

Vertrag über die Auftragsverarbeitung
personenbezogener Daten nach EU Datenschutz-
Grundverordnung (AV-Vertrag)

Schulname
(BSN)

.....
Auftraggeber

und

.....
SenBildJugFam, Berlin, vertreten durch eGovernment@School

Auftragnehmer

1 Einleitung, Geltungsbereich, Definitionen

- (1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
- (2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
- (3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung (DSGVO) zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen:

- (1) Der Auftragnehmer (AN) verarbeitet personenbezogene Daten im Auftrag des Auftraggebers (AG). Der Auftrag umfasst Folgendes:

Der Auftragnehmer betreibt eine Windows-Terminal-Server-Farm unter Citrix, welche die Anwendungen für Schulverwaltungen in Berlin zur Verfügung stellt. Die erforderlichen Daten werden auf Servern des im Auftrag des Auftragnehmers in einem Rechenzentrum in Berlin (ITDZ) gespeichert und verarbeitet. Diese Server werden in einem Rechenzentrum in Berlin betrieben.

Auf die Daten wird über den Citrix-Receiver als Browser-Plugin bzw. installiertes Programm zugegriffen.

- (2) Die Schule (AG) verarbeitet als verantwortliche Stelle zum Zweck der Erfüllung ihrer allgemeinen Verwaltungsaufgaben personenbezogene Daten, die in der jeweils geltenden Fassung des Berliner Schulgesetzes und den abgeleiteten Verordnungen wie der Schuldatenverordnung, der Grundschulverordnung usw. festgelegt sind. Von der Datenverarbeitung betroffen sind u. a. Lehrkräfte, Schülerinnen und Schüler und deren Erziehungsberechtigte.
- (3) Die Datenerhebung erfolgt durch Vertreter der Schulen oder über einen Import von Daten (Stammdaten, Stundenpläne etc.), der vom Auftraggeber bereitgestellt wird.
- (4) Für die Schulverwaltungen werden folgende Softwareprodukte/Fachverfahren zur Verfügung gestellt: Stundenplanverwaltungsprogramm (Untis), Softwareprodukt zur Verwaltung von Schülerdaten (Berliner LUSD, Magellan, ...), MS Office 2010 mit Outlook sowie ReLiV. Es ist möglich, dass besondere Anforderungen an einzelnen Schulen ein zusätzliches Softwareprodukt erfordern.
- (5) Mit dem Fachverfahren Berliner LUSD (Lehrer- und Schülerdatenbank) stellt die Senatsverwaltung für Bildung, Jugend und Familie (AN) dem AG über eine zentrale, mandantenfähige Datenbank Anwendungen zur Verarbeitung seiner internen Schulverwaltungsdaten zur Verfügung.
Art und Umfang der Daten, die zum genannten Zweck in den Datenverarbeitungsprogrammen/ Fachverfahren (LUSD, Untis, ...) verarbeitet werden, sind dem Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 Datenschutzgrundverordnung zu entnehmen.

2.2 Dauer und Kündigung des Auftrags

Die Verarbeitung beginnt voraussichtlich am und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags durch eine Partei.

- (1) Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit der Frist von 30 Tagen gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.
- (2) Der Auftragnehmer kann diese Vereinbarung jederzeit kündigen, wenn der Auftraggeber gegen geltendes Datenschutzrecht oder andere Rechtsvorschriften verstoßen hat. Er hat zuvor den erfolglosen Ablauf einer zur Abhilfe bestimmten angemessenen Frist abzuwarten.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1 Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

Die Verarbeitung dient folgendem Zweck: Wahrnehmung und Durchführung von Schulverwaltungsaufgaben.

3.2 Art der Daten

Die Angabe zur Art der Daten erfolgt in **Anlage 3**.

