Schulsuite

Vertrag zur Auftragsverarbeitung

STAND NOVEMBER 2026

Dieser Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO gilt zwischen den Kunden der TK-Schulsoftware GmbH & Co. KG als Verantwortlichen (**Auftraggeber**) und der TK-Schulsoftware GmbH & Co. KG, Rosenwiesstr. 17, 70567 Stuttgart (**Auftragsverarbeiter**).

Für den Abschluss des AVV füllt der Auftraggeber die Felder in **Anlage 2** aus: die Angaben zur verantwortlichen Stelle, zu ihrem Datenschutzbeauftragten und zu den weisungsberechtigten Personen. Dafür steht der Vertrag als PDF zum Ausfüllen bereit.

Inhalt

Vertrag ... **3**
1 Anwendungsbereich ... 3
2 Begriffsbestimmung ... 3
3 Konkretisierung des Auftragsinhalts ... 3
4 Dauer des Vertrags ... 3
5 Sonstiges ... 3
Anlage 1 · Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Auftragsverarbeitung ... **4**
1 Pflichten des Auftragsverarbeiters ... 4
2 Pflichten des Auftraggebers ... 5
3 Kontrollpflichten ... 5
4 Unterauftragsverhältnisse ... 6
5 Informationspflicht ... 6
6 Sonstiges ... 6
Anlage 2 · Dokumentation der Verarbeitungstätigkeit ... **7**
1 Angaben zum Auftragnehmer ... 7
2 Angaben zur verantwortlichen Stelle / zum Auftraggeber ... 7
3 Kategorien der Verarbeitung ... 7
4 Datenübermittlung in Drittstaaten / internationale Organisationen ... 8
5 Technische und organisatorische Maßnahmen / Datenschutz ... 8
Anlage 3 · Datenschutz, Sicherheitskonzept und Katalog der getroffenen Technischen und Organisatorischen Maßnahmen ... **9**
1 Zutrittskontrolle ... 9
2 Zugangskontrolle ... 9
3 Zugriffskontrolle ... 10
4 Weitergabe- / Transportkontrolle ... 10
5 Eingabekontrolle ... 10
6 Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit b EU-DSGVO) ... 10
7 Trennungskontrolle ... 11
8 Datenträgerkontrolle ... 11
9 Auftragskontrolle ... 11
10 Speicherkontrolle ... 11
11 Benutzerkontrolle ... 11
12 Wiederherstellbarkeit ... 12
13 Belastbarkeit und Zuverlässigkeit (Art. 32 Abs. 1 lit. b EU-DSGVO) ... 12
14 Datenintegrität (Art. 32 Abs. 1 lit. B EU-DSGVO) ... 12
15 Übertragungskontrolle ... 12
Anlage 4 · Subunternehmer zum Auftrag gemäß Art. 28 DSGVO ... **13**

Vertrag

Präambel
Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsdatenverarbeitungsverhältnis gemäß Art. 28 Datenschutzgrundverordnung (DSGVO) eingegangen. Um die Rechte und Pflichten aus dem Auftragsdatenverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

Folgende Anlagen sind Bestandteil des Vertrags:
1. Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Auftragsverarbeitung
2. Dokumentation der Verarbeitungstätigkeit
3. Datenschutz, Sicherheitskonzept und Katalog der getroffenen Technischen und Organisatorischen Maßnahmen
4. Subunternehmer zum Auftrag gemäß Art. 28 DSGVO

1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Auftraggeber die gemäß Art. 4 Nr. 7 DSGVO Verantwortlicher ist

2 Begriffsbestimmung

Diese Vereinbarung bezieht sich nur auf die Durchführung der technischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach einem vom Auftraggeber vorgegebenen Algorithmus (Auftragsdatenverarbeitung). Eine inhaltliche Aufgabenübertragung wird mit dieser Vereinbarung nicht getroffen.

3 Konkretisierung des Auftragsinhalts

(1) Der Gegenstand und die Dauer der Auftragsdatenverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten sind in der Leistungsvereinbarung niedergelegt.

