

Auftragsverarbeitungsvereinbarung

Version: 11

Stand: 02.05.2023

Dokumenten ID: 1915224065

Inhaltsverzeichnis

Auftragsverarbeitungsvereinbarung (AVV).....	4
Vorwort	4
§ 1 Gegenstand und Dauer der Vereinbarung	4
§ 2 Art und Zweck der Verarbeitung, Art der Personenbezogenen Daten und Kategorien Betroffener	5
§ 3 Unterauftragsverarbeitungen.....	7
§ 4 Rechte, Pflichten und Weisungsbefugnisse des Kunden.....	7
§ 5 Pflichten des Auftragnehmers.....	7
§ 6 Mitteilungspflichten des Auftragnehmers.....	8
§ 7 Technische und Organisatorische Maßnahmen	8
§ 8 Verpflichtungen des Auftragnehmers nach Auftragende.....	9
§ 9 Haftung.....	9
§ 10 Aufbewahrungsfristen, Rechtswahl und Gerichtsstand	9
§ 12 Salvatorische Klausel.....	9
Anlagen.....	10
Anlage 1 der AVV - Unterauftragsverarbeiter	11
Unterauftragsverarbeiter mit Auftragsdatenverarbeitung innerhalb Deutschlands und der EU.....	11
Anlage 2 der AVV - TOM zur IT-Sicherheit	14
Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)	14
Zutrittskontrolle.....	14
Zugangskontrolle	14
Zugriffskontrolle.....	15
Trennung der Verarbeitung für verschiedene Zwecke.....	15
Integrität (Art. 32 Abs. 1 lit. b DSGVO).....	15
Eingabekontrolle.....	15
Weitergabekontrolle	16
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO).....	16

Verfügbarkeitskontrolle	16
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO).....	16
Auftragskontrolle	16
Weitere Maßnahmen	17
Anlage 3 der AVV - Gesetz über den Kirchlichen Datenschutz (KDG).....	18
Vorwort	18
Zusatzvereinbarung zum Vertrag Auftragsverarbeitung gemäß § 29 Gesetz über den Kirchlichen Datenschutz (KDG).....	18
Anlage 4 der AVV - Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz).....	19
Vorwort	19
Zusatzvereinbarung zum Vertrag gemäß § 30 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz).....	19
Anlage 5 der AVV - Datenschutzordnung der Israelitischen Religionsgemeinschaft Württembergs K.d.ö.R. (IRGW)	20
Vorwort	20
Zusatzvereinbarung zum Vertrag gemäß DO-IRGW.....	20
Anlage 6 der AVV - Datenschutzordnung Jüdische Gemeinde Frankfurt am Main K.d.ö.R.....	21
Vorwort	21
Zusatzvereinbarung zum Vertrag gemäß Datenschutzordnung der Jüdische Gemeinde Frankfurt am Main K.d.ö.R.....	21

Auftragsverarbeitungsvereinbarung (AVV)

zwischen
dem Kunden im Sinne der AGB
und
der edjufy Software GmbH als Auftragsverarbeiter (fortan Auftragnehmer).

Vorwort

Gender-Hinweis und Gleichstellung

Die edjufy Software GmbH steht für eine vielfältige Gesellschaft, sowie die Gleichberechtigung, Gleichstellung und Gleichbehandlung aller Geschlechter und Geschlechtsidentitäten.

Wir schätzen die Vielfalt von Menschen aller Herkunft, unabhängig von Alter, Abstammung, ethnischer Zugehörigkeit, Sprache, Hautfarbe, Fähigkeiten, Religion, Glaube, religiösen oder politischen Anschauungen, sozioökonomischem Status, Kultur, Weltanschauung, Geschlecht, sexueller Orientierung und Geschlechtsidentität.

Diese Reihenfolge ist rein zufällig und sagt nichts über ihre Wertigkeit aus. Zudem wurde Begriff "Rasse" in dieser Aufzählung (abgeleitet aus dem Grundgesetz Artikel 3) bewusst weggelassen, da es unseres Erachtens keine unterschiedlichen Menschenrassen gibt und der Begriff eine Diskriminierung darstellt.

Wir als edjufy sind zudem davon überzeugt, dass die Gleichstellung aller Menschen, sowie die Diversität für ein leistungsstarkes und innovationsorientiertes Unternehmen unerlässlich ist.

Aus den oben genannten Gründen möchten wir für dieses Dokument auf folgende Besonderheit hinweisen und bitten um Verständnis und Nachsicht.