3.2.1 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Schülerinnen und Schüler der Schule
- Erziehungsberechtigte und Bevollmächtigte
- Lehrkräfte und weiteres schulisches Personal, z.B. Erzieherinnen und Erzieher
- Mitarbeiter von Kooperationspartnern

4 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
- (2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- (3) Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (4) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

- (5) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
- (6) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht werden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
- (7) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
- (8) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (9) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
- (10) Der behördliche Datenschutzbeauftragte des Auftragnehmers ist

Herr Jan-Gerd Henze, behördlicher Datenschutzbeauftragter, 90227-6361

(Name, Organisationseinheit, Funktion, Telefon)

- (11) In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
- (12) Der Auftragnehmer sichert die auftragsgemäße Verarbeitung der personenbezogenen Daten zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Dem Auftragnehmer obliegt die Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz der überlassenen Daten und der dazu notwendigen Anwendung und Systeme, soweit dies in seinem Einflussbereich oder dem seiner Subunternehmer liegt.
- (13) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- (14) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und dieser Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme.
- (15) Ersatzweise kann der Auftragnehmer auch geeignete Testate, zum Beispiel die Zertifizierung nach BSI-Grundschutz, verlangen.

- (16) Der Auftragnehmer nimmt keine Änderung an den gespeicherten Daten vor.
- (17) Die Daten werden täglich auf ein Backupmedium in einem anderen Brandabschnitt gespeichert.
- (18) Der Auftragnehmer verpflichtet sich, den Auftraggeber bei Auskunftersuchen durch Betroffene gemäß Artikel 15 DSGVO unter Berücksichtigung von § 24 BlnDSG und der Aufklärung von Sicherheitsvorfällen im Rahmen seiner Möglichkeiten zu unterstützen.
- (19) Nach Beendigung des Auftragsdatenverarbeitungsauftrags hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen oder zu zerstören. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.
- (20) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR.
- (21) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.
- (22) Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.
- (23) Der Auftragnehmer versichert, Kenntnis über die anzuwendenden Rechtsvorschriften zu haben.

5 Technische und organisatorische Maßnahmen

- (1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
- (2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
- (3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
- (4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
- (5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
- (6) Die Verarbeitung von Daten in Privatwohnungen ist ausgeschlossen.
- (7) Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an den IT-Systemen durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der

Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Pflege von IT-Systemen durchzuführen.

Nähere Ausführungen des noch abzuschließenden Betriebsvertrages nach § 26 BlnDSG i. V. m. Art. 28, DSGVO (Auftragsverarbeiter) und Art. 32 DSGVO (Sicherheit in der Verarbeitung) werden zukünftig in einer neuen Anlage beschrieben.

- (8) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.
- (9) Der Auftraggeber ist berechtigt, regelmäßige Kontrollen zur Wirksamkeit der Maßnahmen durchzuführen. Die Wirksamkeit kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren nachgewiesen werden.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

- (1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- (2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

- (1) Die Beauftragung von Subunternehmern ist zugelassen. Die Kontrollrechte des Auftraggebers dem Auftragnehmer gegenüber bestehen dann in gleicher Weise gegenüber dem Subunternehmer.
- (2) Die Zustimmung zur Beauftragung von Subunternehmern ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
- (3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
- (4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- (5) Der Auftragnehmer hat im Falle der Beauftragung von weiteren Subunternehmern vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber diesen Subunternehmern gelten und überprüft die Einhaltung dieser Pflichten regelmäßig. Insbesondere hat er darauf zu achten, dass die Datenverarbeitung des Subunternehmers in der Bundesrepublik Deutschland stattfindet und der Auftraggeber Kontrollrechte im Rahmen der dort beauftragten Leistungen gegenüber dem Subunternehmer geltend machen kann. Die Weiterleitung von Daten ist erst nach Einwilligung des Auftraggebers zulässig.
- (6) Der Auftragnehmer gewährleistet eine Protokollierung der Systemleistungen, insbesondere wenn Dritte auf das DV-System des Auftragnehmers zugegriffen haben (Fernwartung).