(2) Folgenden Datenarten oder -kategorien sind Gegenstand der Erhebung, Verarbeitung und/oder Nutzung durch den Auftragnehmer:
- siehe Anhang 2 Pkt. 3

(3) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten Betroffenen umfasst:
- Kunden, Schülerinnen und Schüler und deren Erziehungsberechtigte, insbesondere Eltern, und Angehörige bzw. Personen aus dem persönlichen Umfeld der Schüler
- ehemalige Schülerinnen und Schüler
- ehrenamtlich tätige Personen
- Vereinsmitglieder und Genossen
- Lehr- und Erziehungskräfte, Auszubildenden und Praktikanten
- sonstige Beschäftigte und Mitarbeiter: Schulverwaltung, Buchhaltung, Haustechnik
- Förderer der Schule sowie deren Organisationen
- Funktionsträger: Vorstand, Geschäftsführer u.a.

4 Dauer des Vertrags

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

5 Sonstiges

Änderungen oder Ergänzungen dieses Vertrages bedürfen nach Art 28 Abs. 9 EU-DSGVO der Schriftform. Gleiches gilt für die Aufhebung des Schriftformerfordernisses selbst.

Sollte eine Regelung dieses Vertrages nichtig sein oder werden oder sich eine Lücke herausstellen, bleibt der Vertrag im Übrigen gültig. Es soll das gelten, was die Parteien vereinbart hätten, wenn die Unwirksamkeit oder die Lücke bekannt gewesen wäre.

Die Vertragsparteien prüfen dann gemeinsam, ob Änderungen oder Ergänzungen dieses Vertrages erforderlich sind. Kommen sie zu dem Ergebnis, dass eine Änderung oder Ergänzung des Vertrages erforderlich ist, oder wird von einer Vertragspartei eine Änderung oder Ergänzung dieses Vertrages beantragt, so nehmen sie unverzüglich Verhandlungen auf.

Anlage 1 · Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Auftragsverarbeitung

1 Pflichten des Auftragsverarbeiters

1.1. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. So trifft er alle technischen und organisatorischen Maßnahmen zur angemessenen Sicherung der Daten der Auftraggeber vor Missbrauch und Verlust, die den datenschutzrechtlichen Anforderungen (Art. 32 EU-DSGVO) entsprechen.

Art. 32 Abs. 1 EU-DSGVO regelt hierzu:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

1.1.1. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
1.1.2. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
1.1.3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
1.1.4. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Der Auftragsverarbeiter unternimmt zudem Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Der Auftragsverarbeiter unternimmt zudem Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen so gesichert sind, dass diese Daten nicht ohne aktives Eingreifen einer unbestimmten Zahl von natürlichen anderen Personen zugänglich gemacht werden.

1.2. Der Auftragsverarbeiter stellt dem Auftraggeber zu Beginn dieses Vertrages in Anlage 3 ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung. Dieses Konzept beschreibt nach Art. 32 Abs. 2 EU-DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Ferner sind die Voreinstellungen darzustellen, die gewährleisten, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich

im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

Änderungen in diesem Konzept sind dem Auftraggeber vorher so rechtzeitig anzuzeigen, dass diesem genügend Zeit bleibt, um auf Änderungen entsprechend reagieren zu können. Die jeweils aktuelle Fassung des Konzepts wird dem Auftraggeber zur Kenntnisnahme und Zustimmung übersandt.

1.3. Der Auftragsverarbeiter stellt dem Auftraggeber die für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO programmspezifischen notwendigen Angaben zur Verfügung (Anlage 2). Die Auftraggeber sollten in ihrem Verzeichnis von Verarbeitungstätigkeiten auf das gesamte Vertragswerk zur Auftragsverarbeitung verweisen. Ferner führt der Auftragsverarbeiter selbst ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung nach Art. 30 Abs. 2 EU-DSGVO. Dieses Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Der Auftragsverarbeiter stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

1.4. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

1.5. Der Auftragsverarbeiter teilt dem Auftraggeber die Kontaktdaten des betrieblichen oder behördlichen Datenschutzbeauftragten mit.

1.6. Der Auftragsverarbeiter unterrichtet die Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes (z. B. technischer Art), im Falle einer Verletzung des Schutzes personenbezogener Daten oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (Art. 33 Abs.2 EU-DSGVO).

1.7. Datensicherungen sind vom Auftragsverarbeiter sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragsverarbeiter ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Datensicherungen übernimmt der Auftragsverarbeiter in regelmäßigen Abständen, mindestens alle 5 Jahre.

