Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gem. Artikel 28 EU-DSGVO

zwischen dem/der

Träger / Einrichtung

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

Kitalino GmbH

Pohlstraße 20

10875 Berlin

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Der Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich aus der Leistungsvereinbarung.

Die Auftragsverarbeitung bezieht sich auf die Zurverfügungstellung durch den Auftragnehmer der Online-Plattform DOKULINO und der dazugehörigen Modulen, welche der Auftraggeber u,a. zur Entwicklungsdokumentation von Kindern in den von dem Auftraggeber betriebenen Kindertageseinrichtungen einsetzt.

Die übrigen Einzelheiten des Auftrags sind der Leistungsvereinbarung sowie allgemeinen Nutzungsbedingungen zu entnehmen, auf die hier verwiesen wird.

1.2 Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der zugrundeliegenden Leistungsvereinbarung. Diese wird grundsätzlich für die Dauer eines Jahres geschlossen und verlängert sich automatisch um ein weiteres Jahr, wenn der Vertrag nicht von einer Partei mit einer Frist von einem Monat zum Ablauf der vereinbarten Laufzeit gekündigt wird.

2 Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftragnehmer stellt dem Auftraggeber den Zugang zum Online-Dienst DOKULINO und den dazugehörigen Modulen für die Entwicklungsdokumentation von Kindern in Kindertagesstätten zur Verfügung. Weitere Funktionen sind u.a. die Möglichkeit der Erstellung der Portfolios, sowie, bei der Zubuchung der entsprechenden Option, die Aufnahme von Kinderbildern durch Erzieher und Zurverfügungstellung von Bildern der Kinder an die jeweiligen Erziehungsberechtigten.Die Familien-App innerhalb der Kitalino-Plattform ermöglicht zudem den Erziehungsberechtigten die sichere Kommunikation mit der Kita-Leitung und Erziehern.

Im Rahmen dessen werden die personenbezogenen Daten der Kinder, der Erziehungsberechtigten, der Erzieher, und der Ansprechpartner der Einrichtung und Träger verarbeitet. Der Auftragnehmer hat nur auf Anweisung des Auftraggebers (z.B. zwecks Löschens oder Wiederherstellens von Daten) unmittelbaren protokollierten Zugang auf personenbezogene Daten.

Die Daten der Ansprechpartner der Einrichtungen und Träger werden für die Verwaltung und Unterscheidung der Einrichtung verarbeitet.

Bei den Erziehern werden die Daten für die Benutzer- und Erzieherverwaltung verwendet.

Die Daten der Kinder werden zur Dokumentation deren Entwicklung durch die Erzieher verarbeitet. Diese erfolgt online. Dabei findet auf der DOKULINO-Plattform kein Webtracking im Sinne einer Profilbildung zu kommerziellen Zwecken, Einsatz von Cookies auf den Anwender-Systemen, Browser-Fingerprinting o.ä. statt. Die Entwicklungsbeobachtung wird mit Hilfe der standardisierten Beobachtungsbögen dokumentiert. Es besteht die Möglichkeit diese automatisch auszuwerten, sowie nach Beauftragung durch den Auftraggeber auch einrichtungsübergreifend auszuwerten. Es können auch Förder-Vorschläge angezeigt werden. Die Dokumentation der Entwicklungsbeobachtung spielt eine unterstützende Rolle für die Erzieher und Eltern. Weiterhin können zu Zwecken der Durchführung der Betreuung sowie Archivierungszwecken digitale Portfolios und erstellt werden.

Die Erstellung der Fotosammlungen und deren Zurverfügungstellung an die Erziehungsberechtigte dient den privaten Archivierungszwecken der Erziehungsberechtigten.

Die Familien-App dient der Übermittlung von Nachrichten und Terminen der Kita inkl. Übermittlung von Dokumenten der Entwicklungsdokumentation, wie z.B. ePortfolios oder anderen Medien an die Erziehungsberechtigten. Die Familien-App wird als Progressive Web App angeboten, d.h. diese wird direkt über einen Browser verfügbar.

2.2 Ort der Verarbeitung

1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder ggf. in einem Drittland statt.
2) Die Daten der Kinder (siehe unter 2.3 Daten der Kinder) werden ausschließlich in einem Mitgliedsstaat der Europäischen Union verarbeitet. Die Verarbeitung in einem Drittland wird ausschließlich dann durchgeführt, falls die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

.