Um die Lesbarkeit in diesem Dokument zu verbessern, wird ab diesem Kapitel bei Personenbezeichnungen und personenbezogenen Substantiven auf die gleichzeitige Verwendung der Sprachformen männlich/weiblich/divers verzichtet und die männliche Form als generisches Maskulinum (z. B. „der Lehrer“) verwendet.

Im Sinne der Gleichbehandlung gelten sämtliche Personenbezeichnungen grundsätzlich für alle Geschlechter und Geschlechtsidentitäten.

Die verkürzte Sprachform hat nur redaktionelle Gründe, beinhaltet keine Wertung und dient nur der besseren Lesbarkeit.

§ 1 Gegenstand und Dauer der Vereinbarung

1. Gegenstand dieser Vereinbarung ist die Regelung der Rechte und Pflichten des Kunden im Sinne der AGB und des Auftragnehmers im Rahmen der Leistungserbringung (nach AGB und mitgeltenden Dokumenten) bezüglich der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Kunden im Sinne des anwendbaren Datenschutzrechts.
2. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Kunden im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieser Vereinbarung.

3. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
4. Diese Auftragsverarbeitungsvereinbarung besteht so lange der Kunde Leistungen im Sinne der AGB vom Auftragnehmer bezieht.
5. Der Kunde kann die Beauftragung im Sinne der AGB und diese Vereinbarung ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine datenschutzrechtlich veranlasste Weisung des Kunden nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Kunden unzulässig verweigert. Insbesondere die Nichteinhaltung der in dieser Vereinbarung definierten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 2 Art und Zweck der Verarbeitung, Art der Personenbezogenen Daten und Kategorien Betroffener

1. Es werden folgende Daten im Sinne von Art. 4 Nr. 1, 13, 14 und 15 DSGVO verarbeitet:
 - a. Name, Vorname und Anrede
 - b. E-Mailadressen
 - c. Adresse (Straße, Nummer, Ort, PLZ, Land)
 - d. Schulzugehörigkeit
 - e. Klassenstufe und Geburtsdatum
 - f. Erziehungsberechtigung (aus Sicht der Erziehungsberechtigten) und Erziehungsberechtigte (aus Sicht der Schüler)
 - g. Unterrichts- / Notenleistungen sowie schülerbezogene Informationen bzgl. Lernstand und Mitarbeit
 - h. Nachrichten und Rückantworten im Rahmen von Elternbriefen, 1:1- und Gruppenkonversationen
 - i. Das Primärtransportmedium von Nachrichten und Benachrichtigungen ist die E-Mail (ausschließlich über verschlüsselte Verbindungswege (SSL/TLS))
 - ii. Sofern für die Schule verfügbar und aktiviert, werden sog. Push-Benachrichtigungen per Ende-zu-Ende Verschlüsselung direkt auf ein Smartphone verschickt.
 - iii. Die Schule hat zusätzlich die Möglichkeit, z.B. in den System-Einstellungen den E-Mail Privacy Modus zu aktivieren. Mit aktivierten E-Mail Privacy Modus beinhalten die E-Mail-Benachrichtigungen keine sensiblen Daten mehr und verweisen lediglich per Link auf das durch Login geschützte und Ende-zu-Ende verschlüsselte edjufy Portal.
 - i. Informationen zu Abwesenheiten und Entschuldigungen (einschließlich deren Kommentare und Anhänge) und deren Verknüpfungen untereinander
Das System verknüpft zu einer Abwesenheit automatisch die in edjufy hinterlegten Entschuldigungen. Eine manuelle Verknüpfung sowie die damit einhergehende Gefahr, eine Entschuldigung eines anderen Schülers mit einer Abwesenheit zu verknüpfen ist dadurch technisch ausgeschlossen
 - j. Informationen zu Anträgen auf Beurlaubung (einschließlich deren Kommentare und Anhänge)
 - k. Kalender- / Termininformationen einschließlich deren Meta-, Detail- und Freitextdaten (z.B. bei Kalendereinträgen oder bei der Elternsprechtagplanung)
 - l. Teilnahme am Religionsunterricht
 - m. Sonstige für die Abwicklung des Schulbetriebs notwendigen und relevanten Informationen
 - n. Erfolgte Zugriffe und Zugriffsversuche
 - o. Dieser Punkt gilt nur, sofern die Schule im Rahmen der Dokumentationspflicht von Corona Tests für die Teilnahme am Unterricht das edjufy Modul "Corona Test Dokumentation" verwendet.
 - i. Ergebnisse von Corona Tests unterliegen in der DSGVO einem besonderen Schutz. So dürfen Testergebnisse in den Schulen nur dann ohne Einwilligung der Schüler / Erziehungsberechtigten verarbeitet werden, solange eine Rechtsvorschrift dies erlaubt oder die Schule sogar dazu verpflichtet. Dazu zählen z.B. Bundesgesetze wie "§ 28b Abs. 3 - Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz - IfSG)" oder auch Rechtsvorschriften der Länder wie z.B. die CoronaSchVO / CoronaBetrVO (NRW), BeLVO (Rheinland-Pfalz), CoronaVO Schule (Baden-Württemberg) oder die BayIfSMV (Bayern)