1.8. Die Verarbeitung der Daten findet überwiegend im Gebiet der Bundesrepublik Deutschland statt. In Einzelfällen erfolgt die Verarbeitung der Daten in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraums. Eine Verarbeitung in Drittstaaten findet nicht statt.

1.9. Nach Wahl des Auftraggebers werden die personenbezogenen Daten zurückgegeben oder gelöscht, sowie vorhandene Kopien gelöscht, soweit keine gesetzliche Aufbewahrungspflicht besteht.

2 Pflichten des Auftraggebers

2.1. Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei Nutzung der IT-Services Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

2.2. Der Auftraggeber, als für den Datenschutz Verantwortlicher, ist für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO zuständig.

2.3. Dem Auftraggeber obliegt die Einhaltung der in den Artikeln 32 bis 36 EU-DSGVO genannten Pflichten. Der Auftragsverarbeiter wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützen.

Ferner obliegen dem Auftraggeber die aus den Artikeln 15 bis 21 EU-DSGVO resultierenden Pflichten gegenüber den Betroffenen, insbesondere über Auskunft, Berichtigung und Löschung. Der Auftragsverarbeiter wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III EU-DSGVO genannten Rechte der betroffenen Person nachzukommen.

3 Kontrollpflichten

3.1. Der Auftraggeber überzeugt sich in regelmäßigen Abständen von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters und kann sich dazu vom Auftragsverarbeiter deren Einhaltung schriftlich bestätigen lassen. Der Auftraggeber oder dessen Beauftragter kann sich hierüber auch vor Ort selbst überzeugen. Der Auftragsverarbeiter räumt dem Auftraggeber nach angemessener Vorankündigung oder dessen Beauftragten insofern ein Zutrittsrecht während der üblichen Arbeitszeit für die Räumlichkeiten und Einrichtungen des Auftragsverarbeiters ein.

Der Nachweis dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Vorgaben der EU-DSGVO erfolgt, kann der Auftragsverarbeiter auch durch Vorlage einer Bestätigung eines anerkannten lizenzierten Auditors, dass genehmigte Verhaltensregeln gemäß Artikel 40 EU-DSGVO oder ein genehmigtes Zertifizierungsverfahrens gemäß Artikel 42 EU-DSGVI durch den Auftragsverarbeiter eingehalten werden, erbringen.

Der Auftragsverarbeiter muss dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellen sowie Überprüfungen einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die EU-DSGVO oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt.

Der Auftraggeber hat gegenüber dem Auftragsverarbeiter Weisungsbefugnis hinsichtlich der Verarbeitung der personenbezogenen Daten. Der Auftragsverarbeiter erteilt dem Auftraggeber die hierfür notwendigen Auskünfte und ermöglicht die Überprüfung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen in geeigneter Weise. Im Falle einer Überprüfung durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg gilt dies entsprechend. Der Auftragsverarbeiter gestattet dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit gemäß Art. 58 Abs. 1 lit. e EU-DSGVO jederzeit Zutritt zu den Räumen, in denen er Daten des Auftraggebers im Auftrag verarbeitet, und Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung dessen Aufgaben notwendig sind.

4 Unterauftragsverhältnisse

4.1. Dem Auftragsverarbeiter wird allgemein gestattet, Subunternehmer als Unterauftragnehmer in Anspruch zu nehmen. Der Auftragsverarbeiter muss dies gegenüber dem Auftraggeber vorab anzeigen. Der Auftraggeber kann dagegen während einer Frist von 14 Tagen Einspruch erheben. Mit dem Subunternehmer ist durch den Auftragsverarbeiter eine Vereinbarung nach Maßgaben des Art. 28 Abs. 2 bis 4 EU-DSGVO abzuschließen.

4.2. Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Auftraggeber und dem Auftragsverarbeiter gemäß Art. 28 Abs. 3 EU-DSGVO festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

4.3. Der Auftragsverarbeiter verwendet für die Datenspeicherung Server in einem Rechenzentrum.

5 Informationspflicht

Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortliche Stelle“ im Sinne der EU-DSGVO liegen.