2.3 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

1. Stammdaten

   - Name, Anschrift und Kontaktdaten des Auftraggebers

2. Userdaten, Beobachtungsdaten

   a) Kontaktdaten der Mitarbeiter des Auftraggebers

   - Vorname, Name der Ansprechpartner des Trägers (vom Landesverband etc., wenn einschlägig),
   - Vorname, Name, E-Mail, Zugangsdaten der Mitarbeiter in der jeweiligen Kindergartengruppe – Erzieher, Leiter,

   b) Kontaktdaten der Erziehungsberechtigten (Vorname, Name, E-Mailadresse, Handynummer)

c) Daten der Kinder:

- Dokumentationsdaten (Vorname, Nachname, Nationalität, Erstsprache, Zweitsprache, Einschätzungen der BetreuerInnen, Beobachtungsbogen und deren Auswertungen, die unter anderem Sozialdaten, Gesundheitsdaten (Sprachentwicklungsstand, motorische und kognitive Fähigkeiten) beinhalten
- schriftliche und bildliche Dokumentation von Aktivitäten, Fotografien, Video- und Audiodateien

3. Meta-/Kommunikationsdaten (innerhalb der Familien-App: Nachrichten zwischen Erziehungsberechtigten und Kitamitarbeiter, Kalendereinträge).
4. Nutzungsdaten (wann letzte Anmeldung stattgefunden hat)
5. Log- und Protokolldaten

Der Auftraggeber weist den Auftragnehmer darauf hin, dass unter den im Rahmen des Auftrags zu verarbeitenden personenbezogenen Daten in großem Umfang auch Sozialdaten nach § 67 Abs. 2 SGB X, § 35 SGB I, § 61 SGB VIII) und/oder Gesundheitsdaten als Daten besonderer Kategorien nach Art. 9 Abs. 1 DSGVO zu verarbeiten sind.

2.4 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Beschäftigte des Auftraggebers – Ansprechpartner des Trägers, Leiter und Angestellte der Einrichtungen, die DOKULINO oder andere vom Auftragnehmer angebotene Dienste verwenden
- Erziehungsberechtigte
- Kinder, deren Daten in den Einrichtungen dokumentiert werden

3 Technisch-organisatorische Maßnahmen

1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. 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 DS-GVO zu berücksichtigen
3) Der Auftragnehmer ist verantwortlich für die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen (Einzelheiten in Anlage 1).
4) 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.

5) 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.
6) Der Auftragnehmer weist die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrags nach.

7) Die Verarbeitung von Daten in Privatwohnungen ist dem Auftragnehmer gestattet. Der Auftragnehmer hat sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können.

4 Betroffenenrechte

Der Auftraggeber ist berechtigt, den Auftragnehmer in dokumentierter Weise anzuweisen, die Daten, die im Auftrag verarbeitet werden zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Ein eigenmächtiges Löschen ohne Weisung ist nicht vorgesehen.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
   Der Auftragnehmer hat einen Datenschutzbeauftragten berufen. Dieser ist unter datenschutz@kitalino.com erreichbar. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.
4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
5) 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 Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
6) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder 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.
7) 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.

8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6 Unterauftragsverhältnisse

1) Nicht als Unterauftragsverhältnisse sind solche Dienstleistungen anzusehen, die der Auftragnehmer als reine Nebenleistungen zur Erfüllung der geschäftlichen Aufgaben in Anspruch nimmt, die nicht mit konkreten Bezug zur Erfüllung der Leistungen aus der Leistungsvereinbarung stehen z.B. CRM-Systeme, Abrechnungssysteme, Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice (wenn ein Zugriff auf personenbezogene Daten des Auftraggebers ausgeschlossen ist), oder Reinigungsdienste, Bewachungsdienste sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu:

Firma Unterauftragnehmer	**Anschrift/Land**	**Dienstleistung**
noris Network AG	Thomas-Mann-Straße 16 - 20 90471 NürnbergDeutschland	Hosting der DOKULINO-Plattform (Verarbeitung der Kindsdaten und Stammdaten)
Mailjet SAS	13-13 bis, rue de l'Aubrac, 75012 Paris Frankreich	Versand von E-Mails (Verarbeitung von Stammdaten der Einrichtungen, keine Erziehungsberechtigtenkommunikation)
Smart Mobile Factory GmbH	Pohlstraße 20 10785 Berlin Deutschland	Softwareentwicklung und Support der Dokulino-Plattform

