schulträger	[Schulträger]
Kontaktstelle (Name, Funktion, E-Mail)	[Name, Funktion], [E-Mail]
Datenschutzbeauftragte/r	[Datenschutzbeauftragte/r der Schule oder des Trägers]
Weisungsberechtigte Personen	die vorstehende Kontaktstelle sowie die vom Verantwortlichen in der Software mit der Rolle „Verwaltung“ ausgestatteten Nutzer für Weisungen, die durch Bedienung der Software erteilt werden (Anlegen, Ändern, Löschen, Exportieren von Daten)

Auftragsverarbeiter

Name	ZeitFürSchule UG (haftungsbeschränkt)
Anschrift	Kantstr. 106, 10627 Berlin, Deutschland
Vertreten durch	Vianney Lancres
Kontaktstelle Datenschutz und Sicherheitsvorfälle	Vianney Lancres, vianney.lancres@zeitfuerschule.de; datenschutz@zeitfuerschule.de
Datenschutzbeauftragte/r	nicht benannt (siehe Ergänzende Vereinbarung E.8); Ansprechstelle Datenschutz: datenschutz@zeitfuerschule.de
Weisungsempfänger	Vianney Lancres (vianney.lancres@zeitfuerschule.de)

Unterschrift und Beitrittsdatum

Berlin,

Ort, Datum

Ort, Datum

ZeitFürSchule, Vianney Lancres

[Name der Schule]
vertreten durch [Schulträger / zeichnungsberechtigte
Stelle]

Anhang II – Beschreibung der Verarbeitung

Version 2026-09. Dieser Anhang beschreibt die Verarbeitung nach Klausel 6 der Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/915) für die Software „Zeugnisprogramm“ von ZeitFürSchule.

1. Gegenstand und Zweck der Verarbeitung

Der Auftragsverarbeiter betreibt für den Verantwortlichen die webbasierte Software „Zeugnisprogramm“ als Software-as-a-Service. Die Verarbeitung dient ausschließlich folgenden Zwecken:

- Verwaltung der Stammdaten von Schülerinnen und Schülern, Klassen, Kursen und Lehrkräften der Schule;
- Erfassung von Beurteilungen, Bewertungen, Textbausteinen und Fehlzeiten durch die unterrichtenden Lehrkräfte;
- Erzeugung von Zeugnisdokumenten (PDF) nach den Vorlagen des Verantwortlichen;
- Verwaltung der Benutzerkonten und Zugriffsrechte der Lehrkräfte einschließlich Anmeldung, Zwei-Faktor-Authentisierung und Sitzungssteuerung;
- Import und Export der vorgenannten Daten (Excel/CSV) durch berechtigte Nutzer des Verantwortlichen;
- Versand von Systemnachrichten per E-Mail (Einladung, Passwort-Zurücksetzen, Sicherheitshinweise, Export-Benachrichtigung).

Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt. Es werden keine Nutzungsanalysen, kein Tracking und keine KI-Funktionen eingesetzt.

2. Art der Verarbeitung

Speichern, Erheben (durch Nutzer des Verantwortlichen), Ordnen, Verändern, Auslesen, Abfragen, Verwenden zur Dokumenterzeugung, Bereitstellen zum Abruf, Löschen. Die Daten werden auf Systemen des Auftragsverarbeiters in Rechenzentren des Unterauftragsverarbeiters Microsoft (Anhang IV) gespeichert und verarbeitet. Eine Kenntnisnahme von Inhalten durch den Auftragsverarbeiter erfolgt nur im Support- oder Störfall und nur soweit erforderlich.

3. Kategorien betroffener Personen

- Schülerinnen und Schüler des Verantwortlichen
- Lehrkräfte, Schulleitung und Verwaltungspersonal des Verantwortlichen (Nutzerinnen und Nutzer)