6 Sonstiges

Die Vertragspartner vereinbaren, die datenschutzrechtlichen Bestimmungen einzuhalten und ihre Mitarbeiterinnen und Mitarbeiter hierzu zu verpflichten.

Anlage 2 · Dokumentation der Verarbeitungstätigkeit

1 Angaben zum Auftragnehmer

AUFTRAGNEHMER	DATENSCHUTZBEAUFTRAGTER
TK-Schulsoftware GmbH & Co. KG Rosenwiesstr. 17 70567 Stuttgart Telefon: 0711-50 87 00 00 info@tk-schulsoftware.de https://www.tk-schulsoftware.de/impressum	Gabriele Knödler-Bittner Datenschutzbeauftragte unternehmensentwicklung.plus Datenschutzberatung Brommerstrasse 24 70563 Stuttgart datenschutz@tks.eu

Weisungsempfänger beim Auftragnehmer sind:

VORNAME, NAME	ORGANISATIONSEINHEIT	KONTAKT
Tobias Knipping	Geschäftsführung	knipping@tk-schulsoftware.de
Daniel Laiblin	Geschäftsführung	laiblin@tk-schulsoftware.de

2 Angaben zur verantwortlichen Stelle / zum Auftraggeber

AUFTRAGNEHMER	DATENSCHUTZBEAUFTRAGTER

Weisungsberechtigte Personen des Auftraggebers sind:

VORNAME, NAME	ORGANISATIONSEINHEIT	KONTAKT

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. Vertreter mitzuteilen.

3 Kategorien der Verarbeitung

NR.	DATENKATEGORIEN	ZWECK
1.	Zugriffsprotokolle, Sitzungs-IDs	Unterstützung des Auftraggebers durch Fernwartung (TeamViewer)
2.	Zugriffsprotokolle, Sitzungs-IDs, Logdateien, IP-Adressen, Zugangsdaten (Account)	Pseudonymisierte statistische Auswertungen, Wartung und Pflege der Server
3.	Personalaktenführung/ Mitarbeiter-Stammdaten: Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohn- und Gehaltsdaten, Arbeitszeit, bisherige Tätigkeitsbereiche, Qualifikationen, Urlaubsdaten, Krankheitsdaten, Fehlzeiten	Falls durch den Auftraggeber in IPHIS erfasst, erfolgt die Verarbeitung im Falle von SaaS dauerhaft, zur Erbringung der vertraglich vereinbarten Dienstleistungen, andernfalls nur im Rahmen von konkret durch den Auftraggeber

NR.	DATENKATEGORIEN	ZWECK
4.	Arbeitszeugnisse mit Adressdaten, Leistungsdaten, Beurteilungsdaten u.a.	angeforderten Fernwartungs- und Dienstleistungszugriffen. Alle Daten die nicht in IPHIS hinterlegt werden können, werden nur im Rahmen des vom Auftraggeber konkret angeforderten Fernwartungs- und Dienstleistungs-Zugriffs und nur für die Dauer des jeweiligen Zugriffs verarbeitet, falls diese durch den Auftraggeber auf Systemen verarbeitet werden, auf die zugegriffen werden soll.
5.	Abmahnungen mit Adressdaten, Arbeitsverhalten, Leistungsdaten u.a.	
6.	Bewerbungsverfahren: Kontaktdaten, Qualifikationsdaten, Tätigkeiten u.a.	
7.	Telefondatenerfassung	
8.	Beschaffung, Einkauf sowie Finanzbuchhaltung	
9.	Antragsbearbeitung	
10.	Videoüberwachung	
11.	Vertragsstammdaten (Vertragsbeziehung, produkt- bzw. Vertragsinteresse)	
12.	Kundenkontaktdaten, Kundenhistorie (Erziehungsberechtigte, Schüler, Lieferanten und sonstige Vertragspartner) mit Adressdaten, Ansprechpartnern u.a.	
13.	Kundenumsatzdaten, Bonitätsdaten	
14.	Bewerber und Interessenten an der Schulaufnahme ihrer Kinder	
15.	Vertragsabrechnungs- und Zahlungsdaten	
16.	Planungs- und Steuerungsdaten	
17.	Verwaltungs- und Organisationsdaten	
18.	Auskunftsangaben (von Dritten, z.B. Auskunfteien oder aus öffentlichen Verzeichnissen)	
19.	E-Mail-Datenbank	
20.	Einscannen von betrieblichen Schriftstücken	
21.	Archivierung von Datenbeständen	
22.	Löschung von personenbezogenen Daten sowie Entsorgung von Datenträgern	
23.	Personenbezogene Daten für schulische Zwecke im Rahmen der Aufgabenerfüllung	
24.	Stundendaten als Einsatz für Lehrkräfte	
25.	Schülerverwaltung: Zeugnisse, Schulleistungsdaten, Schülerakte, Fehlzeiten- und Krankheitsdaten, Unterrichtsplanung u.a.	
26.	Kommunikationsdaten (z.B. Telefon, E-Mail)	
27.	Nutzungsprotokollierungen IT/Internet/E-Mail	
28.	Schulärztliche Untersuchungen	