- ii. Sofern die Schule im Rahmen einer Rechtsvorschrift Corona Tests mit edjufy dokumentiert, werden folgende Daten verarbeitet:
 - 1. Teilnehmer des Testdurchlaufs
 - 2. Datum des Testdurchlaufs
 - 3. Testaufsicht / Lehrkraft
 - 4. Kommentare der Testaufsicht zum Test
 - 5. Testergebnis der Teilnehmer
 - 6. Test-Befreiung eines Schülers mit Datumsangabe
 - 7. Sofern eine Rechtsvorschrift die Schulen dazu verpflichtet, zwischen verschiedenen Statuswerten bzgl. "Geimpft", "Genesen", "Geboostert" oder ähnliche zu unterscheiden, wird - neben der oben genannten "Test-Befreiung" inkl. Datum - dieser Status ebenfalls verarbeitet und für die Abwicklung der Corona-Test Dokumentation verwendet.
Dies geschieht z.B. wenn Personen ohne "Booster-Impfung" wieder einer Testpflicht im Rahmen einer Rechtsvorschrift unterliegen.
- iii. Die personenbezogenen Testergebnisse werden durch die edjufy Plattform automatisch unter Protokoll mit Ablauf der gesetzlichen Verwahrrfrist vernichtet.
- p. Dieser Punkt gilt nur, sofern die Schule das edjufy Modul "Digitale Schulanmeldung" verwendet. Im Rahmen der "Digitalen Schulanmeldung" von edjufy werden zu den bereits genannten personenbezogenen Informationen folgende weitere Daten verarbeitet:
 - i. Allgemeine Daten im Sinne von Art. 4 Nr. 1, 13, 14 und 15 DSGVO
 - 1. Staatsangehörigkeiten / Staatsbürgerschaften
 - 2. Geburtsort
 - 3. Bekenntnis
 - 4. Schullaufbahn / Schullaufbahneempfehlung
 - 5. (Übertritts-) Zeugnisse
 - 6. Schulweg / Schulwegbeförderung
 - ii. Gesundheitsdaten im Sinne von Art. 9 Abs 1 DSGVO
 - 1. Gesundheitsdaten unterliegen in der DSGVO einem besonderen Schutz (siehe Art. 9 Abs 1 DSGVO). So dürfen z.B. Informationen zum Masernschutzstatus oder Informationen / Nachweise zu verpflichtenden Voruntersuchungen wie z.B. die "Einschulungsuntersuchung" (Baden-Württemberg) oder die "Schuleingangsuntersuchung" (Bayern / Nordrhein-Westfalen) in den Schulen nur dann ohne Einwilligung der Schüler / Erziehungsberechtigten verarbeitet werden, solange eine Rechtsvorschrift dies erlaubt oder die Schule sogar dazu verpflichtet. Dazu zählen z.B. Bundesgesetze wie das "Gesetz für den Schutz vor Masern und zur Stärkung der Impfprävention (Masernschutzgesetz)" und "§ 20 Abs. 9 / § 23 a / § 34 Abs. 5 - Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz - IfSG)" sowie Rechtsvorschriften der Länder wie z.B. das SchG (Baden-Württemberg), SchulG (Nordrhein-Westfalen) oder das BayEUG / GDVG / die BaySchO (Bayern).
 - 2. Gesundheitsdaten von Schülern und Mitarbeitern der Schule werden in edjufy ausschließlich im Rahmen einer jeweils gültigen Rechtsvorschrift verarbeitet.
 - 3. Im Rahmen einer jeweils gültigen Rechtsvorschrift (Beispiele siehe oben) werden zusätzlich folgende Informationen verarbeitet:
 - a. Nachweise zum Impfstatus zu gesetzlich verpflichtenden Impfungen
 - b. Nachweise zum Impfstatus zu Impfungen die durch die Schule verarbeitet werden dürfen oder müssen (z.B. COVID-19)
 - c. Nachweise zu gesetzlich verpflichtenden Untersuchungen / Voruntersuchungen
 - 4. Die Abfrage dieser Daten im Rahmen der "Digitale Schulanmeldung" ist optional und kann aktiviert oder deaktiviert werden.
- 2. Es werden die Daten im Sinne von Art. 4 Nr. 2 DSGVO wie folgt verarbeitet:
Die Daten werden insbesondere zur Abwicklung des Schulbetriebs und von im Schulbetrieb anfallender Kommunikation und zur Prüfung der Legitimation der Kommunikationsempfänger verwendet.
- 3. Der Auftragnehmer erhält die Elternstammdaten (Name, Kontaktadresse) von der Schule. Die Stammdaten können danach nur durch die Eltern verändert werden.
- 4. Die Schülerstammdaten erhält der Auftragnehmer von der Schule.
- 5. Gemäß Art. 4 Nr. 1 DSGVO erfasst die Verarbeitung folgende Kategorien Betroffener:
 - a. Lehrer

