Auftragsverarbeitungsvertrag (AV-Vertrag)

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DS-GVO

zwischen

Träger

als Verantwortliche/r - nachfolgend "Auftraggeber" genannt –

und

Kitalino GmbH

Hermann-Herder-Str. 4

79104 Freiburg im Breisgau

als Auftragsverarbeiter/in - nachfolgend "Auftragnehmer" genannt –

- Auftraggeber und Auftragnehmer nachfolgend jeder auch "Partei" und gemeinsam "Parteien"

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Software as a Service (abgekürzt : SaaS-Dienstleistungen) in Übereinstimmung mit der Nutzung der Kidling Kita-Software (abgekürzt: Kidling). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung ("DSGVO"). Zur Erfüllung der Anforderungen der DS-GVO an derartige Konstellationen schließen die Parteien den nachfolgenden Vertrag, dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§1 Begriffsbestimmungen

In diesem Auftragsverarbeitungsvertrag werden die Begriffe des Verantwortlichen, des Auftragsverarbeiters, der personenbezogenen Daten, der Verarbeitung der

personenbezogenen Daten, der besondere Kategorie der personenbezogenen Daten im Sinne der Art. 4, Art. 9 und Art. 10 DS-GVO verwendet.

§ 2 Gegenstand/Umfang der Beauftragung

1. Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass der Auftragnehmer Zugriff auf personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten des Auftraggebers (nachfolgend "Auftraggeberdaten") erhält und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DS-GVO verarbeitet.
2. Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt ausschließlich im Rahmen der Ausführung des Hauptvertrages zur Erbringung von Software-as-a-Service Dienstleistungen durch Kitalino GmbH im Rahmen der Kidling. Der Zweck der Datenverarbeitung wurde in Anlage 1 dargestellt. Der Kreis, der von der Datenverarbeitung betroffenen Personen und die Art der verarbeiteten Daten ist in Anlage 1 zu diesem Vertrag dargestellt. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.
3. Dem Auftragnehmer ist eine abweichende oder über die Festlegungen in den §2 Abs. 2 hinausgehende Verarbeitung von Auftraggeberdaten untersagt.
4. Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

§ 3 Weisungsbefugnisse des Auftraggebers

1. Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers iSv Art. 28 DS-GVO (Auftragsverarbeitung), dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "Weisungsrecht"). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.
2. Weisungen werden vom Auftraggeber grundsätzlich schriftlich erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer unverzüglich schriftlich zu bestätigen. In beiden Fällen ist die Textform ausreichend. Die weisungs- und empfangsberechtigten Personen ergeben sich aus Anlage 2. Bei einem Wechsel oder einer längerfristigen Verhinderung der in Anlage 2 benannten Personen ist der anderen Partei unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen. Der Auftragnehmer wird dem Auftraggeber einen Wechsel der Person des Weisungsberechtigten frühzeitig anzeigen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die benannten Personen weiter als empfangsberechtigt.

3. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

§ 4 Schutzmaßnahmen des Auftragnehmers

1. Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.
2. Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden "Mitarbeiter" genannt), in Schriftform zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.
3. Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DS-GVO, insbesondere die in Anlage 3 zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten. Die technischen und organisatorischen Maßnahmen des Auftragnehmers sollen nach Möglichkeit so gestaltet werden, dass sie den Auftraggeber in der Umsetzung seiner Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Personen unterstützen.
4. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß Anlage 3 nicht mehr ausreichend sind und wird sich mit ihm hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.
5. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der in Anlage 3 bestimmten technischen und organisatorischen Maßnahmen durch geeignete Nachweise nachweisen.

§ 5 Informations- und Unterstützungspflichten des Auftragnehmers

1. Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder

andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in elektronischer Form informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldungen gemäß § 5 Abs. 1 Satz 1 enthalten jeweils zumindest die in Art. 33 Absatz 3 DS-GVO genannten Angaben.