4 Datenübermittlung in Drittstaaten / internationale Organisationen

Eine Datenübermittlung in Drittstaaten / an internationale Organisationen findet nicht statt.

5 Technische und organisatorische Maßnahmen / Datenschutz

Ergeben sich aus Anlage 3: Datenschutz, Sicherheitskonzept und Technische und Organisatorische Maßnahmen.

Anlage 3 · Datenschutz, Sicherheitskonzept und Katalog der getroffenen Technischen und Organisatorischen Maßnahmen

Nach Art. 32. Abs. 1 DS-GVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der mit ihr verbundenen Risiken geeignete technische und organisatorische Maßnahmen zutreffend, die allgemein wie folgt sichergestellt werden:

- **Pseudonymisierung personenbezogener Daten**
  In Daten für statistische- und Analysezwecke werden nur pseudonymisierte (d.h. durch ein Hashverfahren (SHA-512) geschützte) Referenzen auf den einzelnen Kunden bzw. Benutzer verwendet
- **Verschlüsselung personenbezogener Daten**
  Symmetrische oder asymmetrische Verschlüsselung
- **Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste**
  Eingabekontrolle, Absicherung von Berechtigungen, Protokollierungsmaßnahmen
  Zutritts-, Zugangs-, Zugriffs-, Weitergabe- und Trennungskontrolle
- **Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste**
  Verfügbarkeitskontrolle, Auftragskontrolle
  Leistbarkeit der Systeme auch bei punktuell oder dauerhaften hohen Belastungen von Verarbeitungen, insbes. der Speicher-, Zugriffs und Leitungskapazitäten
- **Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall**
  Backup-Konzept, redundante Datenspeicherung, Verfügbarkeit von Ersatzhardware
- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Daten**
  Entwicklung eines Sicherheitskonzeptes, Prüfung durch Datenschutzbeauftragten

Bei der Auswahl unserer Rechenzentrumsdienstleister achten wir darauf, dass diese mindestens ISO 27001-Zertifiziert sind und mindestens alle Anforderungen die in dieser Auftragsvereinbarung genannt werden erfüllen.

Im Einzelnen werden die technischen und organisatorischen Maßnahmen wie folgt gewährleistet und umgesetzt:

Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

1 Zutrittskontrolle

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

TECHNISCHE MASSNAHMEN	ORGANISATORISCHE MASSNAHMEN
• Manuelles Schließsystem • Sicherheitsschlösser, Türsicherung • Türen mit Knauf Außenseite	• Schlüsselregelung / Liste • Personenkontrolle beim Empfang • Sorgfältige Auswahl des Reinigungspersonals

2 Zugangskontrolle

Die Maßnahmen der Zugangskontrolle tragen der mittleren Risikowahrscheinlichkeit und der erhöhten Risikoschwere Rechnung.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

TECHNISCHE MASSNAHMEN	ORGANISATORISCHE MASSNAHMEN
• Automatische Sperrung der Endgeräte nach 5 Minuten Abwesenheit / Pausenschaltung • Verschlüsselung von Datenträgern mittels SHA-mit 512 Bit Schlüssellänge • Verschlüsselung von Smartphones	• Verwalten von Benutzerberechtigungen • Erstellen von Benutzerprofilen nach dem „Need-to-know“-Prinzip • Zentrale Passwortvergabe

