Datenschutzkonzept der Kinderzeit gUG

Präambel

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeiter, Kunden sowie Geschäftspartner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.
In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben. Außerdem beschreiben wir, mit welchen Maßnahmen wir die Sicherheit der Daten gewährleisten und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn Sie Fragen zu unseren Datenschutzpraxis haben. Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bei der Kinderzeit gUG bestehenden Verantwortlichkeiten.
Alle Mitarbeiter sind zur Einhaltung der Richtlinie verpflichtet. Sie richtet sich an:

- Unsere Verwaltung (Kontakt: Justina Benedik, j.benedik@kinder-zeit.com)
- Pädagogische Leitungen an den Schulen
- Ausgabepersonal in der Mensa, welches über ein online geleitetes System über Fremdanbieter (NT- Consult und MensaMax) Essensbestellungen von Schülerinnen und Schüler abließt
- den betrieblichen Datenschutzbeauftragten (DSB)

Dabei gelten folgende Grundsätze:

- Die DV-Hard- und Software sind für betriebliche Aufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust und Manipulation zu sichern.
- Eine Nutzung für private Zwecke bedarf der ausdrücklichen Genehmigung.
- Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
- Die für die Verarbeitungen der eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter (Benutzer) über diese Richtlinie informiert werden; das gilt auch für temporär Beschäftigte.
- Der Datenschutzbeauftragte berät bei der Umsetzung der Richtlinie und prüft deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie dem DSB auskunftspflichtig.

1. Der betriebliche Datenschutzbeauftragte

(1) Die Kinderzeit gUG hat nach Maßgabe des Artikels 37 DS-GVO einen betrieblichen Datenschutzbeauftragten (DSB) bestellt. Die Kontaktdaten des Datenschutzbeauftragten sind:
Bernd Bittner
Heidberghof 3
47495 Rheinberg
Tel.: 02843/90 70 9 -15
E-Mail: b.bittner@kinder-zeit.com

(2) Der DSB nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation wahr.

(3) Der Datenschutzbeauftragte unterrichtet und berät die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter. Im Falle risikoreicher Datenverarbeitungen steht der DSB dem Verantwortlichem beratend bei der Abschätzung des Risikos zur Seite. Der DSB berichtet unmittelbar der Unternehmensleitung.

(4) Der DSB wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl von der Unternehmensleitung als auch den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

(5) Das Unternehmen hat ein Verzeichnis über alle Verarbeitungsvorgänge zu führen. In jeder Fachabteilung wird mindestens einer Person die Verantwortung übertragen, die dafür notwendigen Informationen zu den Verfahren der jeweiligen Abteilung zusammenzutragen und diese entsprechend den Anforderungen des Art. 30 DS-GVO zu dokumentieren. Bei Unklarheiten hinsichtlich der gesetzlich geforderten Informationen kann der Datenschutzbeauftragte beratend hinzugezogen werden. Dem Datenschutzbeauftragten ist eine Kopie des Verfahrensverzeichnisses zu übergeben. Jeder Mitarbeiter kann sich unmittelbar mit Hinweisen,

Anregungen oder Beschwerden an den DSB wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

2. Beschaffung/Hard- und Software

(1) Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung der über die Verarbeitungen entscheidenden Person durch die zentrale DV-Beschaffung. Bereits bei der Auswahl von Hard-und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.
(2) Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist der Datenschutzbeauftragte rechtzeitig vorab von der anfordernden Stelle zu informieren. Die Beschaffung erfolgt erst nach Stellungnahme des DSB. Der DSB berät dahingehend, ob die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist.
(3) Private Hard- und Software dürfen nicht zur Verarbeitung personenbezogener Daten Verwendung finden. Die dienstliche Nutzung privater Hard- und Software im heimischen und außerbetrieblichen Bereich (z.B. private Notebooks) bedarf der Genehmigung durch die Geschäftsführung im Einzelfall.
(4) Der DSB führt ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme. Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. ist der DSB unverzüglich zu informieren.

3. Verpflichtung/Schulung der Mitarbeiter

(1) Jeder Mitarbeiter, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten.
(2) Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars (Datenschutz-Verpflichtungserklärung für Mitarbeitende) und unter Aushändigung der hier vorgestellten Datenschutzerklärung.
(3) Die jeweilige Verpflichtungserklärung ist zu den Personalakten zu nehmen.