Dem Auftragnehmer ist die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragnehmer gestattet. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragnehmer (unter Angabe des Namen, der Anschrift sowie der vorgesehenen Tätigkeit des Unterauftragnehmers), wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen innerhalb von zwei Wochen nach erfolgter Änderungsanzeige Einspruch zu erheben., sofern er hierfür einen wichtigen Grund hat. Die Parteien regeln, dass in einem solchen Fall eine Möglichkeit gefunden werden soll, um die Einwände auszuräumen, etwa durch entsprechend weitgehende Verpflichtungen des Unterauftragnehmers. Falls die Parteien keine Einigung erzielen, steht dem Auftraggeber ein Sonderkündigungsrecht zu. Der Auftragnehmer wird den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählen. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

3) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss der

Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

4) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO). Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

5) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.
6) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
7) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
8) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7 Kontrollrechte des Auftraggebers

1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer (nach Terminvereinbarung) Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von derEinhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
2) Um das berechtigte Interesse des Auftragnehmers zu wahren, sollen die anlasslosen Stichprobenkontrollen nicht öfters als einmal jährlich stattfinden. Die Beseitigung von bei diesen Sichtproben festgestellten Mängeln darf im Nachgang kontrolliert werden.
3) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
   - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
   - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
   - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
   - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8 Mitteilung bei Verstößen des Auftragnehmers

1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
   - die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
   - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
   - die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
   - die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
   - die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9 Weisungsbefugnis des Auftraggebers

1) Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten.
2) Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrages und anschließend noch für drei Jahre aufzubewahren.
3) Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. In einem solchen Fall ist der Auftragnehmer nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber die Weisung geändert hat oder diese bestätigt. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.
4) Der Auftraggeber legt den oder die Weisungsberechtigten fest. Der Auftragnehmer legt Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

10 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 – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11 Schlussbestimmung

1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht das Schriftformerfordernis.
2) Es gilt ausschließlich deutsches Recht.
3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien werden die jeweils unwirksame Bestimmung durch eine wirksame ersetzen, die dem angestrebten Zweck möglichst nahekommt. Entsprechendes gilt, wenn eine Vertragsbestimmung undurchführbar sein oder der Vertrag eine Lücke aufweisen sollte.

Datum, Ort (Auftraggeberin)	Datum, Ort (Auftragnehmerin)
_____	_____
_____	_____
(Unterschrift Auftraggeberin)	(Unterschrift Auftragnehmerin)

ANLAGE 1:

Diese Anlage und der Auftragsverarbeitungsvertrag korrespondieren mit dem Hauptvertrag zwischen den Parteien vom [Datum, ggf. Vertragsname und Vertragsnummer einfügen]

Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

der Organisation

Kitalino GmbH

Pohlstraße 20

10875 Berlin

für die DOKULINO-Plattform

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die o.g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
▬ Alarmanlage	▬ Schlüsselregelung / Liste
▬ Automatisches Zugangskontrollsystem	▬ Empfang / Rezeption / Pförtner
▬ Türen mit Knauf Außenseite	▬ Besucherbuch / Protokoll der Besucher
▬ Chipkarten / Transpondersysteme	▬ Mitarbeiter- / Besucherausweise
▬ Absicherung der Gebäudeschächte	▬ Besucher in Begleitung durch Mitarbeiter
▬ Sicherheitsschlösser	▬ Sorgfalt bei Auswahl des Wachpersonals

Technische Maßnahmen	Organisatorische Maßnahmen
▬ Videoüberwachung der Eingänge	▬ Sorgfalt bei Auswahl Reinigungsdienste
▬ Klingelanlage mit Kamera	▭

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) 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	Organisatorische Maßnahmen
▬ Login mit Benutzername + Passwort	▬ Verwalten von Benutzerberechtigungen
▬ Anti-Viren-Software Server	▬ Zentrale Passwortvergabe
▬ Firewall	▬ Allg. Richtlinie Datenschutz und / oder Sicherheit
▬ Intrusion Detection Systeme	
▬ Einsatz VPN bei Remote-Zugriffen	

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	Organisatorische Maßnahmen
▬ Aktenschredder (mind. Stufe 3, cross cut)	▬ Einsatz Berechtigungskonzepte

Technische Maßnahmen	Organisatorische Maßnahmen
▬ Externer Aktenvernichter (DIN 32757)	▬ Minimale Anzahl an Administratoren
	▬ Verwaltung Benutzerrechte durch Administratoren

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.