TECHNISCHE MASSNAHMEN	ORGANISATORISCHE MASSNAHMEN
• Verschlüsselung von Notebooks/Tablets mittels hocheffizienter (sog. "military grade“) AES-Verfahren (FileVault, Bitlocker) • Antiviren-Software • Firewall (Hard- / Software) • Absicherung des Remotezugriffs mittels VPN • Intrusion Detection Systeme • Gesicherte WLAN-Netzwerke mittels WPA3	• Richtlinie „Sicheres Passwort“ (u.a. Mindestlänge) • Nutzung von 2FA für alle Administrator-Zugänge

3 Zugriffskontrolle

Der mittleren Risikowahrscheinlichkeit und der erhöhten Risikoschwere Rechnung tragende bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

TECHNISCHE MASSNAHMEN	ORGANISATORISCHE MASSNAHMEN
• Aktenvernichter • Physische Löschung von Datenträgern mittels Überschreiben • Protokollierung von Zugriffen auf Anwendungen (konkret bei der Eingabe, Änderung und Löschung von Daten) • Verschlüsselung der Daten bei Ablage (At-Rest) • Verschlüsselung der Daten bei der Datenübertragung (In-Transit) mittels 2048-Bit-SSL-Schlüssel	• Verwaltung der Rechte durch Systemadministrator • Minimale Anzahl an Administratoren • Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)

4 Weitergabe- / Transportkontrolle

Der niedrigen Risikowahrscheinlichkeit und niedrigen bis mittleren Risikoschwere angepasste Maßnahmen zur Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

TECHNISCHE MASSNAHMEN	ORGANISATORISCHE MASSNAHMEN
• Verschlüsselung / Tunnelverbindungen (VPN) • Protokollierung • Einsatz von Virenscannern	• Sicherer Upload von Daten / E-Mail-Verschlüsselung • Dokumentation der Empfänger der Daten • Festgelegte Transportwege beim Versand personenbezogener Daten in Papierform

5 Eingabekontrolle

Der niedrigen Risikowahrscheinlichkeit und niedrigen Risikoschwere angepasste Maßnahmen zur nachträglichen Überprüfbarkeit, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

TECHNISCHE MASSNAHMEN	ORGANISATORISCHE MASSNAHMEN
• Protokollierungs- und Auswertungssysteme • Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen	• Berechtigungskonzept • Aufbewahrung von Formularen, aus denen Daten übernommen worden sind

6 Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit b EU-DSGVO)

Maßnahmen zur Datensicherung (physikalisch / logisch) zur Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

TECHNISCHE MASSNAHMEN	ORGANISATORISCHE MASSNAHMEN
• Spiegelung von Festplatten, z.B. RAID-Verfahren • RAID-Systeme melden Plattenausfälle • Unterbrechungsfreie Stromversorgung (USV) • Virenschutz / Firewall • Feuerlöschgeräte in Serverräumen • Kurzfristige Verfügbarkeit von Ersatzsystemen • Resilienz: Aufrechterhaltung von Funktionen des Gesamtsystems, unabhängig von einer konkreten Gefahr	• Backup-Verfahren • Testen von Datenwiederherstellung • Regelmäßige Stress-/Belastungstests • IT-Notfallpläne

7 Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

TECHNISCHE MASSNAHMEN	ORGANISATORISCHE MASSNAHMEN
• Trennung von Produktiv- und Testsystemen • Physikalische Trennung (Systeme / Datenbanken / Datenträger) • Mandantenfähigkeit relevanter Anwendungen	• Steuerung über Berechtigungskonzept • Versehen der Datensätze mit Zweckattributen / Datenfeldern • Festlegung von Datenbankrechten

8 Datenträgerkontrolle

Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

- Sammlung von Daten in Papierform und deren Entsorgung in abschließbaren Containern
- Elektronische und optische Datenträger sowie magnetische Datenträger wie Festplatten werden gesondert gesammelt und datenschutzgerecht entsorgt (u.a. geschreddert oder mechanisch zerstört)

9 Auftragskontrolle

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragsverarbeiter zur Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsformular) Kriterien zur Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten, insbesondere Datensicherheit
- Vorherige und anschließend laufende Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters zur Wahrung des Datengeheimnisses
- Kontrolle der Vertragsausführung rechtswirksam vereinbart
- Sicherstellung der Vernichtung personenbezogener Daten nach Beendigung des Auftrags