4. Kategorien personenbezogener Daten

Betroffene	Datenkategorie	Einzelne Datenfelder	Pflicht/optional
Schülerinnen und Schüler	Stammdaten	Vorname, Nachname, Rufname, Geschlecht, Geburtsdatum, Geburtsort, Schulbesuchsjahr, externe Kennung (z. B. Schulverwaltungs-ID)	Vor-/Nachname, Geschlecht, Geburtsdatum, Klasse: Pflicht; übrige: optional
Schülerinnen und Schüler	Organisationsdaten	Jahrgang, Klasse, Kurszuordnungen, Versetzungsvermerk	Pflicht
Schülerinnen und Schüler	Leistungs- und Beurteilungsdaten	Freitext-Beurteilungen je Fach/Kurs, ausgewählte Textbausteine, Bewertungsstufen, Angaben zu Kompetenz-/Zertifikatsstufen, Angaben zum Arbeits- und Sozialverhalten (sofern die Zeugnisvorlage dies vorsieht)	optional (durch Lehrkräfte erfasst)
Schülerinnen und Schüler	Fehlzeiten	Fehltage und Fehlstunden, jeweils entschuldigt/unentschuldigt, Verspätungen	optional
Schülerinnen und Schüler	Zeugnisdokumente	Vorübergehend erzeugte PDF-Dateien mit den vorgenannten Daten sowie Schulname, Anschrift, Name der Schulleitung, Name der Lehrkraft (sofern Vorlage dies vorsieht)	temporär, siehe Ziffer 6
Lehrkräfte / Nutzer	Konto- und Stammdaten	Vorname, Nachname, E-Mail-Adresse (zugleich Benutzername), Geschlecht/Anrede, Kürzel, Klassenleitung(en), Berechtigungsrolle (Lehrkraft, Verwaltung, Klassenleitungs-Zugriffsstufe)	E-Mail, Name: Pflicht; übrige: optional
Lehrkräfte / Nutzer	Authentisierungsdaten	Passwort (nur als Hash, PBKDF2), TOTP-Geheimnis und Wiederherstellungscodes für die Zwei-Faktor-Authentisierung, Sitzungskennungen	bei Nutzung

Betroffene	Datenkategorie	Einzelne Datenfelder	Pflicht/optional
Lehrkräfte / Nutzer	Sicherheits- und Nutzungsprotokoll	Anmeldeereignisse (Anmeldung, Fehlversuch, Abmeldung, Sitzungsablauf, Passwort-/2FA-Änderung, Rechteänderung) mit Zeitstempel und gekürzter IP-Adresse (letztes Oktett bzw. bei IPv6 die letzten 80 Bit entfernt); „zuletzt geändert von“ an Beurteilungen; Änderungsprotokoll der Verwaltungsoberfläche	automatisch, Löschung nach 90 Tagen (Anmeldeereignisse)
Lehrkräfte / Nutzer	Persönliche Einstellungen	Anzeige- und Sortierpräferenzen, Stand gelesener Hinweise	optional
Verantwortlicher	Stammdaten der Schule	Schulname, Anschrift, Schulnummer, Name der Schulleitung, Support-E-Mail-Adresse, Logo, Schuljahr, Zeugnistern	Pflicht

5. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

Die Software sieht keine Datenfelder für besondere Kategorien personenbezogener Daten vor (keine Felder zu Religion, Gesundheit, Herkunft, Förderbedarf o. ä.). Freitextfelder für Beurteilungen können durch Nutzer des Verantwortlichen grundsätzlich beliebige Inhalte aufnehmen. Der Verantwortliche stellt durch Weisung an seine Nutzer sicher, dass in Freitexte nur Inhalte aufgenommen werden, die für das jeweilige Zeugnis nach den landesrechtlichen Vorgaben erforderlich sind. Die in Anhang III beschriebenen Maßnahmen gelten unabhängig davon für alle Daten gleichermaßen.

6. Dauer der Verarbeitung und Löschung

- Die Verarbeitung erfolgt für die Dauer des Hauptvertrags.
- Schüler- und Nutzerdatensätze werden auf Weisung des Verantwortlichen (durch dessen berechnigte Nutzer in der Software) einzeln oder im Rahmen des Schuljahreswechsels gelöscht. Die Löschung erfolgt physisch (kein „Papierkorb“); verknüpfte Beurteilungen werden mitgelöscht.
- Erzeugte Zeugnis-PDFs stehen 2 Stunden zum Abruf bereit und werden spätestens 3 Stunden nach Erzeugung automatisch gelöscht.
- Anmeldeereignisse werden nach 90 Tagen automatisch gelöscht.
- Bei Beendigung des Hauptvertrags gilt Klausel 10 der Standardvertragsklauseln; Löschung des gesamten Datenbestands (Datenbankschema des Verantwortlichen) innerhalb von 30 Tagen nach Wahl des Verantwortlichen mit oder ohne vorherige Herausgabe; Datensicherungen werden spätestens nach Ablauf der Sicherungsaufbewahrung von 35 Tagen überschrieben.