- b. Mitarbeiter der Schulverwaltung
- c. Schüler
- d. Erziehungs- und Sorgeberechtigte

§3 Unterauftragsverarbeitungen

1. Die edjufy Software GmbH greift zur Erfüllung ihrer Aufgaben auf Unterauftragsverarbeiter zurück. Eine Liste mit allen Unterauftragsverarbeitern findet sich in "Anlage 1 der AVV - Unterauftragsverarbeiter".
2. Alle Unterauftragsverarbeiter befinden sich in vertraglichen Beziehungen mit dem Auftragnehmer. Es wurde je ein Auftragsverarbeitungsvertrag oder eine Auftragsverarbeitungsvereinbarung geschlossen. Die Unterauftragsverarbeiter garantieren in diesen, dass geeignete technische und organisatorische Maßnahmen im Einklang mit den Anforderungen des maßgeblichen europäischen und deutschen Datenschutzrechts erfolgen.

§ 4 Rechte, Pflichten und Weisungsbefugnisse des Kunden

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Kunde verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solchen Anfragen, sofern sie erkennbar ausschließlich an den Kunden gerichtet sind, unverzüglich an diesen weiterzuleiten.
2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen dem Kunden und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
3. Der Kunde erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in Textform. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.
4. Der Kunde ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen.
5. Der Kunde informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
6. Der Kunde ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertragsverhältnis bestehen.
7. Weisungsberechtigte des Kunden sind die Schulleitung oder von ihr schriftlich benannte Personen. Weisungsempfänger des Auftragnehmers sind die Geschäftsführer der edjufy Software GmbH. Weisungen erfolgen per E-Mail oder in Schriftform.
8. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§ 5 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Kunden, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).
2. Der Auftragnehmer verwendet die von ihm verarbeiteten personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden lediglich zu Zwecken der notwendigen Datensicherung erstellt.
3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die Abwicklung aller vereinbarten Maßnahmen gemäß dieser Vereinbarung zu. Er sichert zu, dass die für den Kunden verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

4. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Kunden, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Kunden hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Kunden soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die Schulleitung weiterzuleiten.
5. Der Auftragnehmer wird den Kunden unverzüglich darauf aufmerksam machen, wenn eine von ihr erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Kunden nach Überprüfung bestätigt oder geändert wird.
6. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Kunde dies mittels einer Weisung verlangt und berechnete Interessen des Auftragnehmers dem nicht entgegenstehen.
7. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Kunden erteilen.
8. Der Auftragnehmer ermöglicht es dem Kunden - grundsätzlich nach Terminvereinbarung - die Einhaltung der Vorschriften über Datenschutz und Datensicherheit im angemessenen und erforderlichen Umfang zu kontrollieren, insbesondere durch Überprüfungen – einschließlich Inspektionen –, die von dem Kunden oder einem anderen von dieser beauftragten Prüfer durchgeführt werden. (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).
9. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.
10. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch die für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, insbesondere das Fernmeldegeheimnis.
11. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Kunden die Vertraulichkeit zu wahren. Diese Vertraulichkeit besteht auch nach Beendigung des Vertragsverhältnisses.
12. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS- GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
13. Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