10 Speicherkontrolle

Maßnahmen zur Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

- Benutzername und Kennwort
- Automatische Sperrung (Pausenschaltung)
- Sperrung des Accounts bei wiederholter Falschanmeldung
- Dokumentierte Prozesse bei der Nutzerverwaltung

11 Benutzerkontrolle

Maßnahmen zur Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

- Virenscanner mit automatischem Update und automatischer Verteilung an die Clients
- Home-Office Arbeitsplätze sind via VPN angebunden
- Administrative Firewalls
- Server für Zugriffe von außen stehen in einer DMZ

12 Wiederherstellbarkeit

Maßnahmen zur Gewährleistung, dass auftretende Fehlfunktionen gemeldet werden und dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

- Reserve Server stehen bei einem Ausfall zur Verfügung
- IT-Notfallpläne

13 Belastbarkeit und Zuverlässigkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

Maßnahmen zur Gewährleistung das alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

- RAID-Systeme melden Plattenausfälle in den Servern
- Robustheit: Reduzierung der Fehleranfälligkeit von einzelnen Komponenten eines Systems
- Resilienz: Aufrechterhaltung von Funktionen des Gesamtsystems, unabhängig von der konkreten Gefahr

14 Datenintegrität (Art. 32 Abs. 1 lit. B EU-DSGVO)

Maßnahmen zur Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktion des Systems beschädigt werden können.

- Schultz vor Manipulation der Daten (Angriffssicherheit); Message Authentication Code
- Schutz vor unbeabsichtigten Veränderungen durch Fehleingaben oder mechanische Defekte

15 Übertragungskontrolle

Maßnahmen zur Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- für die Übermittlungen von personenbezogenen Daten von und zu den Auftraggebern wird das Internet genutzt
- bei den Verbindungen werden VPN-Tunnelverbindungen genutzt
- Zugriff auf das Online-Kundencenter nur nach dokumentierter Authentifizierung möglich

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1 EU-DSGVO)

- Datenschutz-Management
- IT-Störungsmanagement
- Notfallplan, welcher periodisch evaluiert und an neue Bedrohungslagen angepasst wird
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-.GVO)
- Auftragskontrolle (Art. 28 DS.GVO); Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten
- Berechtigungskonzept, welches periodisch evaluiert und an neue Rollen und Risiken angepasst wird
- Löschbarkeit von Daten
- Wirksame Kontrollrechte

Anlage 4 · Subunternehmer zum Auftrag gemäß Art. 28 DSGVO

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende genehmigte Unternehmen:

UNTERNEHMEN	ANSCHRIFT	LEISTUNG
workBOXX-solutions GmbH	Jesuitenschloss 1, 79249 Merzhausen	IT-Systembetreuung
TRIARGOS GmbH	Jesuitenschloss 1, 79249 Merzhausen	Systemlösung
ALPHA Netzwerk GmbH	Jesuitenschloss 1, 79249 Merzhausen	Vertrieb
TRIARGOS ProBildung GmbH	Jesuitenschloss 1, 79249 Merzhausen	Vertrieb
Gridscale GmbH	Oskar-Jäger-Straße 173, 50825 Köln	Rechenzentrum
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Rechenzentrum
domainfactory GmbH	Oskar-Messter-Str. 33, 85737 Ismaning	Rechenzentrum
acomm GmbH	Bischof-von-Dinkel-Str. 12, 96231 Bad Staffelstein	Telefonanlage
bytemine GmbH	Im Technologiepark 4, 26129 Oldenburg	IT-Security
Heinlein Hosting GmbH	Schwedter Str. 9a, 10119 Berlin	Emailhosting
QuizzBox Sulutions GmbH	Möhringer Landstr. 5, 70563 Stuttgart	Online-Abstimmungen
Sendinblue GmbH	Köpenicker Str. 126, 10179 Berlin	Newsletter-Versand
TecArt GmbH	Fischmarkt 5, 99084 Erfurt	CRM-System
IONOS SE	Elgendorfer Str. 57 56410 Montabaur	Rechenzentrum
IONOS Cloud GmbH	Elgendorfer Straße 57, 56410 Montabaur	Rechenzentrum