2. Der Auftragnehmer wird den Auftraggeber im Falle des § 5 Abs. 1 bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe – und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen. Der Auftragnehmer wird insbesondere unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Auftraggeber hierüber informieren und diesen um weitere Weisungen ersuchen.
3. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle gemäß § 8 Abs. 1 dieses Vertrages erforderlich sind. Ferner wird der Auftragnehmer dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung stellen.

§ 6 Sonstige Verpflichtungen des Auftragnehmers

1. Der Auftragnehmer ist verpflichtet ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gem. Art. 30 Abs. 2 DS-GVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.
2. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz Folgenabschätzung nach Art. 35 DS-GVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO zu unterstützen.
3. Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten bestellt hat. Die Kontaktdaten des Datenschutzbeauftragten sind unter https://kitalino.com/datenschutz abrufbar.
4. Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegt.

§ 7 Subunternehmerverhältnisse

1. Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 4 genannten Subunternehmer

durchgeführt. Der Auftraggeber stimmt der Beauftragung der in Anhang 4 bezeichneten Subunternehmer zu.
Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern ("Subunternehmerverhältnis") befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich oder in dokumentiertem elektronischen Format zugestimmt hat. Der Auftraggeber kann innerhalb von 7 Tagen ab Benachrichtigung der Beauftragung eines neuen Unterauftragnehmer widersprechen. Im Falle eines Widerspruchs werden die Parteien nach Treu und Glauben über Alternativlösungen verhandeln.

2. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standardklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarung mit seinen Subunternehmern nachweisen.

3. Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören zB Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

§ 8 Kontrollrechte

1. Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 5 Abs. 3 dieser Vereinbarung, zu überzeugen. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

2. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

3. Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 9 Rechte Betroffener

1. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie Art. 32 bis 36 DS-GVO.
2. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

§ 10 Laufzeit und Kündigung

1. Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.
2. Der Auftraggeber ist jederzeit zu einer außerordentlichen Kündigung dieses Vertrages aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt vor, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer zunächst eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann. Nach fruchtlosem Ablauf dieser Frist steht dem Auftraggeber sodann das Recht zur außerordentlichen Kündigung zu.

§ 11 Löschung und Rückgabe nach Vertragsende

1. Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrages oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger und zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich zu löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind durch den Auftragnehmer entsprechend der jeweiligen

Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren und auf Verlangen an den Auftragsgeber herauszugeben.

2. Der Wunsch des Auftraggebers zur Löschung oder Rückgabe der Unterlagen, Daten und Datenträger muss schriftlich oder in einer elektronischen Form spätestens vierzehn (14) Tage vor dem Eintritt des Beendigungsdatums des Hauptvertrages dem Auftragnehmer vorgelegt werden. Liegt dem Auftragnehmer keine Entscheidung des Auftraggebers vor oder wurde der Termin oder die elektronische Form nicht eingehalten, erfolgt die Löschung der überlassenen Unterlagen, Daten und Datenträger unverzüglich, spätestens am Tag der Beendigung des Hauptvertrages.
3. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung zu führen und dem Auftraggeber auf dessen Verlangen vorlegen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren; § 8 Abs. 2 dieses Vertrages gilt hierfür entsprechend.
4. Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die Vorliegende Vereinbarung bleibt über das Ende des Hauptvertrages hinaus solange gültig, wie der Auftragnehmer über personenbezogenen Daten verfügt, die ihm von dem Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 12 Geheimhaltungspflichten

1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Drittenerhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 13 Haftung

1. Die Haftung der Parteien richtet sich nach Art. 82 DS-GVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.
2. Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. § 12 Abs. 2 Satz 1 gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 14 Schlussbestimmungen

1. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer iSd § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.
2. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
3. Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
4. Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Freiburg im Breisgau

Auftraggeber:in	Auftragnehmer: Kitalino GmbH

Anlagen

Anlage 1

Zweck der Datenverarbeitung, Beschreibung der Datenarten und der Kategorien betroffener Personen