- (7) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
- (8) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.
- (9) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen.
- (10) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.
- (11) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung (außer Fernwartung) und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8 Rechte und Pflichten des Auftraggebers

- (1) Für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.
- (2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
- (3) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
Weisungsberechtigte Personen werden in **Anlage 4** angegeben.
- (4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (5) Der Auftraggeber ist verpflichtet, alle im Rahmen dieses Auftragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.
- (6) Der Auftraggeber kann in regelmäßigen Abständen die Einhaltung der technischen und organisatorischen Maßnahmen vor Ort überprüfen. Der Auftragnehmer ist dabei rechtzeitig vorab zu informieren.
- (7) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den

Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
 - a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- (2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftrags erledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
- (3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- (4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

10 Weisungen

- (1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- (2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in **Anlage 3**.
- (3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
- (4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- (5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

- (1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 1.
- (2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
- (3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
- (4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12 Vergütung

Eine Vergütung des Auftragnehmers erfolgt nicht, weil SenBildJugFam als übergeordnete Behörde handelt.

13 Haftung

Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haftet die Senatsverwaltung für Bildung.

14 Sonderkündigungsrecht

- (1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
- (2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
- (3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.
- (4) Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Auftraggeber entstehen.

15 Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine

Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

- (2) Für Nebenabreden ist die Schriftform erforderlich.
- (3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. An die Stelle der unwirksamen Bestimmung soll diejenige wirksame Regelung treten, deren Wirkungen der datenschutzrechtlichen Zielsetzung am nächsten kommen, die die Parteien der Vereinbarung mit der unwirksamen Bestimmung verfolgt haben.

Unterschriften

Berlin _____, den _____
Ort Datum

Berlin _____, den _____
Ort Datum

Auftraggeber

Auftragnehmer

Anlage 1 – Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Für die Vernichtung von Datenträgern gemäß DIN 66399 gilt Schutzklasse 1.

Beschreibung der technischen und organisatorischen Maßnahmen des ITDZ Dienstleistungszentrums Berlin.

Wir bestätigen, dass wir als Auftragnehmer im Sinne von Artikel 28 DSGVO personenbezogene Daten ausschließlich nach den mit Ihnen getroffenen Vereinbarungen verarbeiten. Wir gewährleisten als Auftragnehmer im Bereich der auftragsgemäßen Verarbeitung von Daten die Einhaltung der jeweils aktuellen gesetzlichen Bestimmungen zum Datenschutz.

Darüber hinaus bestätigen wir die Gewährleistung der folgenden technischen und organisatorischen Maßnahmen im Sinne von Artikel 32 DSGVO:

- Vertraulichkeit

Unbefugten ist der Zugang zu unseren Datenverarbeitungsanlagen durch adäquate Absicherung der Data-Center, technische Zutrittskontrollen, Festlegung der berechtigten Personen und deren Sicherheitsüberprüfung sowie Schlüsselverzeichnisse, verwehrt. Darüber hinaus können unsere Datenverarbeitungssysteme nicht von Unbefugten genutzt werden. Um dies zu gewährleisten, wurden folgende Maßnahmen getroffen: Zugangsschutz, Passwortschutz, Verschlüsselung der zu übertragenden Informationen und ausschließliche Nutzung sicherer Übertragungswege. Die Zugriffskontrolle für unsere Mitarbeitenden ist im Rahmen unseres Berechtigungskonzepts dergestalt beschränkt, dass jeder Mitarbeitende nur auf diejenigen Verarbeitungsprozesse Einfluss nehmen kann, welche für seine Aufgabenerledigung erforderlich sind. Darüber hinaus können personenbezogene Daten der Auftraggeber nicht gelesen, kopiert, verändert oder entfernt werden. Ferner sind Firewall – Systeme, Passwortschutz und ein Login-System im Einsatz.

- Integrität

Bei der elektronischen Weitergabe oder während ihres Transports sowie der Speicherung können personenbezogene Daten nicht unbefugt kopiert, verändert oder entfernt werden. Dies wird gewährleistet durch Verschlüsselung, Regelung des Kommunikationsverkehrs, Login oder die Nutzung verschlossener Behältnisse beim Transport. Durch regelmäßige Plausibilitätskontrollen wird gewährleistet, dass Ihre Daten vollständig zur Verarbeitung gelangen.