§ 6 Mitteilungspflichten des Auftragnehmers

1. Der Auftragnehmer teilt dem Kunden unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Kunden nach Art. 33 und Art. 34 DSGVO.
2. Der Auftragnehmer sichert zu, dem Kunden erforderlichenfalls bei ihren Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Kunden darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

§ 7 Technische und Organisatorische Maßnahmen

1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Siehe hierzu das in "Anlage 2 der AVV - TOM zur IT-Sicherheit" beschriebene Datenschutzkonzept. Dieses stellt die Auswahl der technischen

und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

2. Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis samt vollständigem Auditbericht ist dem Kunden auf Anfrage mitzuteilen.
3. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und dem Kunden abzustimmen.
4. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Kunden in dokumentierter Form schriftlich oder in Textform abstimmen. Solche Abstimmungen sind für die Dauer dieser Vereinbarung aufzubewahren.

§ 8 Verpflichtungen des Auftragnehmers nach Auftragnehmer

Mit Beendigung der bereitgestellten Leistungen im Sinne der AGB hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Kunden elektronisch auszuhändigen und gleichzeitig die vorhandenen Kopien datenschutzgerecht zu löschen bzw. zu vernichten. Die Löschung bzw. Vernichtung ist dem Kunden mit Datumsangabe schriftlich oder in Textform zu bestätigen.

§ 9 Haftung

Es wird auf Art. 82 DSGVO hingewiesen.

§ 10 Aufbewahrungsfristen, Rechtswahl und Gerichtsstand

1. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen sind von beiden Parteien für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
2. Es gilt deutsches Recht.
3. Der ausschließliche Gerichtsstand ist München, sofern nicht eine Norm einen zwingenden anderen Gerichtsstand anordnet.

§ 12 Salvatorische Klausel

Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam oder undurchsetzbar sein oder werden oder durch ein Gericht der zuständigen Gerichtsbarkeit für gesetzeswidrig oder ungültig erklärt werden, wird die Wirksamkeit und Durchsetzbarkeit aller übrigen verbleibenden Bestimmungen (bzw. des verbleibenden Teils der jeweiligen Bestimmung) davon nicht berührt. Die unwirksame oder undurchsetzbare Bestimmung (bzw. der unwirksame oder undurchsetzbare Teil der jeweiligen Bestimmung) ist, soweit gesetzlich zulässig, als durch diejenige wirksame und durchsetzbare Bestimmung ersetzt anzusehen, die dem mit der unwirksamen oder nicht durchsetzbaren Bestimmung (oder mit dem unwirksamen oder nicht durchsetzbaren Teil der jeweiligen Bestimmung) verfolgten wirtschaftlichen Zweck nach Gegenstand, Maß,

Zeit, Ort und Geltungsbereich am nächsten kommt, während die übrigen Bestimmungen dieser Vereinbarung ihre volle Gültigkeit und Wirksamkeit behalten.

Entsprechendes gilt für die Füllung etwaiger Lücken in dieser Vereinbarung. Es ist der ausdrückliche Wille der Parteien, dass diese salvatorische Klausel keine bloße Beweislastumkehr zur Folge hat, sondern § 139 BGB insgesamt abbedungen ist.

Anlagen

- Anlage 1: Unterauftragsverarbeiter
- Anlage 2: Technische und Organisatorische Maßnahmen
- Anlage 3: Gesetz über den Kirchlichen Datenschutz (KDG)

Anlage 1 der AVV - Unterauftragsverarbeiter

Die edjufy Software GmbH greift zur Erfüllung ihrer Aufgaben auf die nachfolgenden Unterauftragsverarbeiter zurück.

Es findet zu keinem Zeitpunkt eine Weitergabe oder eine Verarbeitung von personenbezogenen Daten außerhalb Deutschlands oder der Europäischen Union statt.