Diese Angaben beziehen sich auf die Anwendung DOKULINO.

Technische Maßnahmen	Organisatorische Maßnahmen
▬ Trennung von Produktiv- und Testumgebung	▬ Steuerung über Berechtigungskonzept
▬ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	▬ Festlegung von Datenbankrechten
▬ Mandantenfähigkeit relevanter Anwendungen	▬ Datensätze sind mit Zweckattributen versehen

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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
n/a	n/a

Bei Recordings und Observations sind nicht direkt die Kinddaten gespeichert, sondern nur ein Verweis. Im Zuge der Microservices werden physisch getrennte Datenbanken eingeführt werden.

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

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	Organisatorische Maßnahmen
▬ Zugriff auf die Webplattform per https.	▬ Berechtigungs- und Rollenkonzept
▬ Einsatz von VPN	▭

2.2. 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	Organisatorische Maßnahmen
n/a	n/a

Die Plattform wird zur Verarbeitung der Daten bereitgestellt. Für die Eingabe von Daten ist ausschließlich der Auftraggeber verantwortlich.

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

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, Raidsysteme, Plattenspiegelungen etc.

Die DOKULINO-Plattform wird in einem ISO 27001 zertifizierten Rechenzentren von noris Network AG in Deutschland gehostet. Die Angaben bzgl. Verfügbarkeit und Belastbarkeit beziehen sich auf den Hosting-Anbieter.

Technische Maßnahmen	Organisatorische Maßnahmen
▬ Feuer- und Rauchmeldeanlagen	▬ Backup & Recovery-Konzept (ausformuliert) - nur für die Systemwiederherstellung -
▬ Feuerlöscher Serverraum	▬ Kontrolle des Sicherungsvorgangs
▬ Serverraumüberwachung Temperatur und Feuchtigkeit	▬ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
▬ Serverraum klimatisiert	▬ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
▬ USV, Netzersatzanlage	▬ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
▬ Schutzsteckdosenleisten Serverraum	▬ Existenz eines Notfallplans
▬ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	
▬ RAID System / Festplattenspiegelung / redundante Speicherorte	▬
▬ Videoüberwachung Serverraum	▬

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

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
▬ Software-Lösungen für Datenschutz-Management im Einsatz	▬ Interner / externer Datenschutzbeauftragter
▬ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	▬ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
▬ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	▬ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
	▬ Interner / externer Informationssicherheitsbeauftragter (Baden-IT)
▬	▬ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
▬	▬ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
▬	▬

Weitere Maßnahmen:

Berufung eines Datenschutzbeauftragten.

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz von Firewall und regelmäßige Aktualisierung	☐ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☐ Einsatz von Spamfilter und regelmäßige Aktualisierung	☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☐ Einsatz von Virenscanner und regelmäßige Aktualisierung	☐ Einbindung von ☐ DSB und ☐ ISB in Sicherheitsvorfälle und Datenpannen
☐ Intrusion Detection System (IDS)	☐ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	☐ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
n/a	Die datenschutzrechtlichen Aspekte werden im Entwicklungsprozess berücksichtigt.

4.4. Auftragskontrolle (Outsourcing an Dritte)

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.

Technische Maßnahmen	Organisatorische Maßnahmen
–	– Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
–	– Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
–	– Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
–	– Schriftliche Weisungen an den Auftragnehmer
–	– Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
–	– Verpflichtung zur Bestellung eines Daten-schutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
–	– Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
–	– Regelung zum Einsatz weiterer Subunternehmer
–	– Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Es findet eine sorgfältige Auswahl der Unterauftragsnehmer statt.

Ausgefüllt für die Organisation durch

Name	Michael Vogelbacher
Funktion	Datenschutzbeauftragter (Kitalino GmbH)
Rufnummer	+49 (0)171 9760 212
E-Mail	michael.vogelbacher@consileo.de