Anlage 2

Weisungs- und empfangsberechtige Personen

Anlage 3

Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DS-GVO)

Anlage 4

Liste der Subunternehmer

Anlage 1

Zweck der Datenverarbeitung, Beschreibung der Datenarten und der Kategorien betroffener Personen

Zweck der Verarbeitung

Zweck der Verarbeitung der personenbezogenen Daten im Rahmen der Kidling ist, die Schaffung einer Kommunikationsplattform zwischen den Kitaerziehern und den Eltern als Grundlage für Übermittlung von Informationen und Daten bzw. Ergebnissen von Datenverarbeitungsprozessen zur Vereinfachung und Optimierung von Bildungs- und Erziehungsmaßnahmen.

Arten der Verarbeitung

Das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, die Einschränkung, das Löschen oder die Vernichtung.

Kategorien betroffener Personen

Kinder, Jugendliche, Eltern bzw. Sorgeberechtigte eines Kindes, Kontaktpersonen der Kinder, Mitarbeitende einer Kitaeinrichtung und andere, die für eine Kitaeinrichtung tätig sind (z.B. studentische und wissenschaftliche Aushilfen, Handwerker, Psychologen, Physiotherapeuten).

Art der personenbezogenen Daten

Die verarbeiteten personenbezogenen Daten können die folgenden Kategorien von Daten umfassen:

- Direkte Identifikationsdaten (z.B. Name, E-Mail-Adresse, Telefonnummer).
- Indirekte Identifikationsdaten (z.B. Berufsbezeichnung, Geschlecht, Geburtsdatum, Benutzer-ID).
- Personenbezogene Daten im Sinne des Art. 4 Nr. 1, 13, 14, 15 DS-GVO.
- Sozialdaten im Sinne des Sozialgesetzes, insbesondere des SGB VIII, SGB X und SGB I.
- Beschäftigungsinformationen einer Kitaeinrichtung (z.B. Namen und Vornamen des Mitarbeiters und anderen Beschäftigten, Kontaktdaten, Personalakte usw.).
- Finanzielle Informationen (z.B. Bankkonto, Gehaltsabrechnungen).
- Vertragsstammdaten, Vertragsabwicklung

- Geräteidentifikationsdaten und Verkehrsdaten (z.B. IP-Adressen, MAC-Adressen, Server-Logfiles).
- Alle personenbezogenen Daten, die von Nutzern der Software bereitgestellt werden.
  − Alle personenbezogenen Daten, die in einem vom Kunden bereitgestellten Dokument enthalten sind.

Anlage 2

Weisungsberechtigte Personen des Auftraggebers sind:

- Name, Vorname, Funktion: _____
- Name, Vorname, Funktion: _____

Weisungsempfänger bei dem Auftragnehmer sind

- Simon Biallowons Geschäftsführer Kitalino GmbH service@kitalino.com
- Philipp Lindinger Geschäftsführer Kitalino GmbH service@kitalino.com

Anlage 3

Dokumentation technisch-organisatorischer Maßnahmen nach Art. 32 DSGVO bei dem Unternehmer Kitalino GmbH

1.1 Zutrittskontrolle

Unter Zutrittskontrolle versteht man die Maßnahmen, die geeignet sind, einen Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. In dem Unternehmen werden folgenden Maßnahmen getroffen:

Technische Maßnahmen:

- Alarmanlage
- Schlüssel/Schlüsselvergabe ist zentral und organisatorisch klar geregelt
- Türen mit Knauf Außenseite
- Absicherung der Gebäudeschächte
- Sicherheitsschlösser Videoüberwachung der Haupteingänge
- Klingelanlage mit Kamera
- Klare Zuweisung der Berechtigungen (Zugang Gebäude, Büro, Serverraum)

Organisatorische Maßnahmen:

- Zutrittskontrollsystem,
- zentrale Schlüsselverwaltung
- Empfang
- Besucherbuch
- Verschließen von Schränken und Büroräumen bei Nichtanwesenheit ist gewährleistet
- Erstellung einer Liste von Personen, die für die Kitalino GmbH auf einer anderen Grundlage als Anstellungsvertrag tätig sind und Zutritt zu den Büroräumen haben
- Regelungen für Besucher (in den Büroräumer werden die Besucher von den Mitarbeitern der Kitalino/Herder Verlag GmbH begleitet)
- Sorgfalt bei Auswahl des Wachpersonals
- Sorgfalt bei der Bestellung einer Reinigungsservice

- Bzgl. Arbeiten im Home-Office gelten zusätzliche Anweisungen an die Mitarbeiter u.a.: Die Mitarbeiter sichern zu, dass der Home-Office Arbeitsplatz über ausreichende Zutrittseinrichtungen verfügt, nach Möglichkeit ist der Arbeitsraum vor/ nach dem Ende der Tätigkeit auf-/abzuschließen

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen:

- Login mit Benutzername und Passwort für den Zugang zu dem Arbeitslaptop
- Jeder Mitarbeiter wurde über die Hinweise über den Umgang mit administrativen Passwörtern belehrt / Vertraulichkeitsverpflichtung der Mitarbeiter
- Keine Gruppenpasswörter
- Verschlüsselung von Datenträgern
- Verschlüsselung von Laptops / Tablets
- Firewall
- Anti-Virus Software mobile Geräte (Laptops)
- Remotegerätzurücksetzung

Organisatorische Maßnahmen:

- Passwortvergabe bei der Nutzung von Kidling: Dezidiertes Kennwortverfahren zum Login Klare Passwortregelung (bestimmte Länge, Kombination aus Buchstaben und Zahlen, keine Trivialpasswörter, Änderung in regelmäßigen Abständen).
- Automatische Sperrung des Laptops der Mitarbeiter nach einer bestimmten Zeit der Inaktivität (ca. 2 Min) mit anschließendem erneutem Login
- Richtlinie Clean Desk Policy
- Verpflichtung zur Vertraulichkeit / Mitarbeiter
- Verwalten von Benutzerberechtigungen

- Zentrale Passwortvergabe
- Allg. Richtlinie Datenschutz und IT-Sicherheit Richtlinie Homeoffice Office
- Bzgl. Arbeiten im Home-Office gelten zusätzliche Anweisungen an die Mitarbeiter u.a.: Mitarbeiter haben sicherzustellen, dass keine Dritte (etwa Haushaltmitglieder) Zugang zu den verarbeiteten Daten erlangen. Beim Verlassen des Arbeitsplatzes ist die passwortgeschützte Bildschirmsperre zu aktivieren

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen:

- Differenzierte Zugriffsberechtigung aufgeteilt auf: Dateien / Datensätze/ Datenfelder/ Anwendungsprogramme / Betriebssysteme/ Server
- Differenziertes Ordnerkonzept (alle Dateien sind einheitlich und nachvollziehbar zu benennen und so abzuspeichern, dass sie problemlos wiedergefunden werden können)
- Wechseldatenträgerlaufwerke sind gegen unbefugte Benutzung gesichert (komplettes System ist verschlüsselt)
- Die Daten auf den mobilen IT Systemen sind verschlüsselt
- Sichere Löschung von Daten (Aktenschredder (mind. Stufe 3, cross cut)
- Physische Löschung von Datenträgern
- Deinstallation bzw. Deaktivierung nicht benötigter sicherheitsrelevanter Programme und Funktionen (bei Smartphones)
- Anpassung sicherheitsrelevanter Standardeinstellungen von neuen Programmen und IT-Systemen

Organisatorische Maßnahmen:

- Minimale Anzahl an Administratoren
- Verwaltung Benutzerrechte durch Administratoren
- Zugriffsrechte für IT Systeme / Servern werden von dem Geschäftsleitungsteam vergeben
- Zugriffsberechtigung auf Daten und Applikationen werden von dem Geschäftsleitungsteam genehmigt
- Ordnung am Arbeitsplatz [Datenträger (USB-Sticks) mit vertraulichem Material dürfen nicht offen herumliegen]
- Clean Desk Policy
- Jeder Mitarbeiter hat den Zugriff nur auf die Programme und Daten, die er zur seinen Aufgabenerfüllung benötigt („Need-to-know-Prinzip“). Der Zugriff wird durch die funktionelle Zuordnung einzelner Datenendgeräte bestimmt

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen:

- Mandantentrennung (softwareseitiger Ausschluss)
- Trennung von Test- und Routineprogrammen
- Trennung von Test- und Produktivdaten
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)

Organisatorische Maßnahmen:

- Rollen- und Rechtekonzept im Unternehmen
- Festlegung von Datenbankrechten

1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen

Technische Maßnahmen

Organisatorische Maßnahmen

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2.0 Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B.

Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen:

- Bei der E-Mail / WWW werden folgende Sicherungsmechanismen eingesetzt:
  - WWW mit SSL

  Folgende Sicherheitsmaßnahmen sind vorhanden:
  - VPN
  - Firewall
- Elektronische Vertragssignatur ist möglich
- Keine Benutzung von nicht freigegebener Hard-/Software
- Keine Weiterleitung von E-Mails an private E-Mail-Accounts von Mitarbeitern

Organisatorische Maßnahmen:

- Vorgaben an Mitarbeiter bzgl. Ausdrucken von geheimen Unterlagen (Sicherstellung, dass kein anderer Zugriff auf Ausdrucke bekommt).

2.2 Eingangskontrolle / Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen:

- Protokollierungs- und Protokollauswertungssysteme werden eingesetzt, bzw. sind als Teile von bestehenden Softwareapplikationen anwendbar
- Ein Schadsoftwareschutz vorhanden mit einem monatlichen/automatischen / Täglichen Update
- Zugriff auf Datenverarbeitungssysteme nur nach Login möglich
- Keine Weitergabe von Passwörtern
- Zusätzlich zur automatischen Sperrung: manuelle Abmeldung beim Verlassen des Büros

Organisatorische Maßnahmen:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis der vordefinierten Funktionen

3.0

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Plattenspiegelungen etc.

Technische Maßnahmen:

- Virenschutz/Firewall nach aktuellem Stand der Technik ist gewährleistet
- Schutz im Serverraum
- Anlage:
    - Vollständig redundante elektrische Anlagen
    - Notstromversorgung
    - Klimaanlagen zur Kontrolle der Betriebstemperatur für Server und andere Hardware
    - Technische und manuelle Überwachung von Temperatur und Luftfeuchtigkeit
    - Automatische Geräte zur Branderkennung und -bekämpfung
    - Wassererkennungssensoren
    - Präventive Überwachung von elektrischen und mechanischen Geräten nach Wartungszeitplan

- Sicherheit:
    - Überwachung durch CCTV-Kameras mit Aufzeichnungsfunktion. Die Aufnahmen werden gemäß behördlichen und Compliance-Anforderungen aufbewahrt
    - Strenges Programm zur Zugangsberechtigung vorhanden
    - 24/7 professionelles Sicherheitspersonal
    - Alarmanlagen / Einbruchmeldesysteme
    - Überwachung durch CCTV-Kameras mit Aufzeichnungsfunktion. Die Aufnahmen werden gemäß behördlichen und Compliance-Anforderungen aufbewahrt

- Organisatorische Maßnahmen:
    - Datenreplikationen von extrem kurzen Wiederherstellungszeiträumen
    - Kontinuierliche Überwachung der Service-Nutzung
    - Höchst dringliche Behandlung von Medienspeichergeräten mit Kundendaten (inkl. Stilllegung gemäß Techniken in NIST 800-88 beschrieben)