Unterauftragsverarbeiter mit Auftragsdatenverarbeitung innerhalb Deutschlands und der EU

Unterauftragsverarbeiter	Tätigkeit
Telekom Deutschland GmbH	<p>Bereitstellung des Rechenzentrums und IT Diensten (T-Systems) auf Servern in Deutschland (u.a. Magdeburg und Biere)</p> <p>Die edjufy Plattform sowie auch die Daten der Schule liegen auf diesen Servern von T-Systems. Zusätzlich sind alle Daten (Datenbank und Files(z.B. Anhänge bei Entschuldigungen)) verschlüsselt. Das bedeutet, dass selbst T-Systems die Daten nicht einsehen kann.</p>
Hetzner Online GmbH	<p>Bereitstellung des Rechenzentrums und IT Diensten auf Servern in Deutschland (Nürnberg und Falkenstein)</p> <p>Die edjufy Plattform sowie auch die Daten der Schule liegen auf diesen Servern von Hetzner. Zusätzlich sind alle Daten (Datenbank und Files(z.B. Anhänge bei Entschuldigungen)) verschlüsselt. Das bedeutet, dass selbst Hetzner die Daten nicht einsehen kann.</p>
BroadSoft Germany GmbH	<p>Bereitstellung einer Cloud Telefonanlage auf Servern in Frankfurt, Deutschland.</p>

Unterauftragsverarbeiter	Tätigkeit
DeepL GmbH	Bereitstellung einer Übersetzungsschnittstelle auf Servern in Finnland (EU).
Mailgun Technologies	<p>Versand von E-Mails auf Servern in Frankfurt, Deutschland.</p> <p>Gemäß DSGVO wird darauf hingewiesen, dass obwohl die Datenverarbeitung in Deutschland stattfindet, die Muttergesellschaft des Unterauftragsverarbeiter ihren Hauptsitz außerhalb der EU hat.</p> <p>Die SCC Regelungen der EU-Kommission (Art. 46. Abs. 2 und 3 DSGVO) liegen vor.</p> <p>Ein TIA wurde intern erfolgreich durchgeführt.</p>
Userlane GmbH	Bereitstellung einer Software für geführte Touren durch die edjufy Plattform auf Servern in Amsterdam, Niederlande (EU).

Unterauftragsverarbeiter	Tätigkeit
1&1 IONOS SE	<p>Backup Rechenzentrum / Disaster Recovery</p> <p>Für den Fall eines größeren Ausfalls sowie bei längeren Ausfallzeiten in einem unserer Primärrechenzentren, greifen wir im Rahmen des edjufy Disaster Recovery Plans (EDRP) auf ein alternatives Rechenzentrum von 1&1 IONOS zurück.</p> <p>Tätigkeit des Unterauftragsverarbeiter: Bereitstellung des Backup-Rechenzentrums und IT Diensten auf Servern in Berlin, Deutschland.</p> <p>Die Daten der edjufy Plattform und suggestive der Schule liegen ausschließlich in den Primärrechenzentren und werden lediglich im Disaster Recovery Fall für die Zeit des Ausfalls durch das edjufy Disaster Recovery Squad umgezogen.</p> <p>Mit Beendigung der Störung und der Wiederaufnahme des Regelbetriebs werden die Daten durch das edjufy Disaster Recovery Squad wieder in die Primärrechenzentren umgezogen und im Backup-Rechenzentrum gelöscht. Im Backup-Rechenzentrum verbleiben keine Datensicherungen.</p> <p>Bei 1&1 IONOS sind alle Daten (Datenbank und Files(z.B. Anhänge bei Entschuldigungen)) verschlüsselt. Das bedeutet, dass selbst 1&1 IONOS die Daten nicht einsehen kann.</p>

Anlage 2 der AVV - TOM zur IT-Sicherheit

Die edjufy Software GmbH (nachfolgend Auftragnehmer) ergreift die folgenden technischen und organisatorischen Maßnahmen (TOM) bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten für die gleichnamige Plattform edjufy.

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

Zutrittskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass der unbefugte Zutritt zu Datenverarbeitungsanlagen, auf denen personenbezogenen Daten verarbeitet, gespeichert und genutzt werden, verhindert wird.

Folgende Maßnahmen werden hierfür ergriffen:

- Überwachung der Zugänge zu Datenverarbeitungsanlagen
- Vergabe von Zugangsberechtigungen ausschließlich an autorisierte Personen
- Zutritt zu Datenverarbeitungsanlagen bzw. allen relevanten Räumen nur für autorisierte Personen (Autorisierte Mitarbeiter sowie Besucher nur in Begleitung von autorisierten Mitarbeitern)
- Protokollierung des Zutritts zu Datenverarbeitungsanlagen
- Protokollierte Vergabe von Zutrittsberechtigungen
- Entzug der Zutrittsberechtigung nach Ausscheiden
- Elektrische Türsicherungen / Zylinder mit Chipkarte / Transponder
- Werkschutz bzw. Pförtner, Alarmanlagen und Videoanlagen

Zugangskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass der unbefugte Zugriff zu Datenverarbeitungsanlagen, auf denen personenbezogenen Daten verarbeitet, gespeichert und genutzt werden, verhindert wird.

