Leitlinie zu
technischen und organisatorischen Maßnahmen
zur Datensicherheit

Inhalt

1. Vertraulichkeit

1.1. Zutrittskontrolle

a) Zutritt

Zutritt zu den Räumlichkeiten der Kita haben neben den MitarbeiterInnen nur die Vereinsmitglieder (also die Sorgeberechtigten der betreuten Kinder). Diesen ist der Code für die Eingangstüre bekannt. Weitere Personen, welche die Kinder abholen, nutzen die Türklingel und halten sich somit begleitet durch eine/n MitarbeiterIn in den Räumen auf. Gleiches gilt für Handwerker oder ähnliche Berufsgruppen.

b) Schlüssel

Schlüssel erhalten nur MitarbeiterInnen und Mitglieder des Vorstands. Das wird natürlich sorgfältig dokumentiert.

c) Überwachung

Es gibt weder eine Videoüberwachung noch eine Alarmanlage. Und auch Werksschutz oder Pförtner sind in der Einrichtung nicht vorhanden.
Das im selben Haus angesiedelte „Haus Martin“ ist allerdings zu jeder Zeit personell besetzt und Unregelmäßigkeiten würden bemerkt werden.

1.2. Zugangskontrolle

a) Analog

Schützenswerte Daten sind in verschlossenen Kästen im Büro gesichert. Der Zugang dazu ist der Leitung und deren Stellvertreterin, sowie dem Vorstand vorbehalten.

b) Digital

Der PC ist passwortgesichert. Dieses Passwort ist nur dem pädagogischen Personal und dem/der Vorstandsvorsitzenden bekannt.

c) Berechtigungen

Aufgrund der reduzierten Personenzahl ist sichergestellt, dass nur erforderliche Berechtigungen einem eingeschränkten Personenkreis eingeräumt werden. Sollte sich eine personelle Veränderung auf den genannten Positionen ergeben, werden die Informationen entsprechend weiter gegeben. Dies wird in den Personalakten der MitarbeiterInnen protokolliert. Der Zugriff auf diese Akten ist im Punkt 1.2.a) geregelt.
Eine periodische Prüfung der Berechtigungen entfällt, da diese nicht erforderlich ist.

d) Passwort

Es gibt eine Passwortrichtlinie, die besagt, dass ein Passwort:

- mindestens acht Zeichen hat
- davon mindestens zwei Buchstaben sind (unter Verwendung von Groß- und Kleinbuchstaben)
- mindestens zwei Ziffern oder Sonderzeichen
- keine (erkennbare) Systematik enthält, d.h. es erscheint wie eine zufällig erzeugte Zeichenfolge
- kein Wort einer bekannten Sprache ist.

Die Passwortkomplexität und der Passwortwechsel werden nicht technisch erzwungen.

e) Schnittstellen und mobile IT-Systeme

USB Ports sind gesperrt und bis auf eine Kamera und ein Kita-Tablet zur (Foto-) Dokumentation werden keine weiteren mobilen Datenträger genutzt.

f) Dienstleister

Aufgrund des Vereinszwecks zur pädagogischen Betreuung von Zwei- bis Sechsjährigen ist die Kooperation mit dem Jugendamt, Schulen und ähnlichen Institutionen unerlässlich. Die Kita Pinocchio e.V. geht davon aus, dass auch diese den Richtlinien gewahr sind.

1.3. Zugriffskontrolle

a) Berechtigung und Protokollierung

Aufgrund der geringen Personenzahl gibt es nur 3 Berechtigungsgruppen:

I. Nicht berechtigt
II. Pädagogisches Personal
III. Vorstandsvorsitz

Damit ist gewährleistet, dass Berechtigungen differenziert vergeben werden. Die so entstehenden Benutzerrollen werden, wenn nötig, reflektiert und angepasst.

Daraus folgt auch automatisch, dass die Rechte angepasst werden, wenn Personen ausscheiden. Denn die Passwörter werden geändert und die Schlüssel retourniert.

In weiterer Folge ergibt sich daraus, dass die Anzahl der Administratoren auf das Notwendigste beschränkt ist.

Zugriffe auf Anwendungen und/oder Daten werden nicht explizit protokolliert.

b) Löschen von Daten

Sobald Daten für die Erfüllung des Vereinszwecks nicht mehr erforderlich sind, werden diese gelöscht bzw. vernichtet. Dies erfolgt sowohl für digitale als auch für analoge Medien. Maßgebend ist hierfür der Zeitpunkt des Ausscheidens aus dem Verein (Schuleintritt oder Kündigung).

1.4. Trennung

Personenbezogene Daten zu Kindern, Vereinsmitgliedern oder MitarbeiterInnen werden auf einer separat verschlüsselten Festplatte gespeichert. Das stellt sicher, dass diese nur für die entsprechenden Benutzergruppen zugänglich sind und getrennt voneinander bearbeitet werden. Die Strukturierung der Daten erfolgt nach der Zugehörigkeit zum einzelnen Kind. Mitglieder haben nur das Recht, auf die eigenen Daten Einblick zu erhalten.

Es gibt kein Test-System, weshalb auf die Trennung von diesem zum Produktivsystem nicht geachtet werden muss.

1.5. Pseudonymisierung & Verschlüsselung

In dem seltenen Fall von Fallsupervision oder dem Heranziehen von Beispielen, werden die Kinder nicht beim korrekten Namen genannt, sondern mit einem Fantasienamen bedacht oder „Kind 1“, „Kind 2“ etc. genannt.

2. Integrität

2.1. Eingabekontrolle

Aufgrund der geringen Personenanzahl und der dabei gültigen Aufgabentrennung ist nachvollziehbar, wer an personenbezogenen Daten gearbeitet hat. Protokolle darüber werden nicht explizit ausgewertet.