4.0 Verfahren zur regelmäßigen Überprüfung, Bewertung, und Evaluierung

4.1 Datenschutzfreundliche Voreinstellung

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

4.2 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

- eindeutige Vertragsgestaltung/Standardvertrag zu Art. 28 DS-GVO vorhanden
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Anlage 4

Liste der Subunternehmer:

Amazon Web Services (AWS); Region Frankfurt, Deutschland Eschborner Landstraße 100, 60489 Frankfurt am Main (nachfolgend: „AWS“), ist ein zertifizierter und sicherer Hosting-Dienstleister, der die Daten der Auftragnehmer hosted. AWS bietet einen DSGVO-konformen Zusatz zur Datenverarbeitung (DSGVO DPA), der die Standardvertragsklauseln beinhaltet. Die Standardvertragsklauseln sind Standardbestimmungen, die von der Europäischen Kommission definiert und genehmigt wurden. Die AWS hat u.a. folgende Zertifikate erlangt, die den sicheren Umgang mit den Daten beweisen, die sich im Rahmen der Sicherheitsgewährleistungsprogramme von AWS befinden:

- ISO- und CSA-STAR-Zertifikate Internationale Organisation für Standardisierung (ISO) und Cloud-Sicherheitsallianz (CSA) Sicherheitsvertrauensgewährleistung und Risiko (STAR): ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 und CSA STAR CCM v4.0
- C5 Katalog der Compliance-Kontrollen für Cloud-Computing
- CISPE Cloud Infrastructure Services Providers in Europe Data Protection Code of Conduct
- CPSTIC STIC-Produkt- und Dienstleistungskatalog des National Cryptologic Center (CCN) (CPSTIC)
- HITRUST CSF Gemeinsame Sicherheits-Rahmenbedingungen der Trust Alliance für Gesundheitsdaten
- IRAP Information Security Registered Assessors Program
- ISMAP Programm zur Verwaltung und Bewertung der Informationssystemsicherheit
- MTCS Mehrschichtige Cloud-Sicherheit
- OSPAR Outsourced Service Provider’s Audit Report (Prüfbericht für externe Serviceanbieter)
- Pinakes Bankenverband CCI – Qualifizierung Dritter
- PiTuKri Kriterien für die Bewertung der Informationssicherheit von CloudServices
- SOC System and Organization Controls
- Hubspot Incl. EU- Standort (Dublin, Ireland), Hauptsitz: 25 First Street, 2nd Floor, Cambridge, MA 02141, USA,: Dublin, Irland, ist eine Software, die ermöglicht, ein besseres Kundenservicemanagement wodurch die Kundendaten transparenter und ordentlicher bewahrt werden können und die Fehler bei der Nutzung der SaaS – Dienstleistungen schneller behoben werden können.
- Jira Service Management (Support) sowie Jira Software (Product Support) EU-Standort (Dublin, Ireland) sind Produkte der Atlassian Pty Ltd, Level 6, 341 George

Street, Sydney NSW 2000 Australien, die ermöglichen eine schnelle Fehlerverwaltung bei der Nutzung der SaaS – Dienstleistungen, Problembehandlung und ein operatives Projektmanagement, sowie eine Zuordnung von Kundenstammdaten.

- Strato AG, Otto-Ostrowski-Straße 710249 Berlin; Deutschland, ist der Webhoster für die Website von Kidling.
- Microsoft Deutschland GmbH, Walter-Gropius-Straße 5 80807 München Unterstützung von dem Mailserver der Kitalino GmbH. Für die unterschiedlichen Hilfeleistungen werden personenbezogene Daten erhoben, die ausschließlich zur Erfüllung der Anfrage dienen.
- sipgate GmbH, Gladbacher Straße 74 40219 Düsseldorf, Cloud-Telefonanlage für die Kundenbetreuung
- pipedrive Pipedrive OÜ, Mustamäe tee 3a, 10615 Tallinn Estland, CRM-System