7. Häufigkeit

Kontinuierlich während der Vertragslaufzeit, mit Nutzungsschwerpunkten zu den Zeugnisterminen.

Anhang III – Technische und organisatorische Maßnahmen

Version 2026-09. Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO für die Software „Zeugnisprogramm“, einschließlich der Maßnahmen zur Unterstützung des Verantwortlichen (Klausel 8 Buchstabe d und Klausel 9.2). Die Beschreibung folgt dem tatsächlichen Stand von Software und Betrieb; Angaben zum Rechenzentrumsbetreiber beruhen auf dessen veröffentlichten Nachweisen.

1. Betriebsumgebung

- Betrieb ausschließlich auf Microsoft Azure in der Region Microsoft Azure, Region „Germany West Central“ (Frankfurt am Main). Eine Verarbeitung außerhalb der EU findet nicht statt; Microsoft sichert dies über die „EU Data Boundary“ zu (Anhang IV).
- Komponenten: Azure App Service (Anwendung: Webserver, Anwendungsserver, Hintergrundverarbeitung), Azure Database for PostgreSQL (Datenbank), Azure Files (Zeugnisvorlagen). Es werden keine weiteren Cloud-Dienste für personenbezogene Daten genutzt.
- Getrennte Umgebungen für Entwicklung/Test und Produktion. In der Entwicklungsumgebung werden ausschließlich Testdaten und keine Produktivdaten von Schulen verwendet.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b)

2.1 Zutrittskontrolle

Die Rechenzentren werden von Microsoft betrieben. Physische Sicherheit (Zutrittskontrolle mit mehrstufiger Authentisierung, Videoüberwachung, Sicherheitspersonal, Besucherprotokollierung) ist durch die Zertifizierungen ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3 und den BSI C5-Testat nachgewiesen; Nachweise sind über das Microsoft Service Trust Portal abrufbar. Der Auftragsverarbeiter selbst betreibt keine eigenen Serverräume; an seinem Firmensitz werden keine personenbezogenen Daten des Verantwortlichen dauerhaft gespeichert.

2.2 Zugangskontrolle (Systemzugang)

- Anmeldung der Nutzer nur mit persönlichem Benutzerkonto (E-Mail-Adresse) und Passwort.
- Passwortregeln: mindestens 8 Zeichen, mindestens eine Ziffer und ein Sonderzeichen, keine Ähnlichkeit zu Name/E-Mail, Abgleich gegen eine Liste häufiger Passwörter, keine rein numerischen Passwörter. Passwörter werden ausschließlich als Hash (PBKDF2-SHA256, Django-Standard) gespeichert.
- Zwei-Faktor-Authentisierung (TOTP nach RFC 6238 mit Authenticator-App, dazu zehn Einmal-Wiederherstellungscodes). Der Verantwortliche kann die 2FA je Schule für alle Nutzer oder für Nutzer mit Verwaltungsrechten verpflichtend machen (Übergangsfrist wählbar bis 30 Tage). Die 2FA-Geheimnisse werden mandantengetrennt gespeichert.
- Schutz vor Brute-Force-Angriffen: Drosselung der Anmeldeversuche je IP-Adresse (20 pro Minute), Drosselung von Passwort-Zurücksetzen (10 pro Stunde); Kontosperrung für 15 Minuten

nach 10 Fehlversuchen innerhalb von 15 Minuten. Fehlermeldungen lassen nicht erkennen, ob ein Konto existiert.

- Sitzungssteuerung: automatische Abmeldung nach 60 Minuten Inaktivität und spätestens 12 Stunden nach Anmeldung (Plattform-Obergrenzen); der Verantwortliche kann je Schule kürzere Werte einstellen (15 bis 60 Minuten bzw. 4 bis 12 Stunden), nie längere. Bei Ablauf wird die Anzeige personenbezogener Daten im Browser verdeckt. Passwortänderungen beenden alle anderen Sitzungen des Kontos.
- Sitzungs-Cookies mit den Attributen Secure, HttpOnly und SameSite=Lax; Schutz gegen Cross-Site-Request-Forgery durch CSRF-Token.
- Einladung neuer Nutzer und Passwort-Zurücksetzen ausschließlich über personalisierte, 7 Tage gültige Einmal-Links; Passwörter werden nie per E-Mail versendet.
- Administrativer Zugang des Auftragsverarbeiters: personengebundene Konten mit Zwei-Faktor-Authentisierung für Azure-Portal und Quellcodeverwaltung; Zugriff auf Produktionssysteme (Azure-Portal, Datenbank, Quellcodeverwaltung) hat ausschließlich der Geschäftsführer Vianney Lancres; Azure-Portal und GitLab sind mit Zwei-Faktor-Authentisierung gesichert.