2.2. Weitergabekontrolle

Personenbezogene Daten werden über spezielle Plattformen an die entsprechenden Institute kommuniziert. Da der Zugriff auf die Portale nur mit Passwort möglich ist, ist der Schutz der Daten während der Verarbeitung (während des Transports) gewährleistet.

3. Verfügbarkeit und Belastbarkeit

Eine unterbrechungsfreie Stromversorgung ist nicht vorhanden, außerdem entfällt die Klimatisierung für Serverräume. Gemäß der Brandschutzverordnung für Kindergärten sind Rauchmelder vorhanden.

Ein Konzept zur Datensicherung und Wiederherstellung ist aktuell nicht vorhanden. Es wird allerdings daran gearbeitet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Leitlinie

Der Vorstand hat sich mit den Regularien des EU- DSGVO auseinandergesetzt und entsprechende Maßnahmen veranlasst. Im Zuge dessen ist auch die vorliegende Leitlinie erarbeitet worden.

b) Überprüfung von MitarbeiterInnen Wissen

MitarbeiterInnen werden bei Aufnahme des Beschäftigungsverhältnisses zum Datenschutz aufgeklärt. Eine Auffrischung der Regularien erfolgt ein Mal jährlich im Zuge eines Teammeetings.

Alle MitarbeiterInnen haben mit ihrer Unterschrift bestätigt, die Datenschutzrichtlinien zur Kenntnis genommen zu haben und sich somit dem vertraulichen Umgang mit schützenswerten Daten verpflichtet.

Es ist kein Datenschutzbeauftragter benannt worden.

c) Weitere Maßnahmen und Richtlinien

Die Passwortabfrage ist vorab eingestellt, die USB Ports sind gesperrt und eine separat verschlüsselte Festplatte zur speziellen Speicherung personenbezogener Daten ist vorhanden.

Der Verein benötigt zur Erfüllung seiner Zwecke die personenbezogenen Daten seiner Mitglieder. Dabei gelten die Regelungen der EU-Datenschutzgrundverordnung sowie des Bundesdatenschutzgesetzes. Jedes Vereinsmitglied hat das Recht auf:

- Auskunft über die zu seiner Person gespeicherten Daten,
- Berichtigung der Daten, sofern diese unrichtig sind,
- Sperrung der Daten, wenn deren Richtigkeit nicht feststeht,
- Löschung der Daten, wenn die Speicherung unzulässig war oder wird, z. B. bei Austritt aus dem Verein (Recht auf Vergessen werden)
- Bereitstellung dieser Daten in einem gängigen Format (Recht auf Datenübertragung), Art. 20 DS-GVO.

Jedes Vereinsmitglied ist über den Umgang mit Daten im Kindergarten und über die Rechte und Pflichten jedes Einzelnen informiert. Durch diese breite Wissensbasis können Datenschutzverletzungen rasch erkannt und behoben werden. Es gibt dabei keinen spezifischen Prozess zur Durchführung von Datenschutz-Folgenabschätzungen.

Durch kurze Kommunikationswege und klare Verantwortlichkeiten ist sichergestellt, dass Anfragen von Betroffenen fristgemäß bearbeitet werden. Dabei gibt es kein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO

<u>Sonstige Maßnahmen:</u>
Im Zuge der Mitgliederversammlung wurden die Mitglieder darauf hingewiesen, welche Richtlinien und Maßnahmen durch die Vorgaben der DSGVO zu berücksichtigen sind. Dies ist im Protokoll der Mitgliederversammlung dokumentiert:

- Adressliste
  Diese dient nicht dem Vereinszweck und beinhaltet personenbezogene Daten.
  Es wurde zur Abstimmung gebracht, ob diese beibehalten werden soll.
  Einstimmig wurde dafür gestimmt.

- Messenger-Dienste und Facebook
  Einstellen von Fotos, Sprachaufnahmen oder Videos in geschlossenen Benutzergruppen von Messenger-Diensten oder in geschlossenen Gruppen in sozialen Medien wie Facebook ist nach aktueller Rechtsprechung selbst beim Vorliegen einer schriftlichen Einwilligung verboten.
  Es werden andere Messenger Dienste als Ersatz für WhatsApp geprüft.

- Smartphones und ähnliche Geräte von Eltern
  Es ist dem ErzieherInnen-Team im Einzelnen nicht möglich, das Vorliegen einer Fotoerlaubnis anderer Kinder und der MitarbeiterInnen im Blick zu behalten. Daher liegt die Verantwortung zur Einhaltung des Datenschutzes bei den Eltern.

  Eltern, die in der Einrichtung fotografieren oder filmen, ohne das Einverständnis der abgebildeten Personen, geraten in Konflikt mit den allgemeinen Rechtsvorschriften. Die Kita hat die Eltern darauf bereits aufmerksam gemacht.

Es ist Eltern nicht gestattet Fotos oder Videos in den Räumlichkeiten der Kita aufzunehmen und die Eltern wurden aktiv dazu aufgefordert, den Moment mit ihrem Kind ungetrübt und ungeteilt zu genießen und auf die Nutzung elektronischer Endgeräte zu verzichten.

Außerdem wurde an die Eltern appelliert, dass auch sie in der Bring- und Abholsituation der Kinder die Nutzung von Mobiltelefonen möglichst einschränken, um sich gut auf ihr Kind konzentrieren zu können. Die Eltern sind sensibilisiert, bei ihren Kindern darauf hinzuwirken, bei der Benutzung digitaler Medien die Rechte der anderen zu respektieren.

Es ist kein Datenschutzmanagementsystem (DSMS) implementiert worden.