4. Transparenz der Datenverarbeitung

(1) Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt der Datenschutzbeauftragte ein Verzeichnis von Verarbeitungen gem. Art. 30 DS-GVO.
(2) Der DSB ist bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren Bei standardisierten Erhebungen (z.B. Elternvereinbarungen zu Betreuungsangeboten und/oder zur Mittagsverpflegung) ist der Erhebungsbogen etc. dem DSB zur Abstimmung vorzulegen.
(3) Soweit der DSB feststellt, dass die beabsichtigte Verarbeitung einer Datenschutz-Folgenabschätzung unterliegt, teilt er dies umgehend mit. Das Verfahren darf erst nach Zustimmung des DSB durchgeführt werden. Im Zweifel entscheidet die Geschäftsleitung.
(4) Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DS-GVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DS-GVO Gebrauch, so erfolgt die zentrale Bearbeitung durch den DSB. Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Personalverwaltung erfüllt. Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können.

5. Erhebung/Verarbeitung von personenbezogenen Daten

(1) Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DS-GVO zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen. Weitere Erlaubnistatbestände, die den Umgang mit personenbezogenen Daten im Unternehmen legitimieren können, werden im Folgenden einzeln aufgelistet:

Wir erheben folgende Daten:

- Name, Anschrift, Telefonnummer und ggf. E-Mailadressen von Kindern und deren Eltern zur vertraglichen Gestaltung von Elternverträgen bei Betreuungs-und/oder Verpflegungsverträgen
- Bankverbindungen von Eltern, zur Vereinbarung von Lastschriften bei Betreuungs-und/oder Verpflegungsverträgen
- Name, Anschrift, Telefonnummer und soziale Daten bei dem Anschein/begründeten Verdacht von Kindeswohlgefährdung nach § 8a SGB VIII (Konzept zur Wahrnehmung des Schutzauftrags bei Kindeswohlgefährdung nach § 8a SGB VIII der Kinderzeit gUG)

(2) Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen.

(3) Vor Einführung neuer Arten von Erhebungen ist die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind.

(4) Die im Rahmen der Zweckänderung genutzten Abwägungs-Kriterien sind einzeln zu prüfen. Die Prüfung ist darüber hinaus auch zu einem ordnungsgemäßen Nachweis zu dokumentieren. Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

(5) Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der DSB zu kontaktieren.

6. Datenhaltung/Versand/Löschung

(1) Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern oder Cloudspeicher (z.B. Flashspeicher, Streamer-Bändern) bedarf der Genehmigung durch den DSB und der Registrierung durch die den Träger einsetzende Abteilung/Benutzer. Bei Netzwerken ist der DSB für die Sicherung der Daten verantwortlich, die auf dem Server gespeichert sind.

(2) Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. Notebook, Desktop-PC), ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook mit WLAN, Tablet), ist zumindest einmal wöchentlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerk zu überspielen. Die gewählten Datensicherungsmaßnahmen sind in dem Verfahrensverzeichnis zu dokumentieren.

(3) Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten.

(4) Der DSB ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren.

(5) Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist der Benutzer verpflichtet, dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht wurden.

7. Externe Dienstleister/Auftragsverarbeitung/Wartung

(1) Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist der DSB vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DS-GVO genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren. Entsprechendes gilt, falls die Kinderzeit gUG entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

8. **Sicherheit der Verarbeitung**

(1) Für jedes Verfahren sind eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen. Diese richten sich an der Art, dem Umfang, der Umstände und Zwecke der Verarbeitung sowie der Wahrscheinlichkeit des Eintritts einer solchen Gefahr.

(2) Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der Datenverarbeitenden Systeme ist ein allgemeines Sicherheitskonzept zu erstellen. Das Konzept orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risikoanalyse. Dieses Konzept ist maßgeblich für alle weiteren Verfahren. Neben dieser Richtlinie bestehen ergänzende Regelungen, die insbesondere zur Realisierung der Datensicherungsgebote des Art. 32 DS-GVO zu treffende Maßnahmen betreffen. Hierzu gehören u.a.

- Arbeitsanweisung zum datenschutzgerechten Versand von Datenträgern und zur Verschlüsselung von Daten
- Arbeitsanweisung zum Passwortverfahren
- Arbeitsanweisung zur Erteilung von Auskünften im Personalbereich
- Arbeitsanweisung zur PC- und Laptop-Nutzung
- Arbeitsanweisung Telearbeit/Home-Office

(3) Ferner ist die Verarbeitung von Personaldaten in einer Anzahl von Betriebsvereinbarungen näher festgelegt. Hierzu gehört u. a. die Vereinbarung über die Nutzung von Telekommunikation (Telefon, E-Mail, Internet) in der Kinderzeit gUG.

9. **Rechenschafts- und Dokumentationspflicht**

(1) Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, ist jederzeit unter der aktiven Anwendung einer nachvollziehbaren und schlüssigen Dokumentation nachweisbar.

Stand: 08. Mai 2018