2.3 Zugriffskontrolle (Berechtigungen innerhalb der Software)

- Rollenmodell je Schule: „Lehrkraft“ (Standard), „Verwaltung“ (erweiterte Rechte, vom Verantwortlichen vergeben), zusätzlich je Lehrkraft eine Klassenleitungs-Zugriffsstufe (kein Zugriff / lesend / schreibend auf Beurteilungen der eigenen Klasse durch andere Fächer).
- Lehrkräfte sehen ausschließlich Schülerinnen und Schüler der Kurse und Klassen, denen sie zugeordnet sind, und können nur dort Beurteilungen erfassen. Stammdatenpflege, Import/Export, Zeugniserzeugung und Schuljahreswechsel sind Nutzern mit Verwaltungsrechten vorbehalten.
- Jede Berechtigungsänderung (Verwaltungsrolle, Klassenleitungs-Zugriff, 2FA-Zurücksetzen durch Verwaltung) wird protokolliert (Ziffer 5).
- Plattformadministration durch den Auftragsverarbeiter über gesonderte Administratorkonten, ausschließlich für Einrichtung, Support und Störungsbeseitigung.

2.4 Trennungskontrolle (Mandantentrennung)

- Jede Schule erhält ein eigenes Datenbankschema in der PostgreSQL-Datenbank (schema-basierte Mandantentrennung mit django-tenants). Benutzerkonten, Sitzungen, 2FA-Geheimnisse, Fachdaten und Protokolle liegen vollständig im Schema der jeweiligen Schule.
- Die Zuordnung eines Aufrufs zum Schema erfolgt serverseitig über den Hostnamen der schulindividuellen Subdomain; Datenbankabfragen werden auf das aktive Schema beschränkt. Ein schemaübergreifender Zugriff ist in der Anwendung nicht vorgesehen. Hintergrundaufgaben (z. B. Zeugniserzeugung) laufen ebenfalls schemagebunden.
- Erzeugte Zeugnisdateien werden in schulindividuellen, zugriffsbeschränkten Verzeichnissen (Rechte 0700) abgelegt.
- Demo-/Testumgebung für Interessenten in einem gesonderten Schema mit fiktiven Daten, ohne Verbindung zu Schuldaten.

2.5 Pseudonymisierung und Datensparsamkeit

- Es werden nur die für Zeugnisse erforderlichen Datenfelder vorgehalten (Anhang II); keine Adress-, Eltern-, Gesundheits- oder Herkunftsdaten.
- IP-Adressen im Anmeldeprotokoll werden gekürzt gespeichert (IPv4: letztes Oktett entfernt; IPv6: auf /48 gekürzt); keine Speicherung von Browserkennungen.
- Importdaten werden nach Abschluss des Imports aus der Auftragsverwaltung entfernt; die hochgeladene Datei wird nicht gespeichert.
- Eine Pseudonymisierung der Schülernamen ist wegen des Zwecks (Zeugnisdokument) nicht möglich; für Lehrkräfte können vom Verantwortlichen funktionale E-Mail-Adressen verwendet werden.

2.6 Verschlüsselung

- Transport: ausschließlich HTTPS mit TLS 1.2 oder höher (mindestens TLS 1.2 auf App Service und Datenbank erzwungen); HTTP wird auf HTTPS umgeleitet; HSTS mit einjähriger Gültigkeit inklusive Subdomains und Preload. Verbindung Anwendung–Datenbank ebenfalls TLS-verschlüsselt. E-Mail-Versand über TLS (STARTTLS) an den Mailserver.
- Ruhende Daten: Datenbank, Datensicherungen und Dateispeicher sind auf Azure-Seite mit AES-256 verschlüsselt (Storage Service Encryption, von Microsoft verwaltete Schlüssel).
- Passwörter als Salted Hash (Ziffer 2.2).