Folgende Maßnahmen werden hierfür ergriffen:

- Zugriff ausschließlich durch autorisierte Mitarbeiter mit individuellen Zugangsdaten
- Sichere Kennwörter (Passwort-Policy)
- Automatische Sperrmechanismen
- Verwendung von Zwei-Faktor Authentifizierung
- Zugriff auf Datenverarbeitungsanlagen ausschließlich über abgesichertes VPN (Virtual Private Network)
- Verschlüsselung von Datenträgern und Systemen

Zugriffskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten, dass zur Nutzung von Datenverarbeitungsanlagen autorisierten Personen ausschließlich auf die ihrer Berechtigung unterliegenden Daten zugreifen können. Des Weiteren wird verhindert, dass personenbezogene Daten ohne entsprechende Berechtigung nicht gelesen, geändert, kopiert oder gelöscht werden können.

Folgende Maßnahmen werden hierfür ergriffen:

- Datenzugriff nur für berechtigte Personen (Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte)
- Schutz gegen unberechtigte interne sowie externe Zugriffe
- Unterweisung von Mitarbeitern bezüglich der individuellen Zugriffsrechte

Trennung der Verarbeitung für verschiedene Zwecke

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass Datenbestände welche für unterschiedliche Zwecke erhoben werden, getrennt verarbeitet werden können.

Folgende Maßnahmen werden hierfür ergriffen:

- Getrennte Verarbeitung zweckgebundener Datenbestände (z.B. Mandantenfähigkeit und Sandboxing)
- Trennung von Test- und Produktionssystemen

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Eingabekontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass keine personenbezogenen Daten in die Datenverarbeitungssysteme zusätzlich eingegeben oder entfernt wurden sowie eine entsprechende Überprüfung möglich ist.

Folgende Maßnahmen werden hierfür ergriffen:

- Erstellung eines Audit-Trails bei der Eingabe, Änderungen und Löschung von Daten
- Versionierung von Datenbeständen um Änderungen nachzuvollziehen
- Verschlüsselung von Datenbeständen
- Zugriffsbeschränkungen beim Zugriff auf Datenbestände

Weitergabekontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass bei der Übertragung und dem Transport von personenbezogenen Daten diese nicht durch unbefugte dritte gelesen, kopiert, verändert oder gelöscht werden können.

Folgende Maßnahmen werden hierfür ergriffen:

- Verschlüsselung von Datenübertragungen mit gängigen Verschlüsselungstechniken wie z.B. HTTPS Verbindungen (SSL)
- Versand von E-Mail Nachrichten ausschließlich über verschlüsselte Verbindungswege (SSL/TLS)
- Einsatz von verschlüsselten VPN (Virtual Private Network) Verbindungen zur Verbindung mit Datenverarbeitungsanlagen
- Verschlüsselung von internen und externen Speichermedien (Festplatten Verschlüsselung)

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

Verfügbarkeitskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass es nicht zu zum unbeabsichtigten Verlust oder zur Zerstörung von Datenbeständen kommt.

Hierfür - sowie für eine rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO) - werden folgende Maßnahmen ergriffen:

- Backup-Strategie
- Unterbrechungsfreie Stromversorgung (USV)
- Virenschutz und Firewall
- Meldewege, Notfallpläne, Disaster Recovery Management
- Regelmäßige Datensicherung auf externen und gesicherten Speichermedien
- Regelmäßige Überprüfung der Datensicherungen auf eine mögliche Wiederherstellbarkeit

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

Auftragskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass die Auftragsdatenverarbeitung von personenbezogene Daten auf Basis der mit dem Auftraggeber geschlossenen Auftragsverarbeitungsvereinbarung durchgeführt wird. Hierfür wird insbesondere auch auf die in der Auftragsverarbeitungsvereinbarung vereinbarte Weisungsbefugnis hingewiesen.

