Vertrag zur Auftragsverarbeitung kidesia GmbH

ZWISCHEN	Kita XY Strasse PLZ ORT Verantwortlicher - nachstehend Auftraggeber genannt
UND:	Kidesia GmbH Waldstätterstrasse 16 6003 Luzern Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Anwendungsbereich und Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmässigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmässigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 (7) DSGVO). Die Verarbeitung erfolgt, um die Nutzung der Software gemäss den Wünschen der Kindertagesstätten bzw. deren Personal und der Erziehungsberechtigten sicherzustellen. Dies umfasst insbesondere den Informationsaustausch zwischen den Kindertagesstätten bzw. deren Personal und den Erziehungsberechtigten sowie die Verwaltung des Softwarezugriffs und die Verbesserung der Softwareleistung. Die Bearbeitung der Personendaten wird auf das notwendige Mindestmass beschränkt, es sei denn, es wird ausdrücklich etwas anderes gewünscht.

2. Art und Zweck der Datenverarbeitung

Die kidesia Gmbh bietet einen cloud basierten Service an, um die vollständige Administration einer Kindertagesstätte zu vereinfachen. Die Verarbeitung erfolgt, um die Nutzung der Software gemäss den Wünschen der Kindertagesstätten bzw. deren Personal und der Erziehungsberechtigten sicherzustellen. Dies umfasst insbesondere den Informationsaustausch zwischen den Kindertagesstätten bzw. deren Personal und den Erziehungsberechtigten sowie die Verwaltung des Softwarezugriffs und die Verbesserung der Softwareleistung.

3. Art der personenbezogenen Daten

Die zu verarbeitenden personenbezogenen Daten umfassen folgende Kategorien:

- Kontaktdaten (z.B. Name, Adresse, Telefonnummer, E-Mail-Adresse)
  von MitarbeiterInnen, Kindern, Geschwistern, Erziehungsberechtigten und Notfallkontakte/Abholberechtigten Personen
- Geschlecht und Geburtsdatum der Kinder
- Gesundheitsdaten der Kinder
- Allgemeine Personendaten
  Weitere personenbezogene Daten, die für den Betrieb und die Nutzung der Software notwendig sind.

4. Kategorie betroffener Personen

Folgende natürliche Personen sind von der Datenverarbeitung im Rahmen der Softwarenutzung betroffen:

(a) Erziehungsberechtigte Personen

(b) Kinder und deren Geschwister

(c) Notfallkontakte/Abholberechtigte Personen

(d) MitarbeiterInnen der Kindertagesstätte

5. Kategorie der personenbezogenen Daten

(1) Allgemeine Personendaten

(2) Besonders schützenswerte Daten:
Gesundheitsdaten der Kinder welche notwendig zur Leistungserbringung durch die Kindertagesstätte sind

6. Gegenstand und Dauer des Auftrags

Der Gegenstand und Dauer des Auftrags sind im Lizenzvertrag festgehalten.

7. Erbringung der Leistung in örtlicher Dimension

Die Erbringung der vertraglich vereinbarten Leistungen findet ausschliesslich in der Schweiz statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

8. Technisch organisatorische Massnahmen

Wir stehen in einem Auftragsverhältnis mit der Nine Internet Solutions AG (Hosting-Anbieter). Die technisch-organisatorischen Massnahmen werden somit von der Nine Internet Solutions AG gewährleistet. Durch die Unterschrift des Vertrags erklärt sich der Auftraggeber damit einverstanden, dass die Nine Internet Solutions AG als Unterauftragsbearbeiter Personendaten bearbeitet, welche dem Auftragnehmer vom Auftraggeber zur Verfügung gestellt worden sind. Die nachfolgenden Ausführungen sind zur Kenntnisnahme.

> *«(1) Der Auftragnehmer dokumentiert die Umsetzung der erforderlichen technischen und organisatorischen Massnahmen.*
>
> *(2) Insgesamt handelt es sich bei den zu treffenden Massnahmen um Massnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.*
>
> *(3) Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.*

Technische und organisatorische Massnahmen gemäss Art. 32 Abs. 1

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

- *Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen*
- *Zugangskontrolle: Keine unbefugte Systembenutzung*
- *Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems*

Integrität (Art. 32 Abs. 1 lit. b DSGVO), insbesondere kein unbefugtes Verändern oder Entfernen bei elektronischer Speicherung, Übertragung oder Transport:

- *Technische Systeme zur Verschlüsselung, elektronische Signaturen*
- *Organisatorische Vorgaben zur sicheren Datenlöschung*

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO), insbesondere der Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

- *Backups*
- *Brandschutz*
- *Unterbrechungsfreie Stromversorgung (USV)*
- *Firewall*

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO):

- *Meldewege*
- *Notfallkonzept/Notfallpläne/Notfallhandbuch*
- *Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)»*

9. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäss Art. 31 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

b) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Massnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

c) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

d) Der Auftragnehmer 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 Person gewährleistet wird.

e) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Massnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse dieses Vertrages.

10. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, Überprüfungen durchzuführen oder durch einen im Einzelfall zu benennenden Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangten Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu vernichten.

12. Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Massnahmen Dritter, etwa 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. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschliesslich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschliesslich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt.

(3) Dieser Vertrag unterliegt dem Schweizer Recht. Für alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag ergeben, ist ausschließlich das zuständige Gericht in Luzern zuständig.

CH-Luzern, 26. Juli 2023