3. Integrität (Art. 32 Abs. 1 lit. b)

3.1 Weitergabekontrolle

- Datenübertragung nur über TLS (Ziffer 2.6). Keine Übermittlung an Dritte außer an die Unterauftragsverarbeiter nach Anhang IV.
- Datenexporte (Zeugnis-PDF, Excel) nur durch Nutzer mit Verwaltungsrechten; Exportdateien nur nach Anmeldung abrufbar; Excel-Exporte mit Schutz gegen Formel-Injektion.
- E-Mails des Systems enthalten keine Beurteilungs- oder Schülerdaten, sondern nur Namen der Empfänger, Klassenbezeichnungen und Links.
- Support erfolgt ausschließlich durch Mitarbeitende des Auftragsverarbeiters; keine Fernwartungssoftware auf Endgeräten des Verantwortlichen.

3.2 Eingabekontrolle

- Anmeldeprotokoll je Schule: Anmeldung, fehlgeschlagene Anmeldung, Abmeldung, Sitzungsablauf, Passwortänderung, 2FA-Änderungen, Kontosperre und Berechtigungsänderungen, jeweils mit Zeitstempel, Konto und gekürzter IP-Adresse; Aufbewahrung 90 Tage; Nutzer können ihre eigene Anmeldehistorie einsehen.
- Beurteilungen speichern den zuletzt ändernden Nutzer; Änderungen an Stammdaten über die Verwaltungsoberfläche werden mit Nutzer und Zeitpunkt protokolliert.
- Sicherheitshinweis per E-Mail an den Nutzer bei Passwort- und 2FA-Änderungen.

- Versionierte Quellcodeverwaltung mit Änderungshistorie; Auslieferung nur über die automatisierte Build-Pipeline (Build einmal, Ausrollen auf Test, dann Produktion).

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c)

- Datensicherung: automatische, stündliche Sicherungen der PostgreSQL-Datenbank durch Azure mit Point-in-Time-Wiederherstellung; Aufbewahrung 35 Tage. Sicherungen der Anwendungsumgebung (App Service) mit Aufbewahrung 30 Tage. Sicherungen sind verschlüsselt (Ziffer 2.6) und werden innerhalb der Region Frankfurt am Main vorgehalten (keine Georedundanz, keine Speicherung außerhalb Deutschlands).
- Wiederherstellbarkeit: Wiederherstellung eines Datenbankstands ist über das Azure-Portal jederzeit möglich; Ein Wiederherstellungstest (Rücksicherung eines Sicherungsstands auf einen Testserver und Prüfung auf Vollständigkeit) wird jährlich durchgeführt und dokumentiert.
- Infrastruktur: Rechenzentren mit redundanter Strom- und Netzanbindung, Klimatisierung, Brandschutz und unterbrechungsfreier Stromversorgung (Nachweis über Zertifizierungen, Ziffer 2.1).
- Betriebsüberwachung: Überwachung der Verfügbarkeit und Fehler über Azure-Bordmittel und Anwendungsprotokolle; Rate-Limiting gegen Überlastung durch einzelne Quellen.
- Zeugniserzeugung als Hintergrundaufgabe mit Statusverfolgung; hängende Aufgaben werden automatisch als fehlgeschlagen markiert und können erneut angestoßen werden.
- Aktualisierungen: regelmäßige Sicherheitsaktualisierungen von Betriebssystem-Images, Laufzeitumgebung und Bibliotheken über die Build-Pipeline; Wartungsfenster vorzugsweise zwischen 20 und 8 Uhr.

5. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d)