- Verfügbarkeit

Wir gewährleisten, dass die von uns im Auftrag verarbeiteten Daten jederzeit für den Auftraggeber verfügbar sind. Sie sind ferner geschützt gegen zufällige Zerstörung oder Verlust. Dies erfolgt durch ein permanentes Backup sowie adäquate Infrastrukturmaßnahmen, gemäß dem zugrundeliegenden Sicherheitskonzept für die Data – Center des ITDZ Berlin.

- Authentizität
Eine unzulässige Zusammenführung von Daten außerhalb deren Zweckbindung wird durch die technische Gestaltung der von uns verwendeten Programme ausgeschlossen.
- Revisionsfähigkeit
Durch Protokollierungssysteme wird festgehalten, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies wird sichergestellt durch die Verwendung von Sicherungssoftware, unser Berechtigungskonzept sowie Login – Regelungen.
- Transparenz
Durch eine umfangreiche Protokollierung von Bearbeitungs- und Administratortätigkeiten wird eine vollständige Nachvollziehbarkeit gewährleistet. Die Auswertung von Logdateien ist jederzeit kurzfristig möglich.

Wir berechtigen Sie als Auftraggeber, jederzeit die Einhaltung der Vorschriften über den Datenschutz und der von Ihnen uns gegenüber getroffenen Weisungen zu überprüfen.

Wir bestätigen, dass das durch uns mit der Verarbeitung der von Ihnen bereitgestellten personenbezogenen Daten betraute Personal datenschutzrechtlich unterwiesen und auf das Datengeheimnis verpflichtet worden ist.

Wir bestätigen, dass unser Unternehmen über einen schriftlich bestellten, fachkundigen behördlichen Datenschutzbeauftragten gemäß § 4 BlnDSG verfügt.

Wir verpflichten uns generell, die Vertraulichkeit der uns überlassenen und zur Kenntnis gelangten Informationen zu wahren.

Der Auftragnehmer führt zur Gewährleistung der Funktionalität des Systems Wartungs- und Supportarbeiten aus. Hierbei stellt er sicher, dass

1. nur dafür autorisiertes Personal die Wartung vornimmt, welches schriftlich zur Verschwiegenheit verpflichtet wurde,
2. jeder Wartungsvorgang nur mit Wissen und Wollen der speichernden Stelle erfolgt,
3. personenbezogene Daten im Rahmen der Wartung nicht unbefugt entfernt oder
4. übertragen werden,
5. alle Wartungsvorgänge während der Durchführung kontrolliert werden können,
6. alle Wartungsvorgänge nach der Durchführung nachvollzogen werden können,
7. verhindert wird, dass bei der Wartung Programme unbefugt aufgerufen werden können, die für die Wartung nicht benötigt werden,
8. verhindert wird, dass bei der Wartung Datenverarbeitungsprogramme unbefugt verändert werden können und
9. die Wartung so organisiert und gestaltet wird, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Für die Wartung sind folgende Punkte grundsätzlich zu berücksichtigen:

1. Art und Umfang der Wartung:
 - Wartung und Pflege der Serversysteme, Clients, IT-Infrastruktur und Transportnetze
 - Wartung und Pflege der Softwareprodukte
 - Unterstützung der Benutzer durch Fernwartung

2. Rechte und Pflichten zwischen Auftraggeber und Auftragnehmer:
 - Siehe 4, 8 und 9 dieser Vereinbarung
3. Protokollierung der Wartungstätigkeiten durch den Auftragnehmer und Pflicht des Auftragnehmers, Weisungen des Auftraggebers zum Umgang mit den Daten auszuführen,
4. wird auf personenbezogene Daten zugegriffen, werden diese ausschließlich für den Zweck der Wartung verwendet,
5. es wird sichergestellt, dass ohne Zustimmung des Auftraggebers, durch den Auftragnehmer keine Daten an andere Stellen übermittelt werden,
6. beim Auftragnehmer anfallenden Daten werden nach Abschluss der Wartungsarbeiten gelöscht,
7. für die Fernwartung wird das Rückrufverfahren verbindlich festgelegt,
8. Anwesenheit des Benutzers ist bei der Fernwartung möglichst sicherzustellen,
9. personenbezogene Daten werden auf dem Übertragungsweg nach dem jeweiligen Stand der Technik verschlüsselt übertragen.