Es erfolgt keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Weitere Maßnahmen

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Anlage 3 der AVV - Gesetz über den Kirchlichen Datenschutz (KDG)

Vorwort

Diese Anlage gilt nur, sofern

- die Schule und oder der Schulträger eine caritative / kirchliche Einrichtung ist und oder
- dem Gesetz über den Kirchlichen Datenschutz (KDG) unterliegt

Zusatzvereinbarung zum Vertrag Auftragsverarbeitung gemäß § 29 Gesetz über den Kirchlichen Datenschutz (KDG)

Der Auftragnehmer nimmt zur Kenntnis, dass der Auftraggeber eine caritative / kirchliche Einrichtung ist, die zwingend dem Anwendungsbereich des Kirchlichen Gesetzes über den Datenschutz (KDG) unterliegt.

Die Parteien beziehen daher die Anwendung des KDG, insbesondere §§ 29 und 31 KDG, sowie die Beachtung der dort getroffenen Vorschriften ausdrücklich in diese Vereinbarung ein.

Anlage 4 der AVV - Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD- Datenschutzgesetz)

Vorwort

Diese Anlage gilt nur, sofern

- die Schule und oder der Schulträger eine diakonische Einrichtung / eine Einrichtung der Evangelischen Kirche ist und oder
- dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz) unterliegt

Zusatzvereinbarung zum Vertrag gemäß § 30 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD- Datenschutzgesetz)

Der Auftragnehmer nimmt zur Kenntnis, dass der Auftraggeber diakonische Einrichtung / eine Einrichtung der Evangelischen Kirche ist, die zwingend dem Anwendungsbereich des Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz) unterliegt.

Die Parteien beziehen daher die Anwendung des EKD-Datenschutzgesetz, insbesondere §§ 30 Absatz 5, 43, 44 EKD-Datenschutzgesetz, sowie die Beachtung der dort getroffenen Vorschriften ausdrücklich in diese Vereinbarung ein.

Anlage 5 der AVV - Datenschutzordnung der Israelitischen Religionsgemeinschaft Württembergs K.d.ö.R. (IRGW)

Vorwort

Diese Anlage gilt nur, sofern

- die Schule und oder der Schulträger eine Einrichtung der Israelitischen Religionsgemeinschaft Württembergs K.d.ö.R. (IRGW) - im weiteren Verlauf kurz IRGW - ist und oder
- der Datenschutzordnung der Israelitischen Religionsgemeinschaft Württembergs K.d.ö.R. (IRGW) - im weiteren Verlauf kurz DO-IRGW - unterliegt

Zusatzvereinbarung zum Vertrag gemäß DO-IRGW

Der Auftragnehmer nimmt zur Kenntnis, dass der Auftraggeber eine Einrichtung der Israelitischen Religionsgemeinschaft Württembergs K.d.ö.R. (IRGW) ist, die zwingend dem Anwendungsbereich der DO-IRGW unterliegt.

Die Parteien beziehen daher die Anwendung der DO-IRGW, insbesondere §§ 1, 3 und § 7 (Datenschutzaufsicht durch das Obere Schieds- und Verwaltungsgericht beim Zentralrat der Juden in Deutschland) sowie die Beachtung der dort getroffenen Vorschriften ausdrücklich in diese Vereinbarung ein.

Anlage 6 der AVV - Datenschutzordnung Jüdische Gemeinde Frankfurt am Main K.d.ö.R.

Vorwort

Diese Anlage gilt nur, sofern

- die Schule und oder der Schulträger eine Einrichtung der Jüdische Gemeinde Frankfurt am Main K.d.ö.R. ist und oder
- der Datenschutzordnung Jüdische Gemeinde Frankfurt am Main K.d.ö.R. unterliegt

Zusatzvereinbarung zum Vertrag gemäß Datenschutzordnung der Jüdische Gemeinde Frankfurt am Main K.d.ö.R.

Der Auftragnehmer nimmt zur Kenntnis, dass der Auftraggeber eine Einrichtung der Jüdische Gemeinde Frankfurt am Main K.d.ö.R., die zwingend dem Anwendungsbereich der Datenschutzordnung Jüdische Gemeinde Frankfurt am Main K.d.ö.R. unterliegt.

Die Parteien beziehen daher die Anwendung der Datenschutzordnung Jüdische Gemeinde Frankfurt am Main K.d.ö.R., insbesondere §§ 1, 3 und § 7 (Datenschutzaufsicht durch das Obere Schieds- und Verwaltungsgericht beim Zentralrat der Juden in Deutschland) sowie die Beachtung der dort getroffenen Vorschriften ausdrücklich in diese Vereinbarung ein.