- Jährliche Überprüfung dieses Anhangs und der Subunternehmerliste anhand des tatsächlichen Softwarestands; Änderungen werden versioniert und dem Verantwortlichen mitgeteilt (Ergänzende Vereinbarung E.5).
- Sicherheitsprüfung des Quellcodes bei wesentlichen Änderungen (Code Review nach Checkliste: Eingabevalidierung, Berechtigungsprüfung, Pfadvalidierung, Fehlerbehandlung, Protokollierung ohne Inhaltsdaten); letzte umfassende Sicherheitsüberprüfung Juli/August 2026 mit dokumentierter Nachverfolgung der Befunde.
- Automatisierte Tests (u. a. für Berechtigungen und Mandantentrennung) laufen bei jeder Auslieferung in der Build-Pipeline.
- Auftragskontrolle: Mit den Unterauftragsverarbeitern bestehen Verträge zur Auftragsverarbeitung (Anhang IV); ihre Zertifizierungen werden jährlich geprüft.
- Vertraulichkeitsverpflichtung aller Personen, die Zugang zu Daten des Verantwortlichen haben, nach Art. 28 Abs. 3 lit. b und Art. 32 Abs. 4 DSGVO; Derzeit hat ausschließlich der Geschäftsführer Zugriff auf Daten des Verantwortlichen; er unterliegt der Verschwiegenheitspflicht aus diesem Vertrag. Weitere Personen erhalten Zugriff erst nach schriftlicher Verpflichtung auf Vertraulichkeit und Datengeheimnis.

6. Löschung und Datenlebenszyklus

- Löschung einzelner Datensätze (Schüler, Lehrkräfte, Kurse) durch Nutzer mit Verwaltungsrechten jederzeit; physische Löschung einschließlich verknüpfter Beurteilungen.
- Assistent für den Schuljahreswechsel: Leeren der Beurteilungen, Versetzung, Entfernen ausgeschiedener Schülerinnen und Schüler.
- Automatische Löschung: Zeugnis-PDFs spätestens 3 Stunden nach Erzeugung (Bereitstellung 2 Stunden, stündlicher Löschlauf); Anmeldeprotokoll nach 90 Tagen; Importdaten sofort nach Abschluss des Imports.
- Mandantenlöschung bei Vertragsende: Löschung des gesamten Schemas und der Dateiverzeichnisse innerhalb von 30 Tagen nach Wahl des Verantwortlichen, schriftliche Bestätigung; Datensicherungen werden nach Ablauf der Aufbewahrung (Ziffer 4) automatisch überschrieben.
- Datenträger werden vom Rechenzentrumsbetreiber nach NIST SP 800-88 gelöscht bzw. vernichtet (Nachweis über Microsoft-Dokumentation). Beim Auftragsverarbeiter werden keine Datenträger mit Daten des Verantwortlichen geführt.

7. Unterstützung des Verantwortlichen (Klausel 8 Buchstabe d)

- Betroffenenrechte: Auskunft, Berichtigung und Löschung kann der Verantwortliche über die Verwaltungsoberfläche selbst ausführen (Datensatzansicht, Bearbeitung, Löschung, Excel-Export je Datentyp). Auf Anfrage stellt der Auftragsverarbeiter innerhalb von 10 Werktagen einen Gesamtexport der Daten einer betroffenen Person bereit.
- Datenschutz-Folgenabschätzung: Der Auftragsverarbeiter stellt dieses Dokument, Anhang II und auf Anfrage eine Beschreibung der Systemarchitektur als Grundlage zur Verfügung und beantwortet Rückfragen innerhalb von 10 Werktagen.
- Informationspflichten: Die Angaben in Anhang II (Zwecke, Datenkategorien, Empfänger, Speicherdauer) und Anhang IV (Unterauftragsverarbeiter) sind so gefasst, dass der Verantwortliche sie unmittelbar in seine Informationen nach Art. 13 DSGVO übernehmen kann; Rückfragen dazu beantwortet der Auftragsverarbeiter innerhalb von 10 Werktagen.
- Richtigkeit: Unrichtige Daten, die dem Auftragsverarbeiter bei Support oder Störungsbeseitigung auffallen, werden dem Verantwortlichen mitgeteilt.

8. Meldung von Verletzungen (Klausel 9.2 – weitere Angaben)

- Meldung an die Kontaktstelle des Verantwortlichen per E-Mail und, bei hohem Risiko, zusätzlich telefonisch, spätestens 24 Stunden nach Kenntnis.
- Inhalt zusätzlich zu Klausel 9.2: Zeitpunkt und Zeitraum des Vorfalls, betroffene Systeme und Schemata, ob Daten verschlüsselt waren, ob Unterauftragsverarbeiter betroffen sind, Ansprechpartner für Rückfragen, geplante Folgemeldungen.
- Der Auftragsverarbeiter dokumentiert alle Sicherheitsvorfälle einschließlich Ursache, Auswirkung und Abhilfemaßnahmen.