Anlage 2 – Zugelassene Subdienstleister

- a. **ITDZ Berlin,**
Berliner Str. 112 – 115, 10713 Berlin

ITDZ stellt die zentrale Rechnerinfrastruktur für die Terminalserverumgebung zur Verfügung. Zusätzlich betreibt das ITDZ diese Infrastruktur.

- b. **CANCOM on line GmbH Berlin,**
Granatenstr. 19, 13409 Berlin

CANCOM on line GmbH betreibt im Auftrag der SynTAGit GmbH das Client Management für die lokalen Thin Clients an den Schulen. Dort werden in der Regel nur Gerätedaten verwaltet. Allerdings kommt es zum Beispiel im Rahmen des Zertifikatsmanagements zur Verarbeitung persönlicher Daten.

- c. **SynTAGit GmbH,**
Stromstraße 38, 10551 Berlin

SynTAGit GmbH übernimmt in großem Umfang den Rollout der Zentralen Schulverwaltungsumgebung von der Planung über die Beratung bis zur Durchführung. Weiterhin übernimmt SynTAGit die Entwicklung von Betriebsstrukturen im Rahmen des Projektes.

- d. **]init[Berlin,**
Köpenicker Str. 9, 10997 Berlin

]init[verantwortet die Weiterentwicklung des Softwareproduktes Berliner LUSD und den Betrieb der Infrastruktur für die Berliner LUSD in Kooperation mit dem ITDZ.

- e. **topdev Erfurt**
Am Seegraben 2,99099 Erfurt

topdev übernimmt im Auftrag von]init[die Weiterentwicklung der Berliner LUSD. Zusätzlich übernimmt topdev den 3rd-Level-Support und kann dabei evtl. Daten verarbeiten.

- f. **SINC GmbH**
Hufelandstr. 22, 10407 Berlin

SINC betreut im Auftrag der]init[die Infrastruktur der Berliner LUSD und verantwortet die Migration der Daten in die LUSD.

Anlage 3 – Art der Daten

Kategorien betroffener Personen	Art der Daten
Schüler*innen	Stammdaten, Adressdaten, Kontaktdaten, Leistungsdaten, Zeugnisdaten, Sozialdaten (BUT)
Lehrkräfte, Erzieher*innen, sonstige schulische Mitarbeiter*innen	Personaldaten, Kontaktdaten; Leistungsdaten
Mitarbeiter*innen (Schulverwaltung)	Personaldaten, Kontaktdaten; Leistungsdaten
Eltern/ Erziehungsberechtigte	Stammdaten, Adressdaten, Kontaktdaten
Betriebe	Stammdaten, Adressdaten, Kontaktdaten

Anlage 4 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Weisungsempfangsberechtigte Personen des Auftragnehmers:

Für den Bereich	Schule
Schulleiterin/Schulleiter	<i>Name</i> <i>Telefon</i> <i>E-Mail Adresse</i>
Stellvertretende Schulleiterin/Stellvertretender Schulleiter	<i>Name</i> <i>Telefon</i> <i>E-Mail Adresse</i>

Datenschutzbeauftragter des Auftragsgebers:

Für den Bereich	Schule
Schulische Datenschutzbeauftragte/Schulischer Datenschutzbeauftragter	<i>Name</i> <i>Telefon</i> <i>E-Mail Adresse</i>

Für den Bereich	Senatsverwaltung für Bildung, Jugend und Familie
Zentrale Schulverwaltungs- umgebung (ZSVU)	<i>Name</i> Kay Hansen <i>Position</i> Gesamtprojektleiter <i>Stellenzeichen</i> I eGov <i>Telefon</i> 90227-5630 <i>E-Mail Adresse</i> kay.hansen@senbjf.berlin.de
ZSVU – als Stellvertreter	<i>Name</i> Horst Daniel <i>Position</i> Teilprojektleiter ZSVU <i>Stellenzeichen</i> I eGov 2 <i>Telefon</i> 90227-5873 <i>E-Mail Adresse</i> horst.daniel@senbjf.berlin.de