9. Rückgabe und Löschung bei Vertragsende (Klausel 10 Buchstabe d)

- Rückgabeformat: Excel-Dateien je Datentyp (Schüler, Lehrkräfte, Kurse, Textbausteine) über die Exportfunktion sowie auf Anfrage ein vollständiger Datenbankexport des Schemas (SQL-Dump) und die Zeugnisvorlagen.
- Löschung: Schema, Dateiverzeichnisse und Benutzerkonten innerhalb von 30 Tagen; Bestätigung in Textform mit Datum; Sicherungen laufen nach spätestens 35 Tagen aus.

Anhang IV – Liste der Unterauftragsverarbeiter

Version 2026-09. Der Verantwortliche hat die Beauftragung der folgenden Unterauftragsverarbeiter genehmigt (Klausel 7.7 Buchstabe a). Die Dauer der Unterauftragsverarbeitung entspricht der Dauer des Hauptvertrags. Die jeweils aktuelle Liste ist unter www.zeitfuerschule.de/datenschutz/avv abrufbar.

Unterauftragsverarbeiter	Anschrift	Gegenstand und Art der Verarbeitung	Ort der Verarbeitung	Vertrag und Garantien nach Kapitel V DSGVO
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Cloud-Infrastruktur (Microsoft Azure): App Service, Azure Database for PostgreSQL, Azure Files, Datensicherung	Rechenzentrumsregion Microsoft Azure, Region „Germany West Central“ (Frankfurt am Main); Speicherung und Verarbeitung von Kundendaten innerhalb der EU („EU Data Boundary“)	Vertragspartner ist die irische Microsoft-Gesellschaft. Auftragsverarbeitungsvertrag „Datenschutznachtrag für Produkte und Services von Microsoft“ (DPA, Stand 22. Mai 2026), Bestandteil der Azure-Nutzungsbedingungen; er enthält die Standardvertragsklauseln der Kommission von 2021 (Auftragsverarbeiter-zu-Auftragsverarbeiter) für etwaigen Zugriff durch Microsoft Corporation (USA). Microsoft ist zudem unter dem EU-US Data Privacy Framework zertifiziert. Speicherung und Verarbeitung der Kundendaten innerhalb der EU nach Microsofts „EU Data Boundary“-Zusage für Azure. Zertifizierungen: ISO/IEC 27001, 27017, 27018, SOC 2, BSI C5. DPA liegt dem Auftragsverarbeiter vor und wird auf Anfrage bereitgestellt.

Unterauftragsverarbeiter	Anschrift	Gegenstand und Art der Verarbeitung	Ort der Verarbeitung	Vertrag und Garantien nach Kapitel V DSGVO
STRATO GmbH	Otto-Ostrowski-Straße 7, 10249 Berlin, Deutschland	Versand von System-E-Mails (SMTP-Relay über das E-Mail-Postfach des Auftragsverarbeiters)	Deutschland	Anbieter mit Sitz in Deutschland (IONOS-Gruppe). Vereinbarung zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO mit STRATO (Version 3.6, abgeschlossen am 24.09.2026). Für den E-Mail-Dienst setzt STRATO laut seiner Subunternehmerliste Dienstleister in Deutschland ein (IONOS SE, Montabaur: Betrieb der Plattform; Elevenlabs GmbH, Berlin: Spamfilter); die dort für andere STRATO-Produkte genannten Drittländerdienstleister (Mail-Archivierung, Malware-Scans für Webhosting) werden vom Auftragsverarbeiter nicht genutzt. E-Mails enthalten Empfängername, E-Mail-Adresse und Links, keine Schülerdaten.

Keine Unterauftragsverarbeitung liegt vor bei: GitLab (Quellcodeverwaltung und Build-Pipeline; verarbeitet keine personenbezogenen Daten des Verantwortlichen), Microsoft Corporation als Konzernmutter (kein eigener Vertragspartner; siehe Garantien oben).

Änderungshistorie

Version	Änderung
2026-09	Fehlermonitoring-Dienst Sentry (Functional Software, Inc., USA) und externe Schriften-/Icon-Bereitstellung (rsms.me, fontawesome.com) aus der Anwendung entfernt; Schriften werden selbst gehostet. STRATO als E-Mail-Dienstleister ergänzt. Microsoft-Angaben um DPA, Region und Garantien konkretisiert.
2025-02 (Altfassung)	Microsoft Ireland Operations Limited (Azure), Standorte Frankfurt, Berlin