Whitepaper 27

Digitalisierung in der Kinderbetreuung

Nutzen und Risiken von digitalen Strukturen und Prozessen und der damit verbundene Paradigmenwechsel im Datenschutz, der Informationssicherheit, dem Qualitätsmanagement und der Sicherheits-Regulatorik in KITAs und Kindergärten

MCSS AG
MioCloud
Solution Systems

Sicherheit durch Technologie.

INHALT

1 Extrakt

Die Kinderbetreuung in Deutschland befindet sich in einem Spannungsfeld zwischen neuen Herausforderungen in der Digitalisierung und steigenden Sicherheits- und Qualitätsanforderungen mit immer höheren Regulatorik-Verpflichtungen. Dazu kommen die Abgrenzungsfragen der Verantwortungsbereiche zwischen den Trägern und den Verantwortlichen in den KITAs und KIGAs.

Unterschätzt werden dabei oftmals die Auswirkungen einer professionellen Digitalisierung und den damit verbundenen Effekten auf Cybersicherheit, Datenschutz, Sicherheits- und Qualitätsmanagement. Die Ursachen hierfür sind fehlende Qualifikationen und teilweise ein fehlendes Problembewusstsein auf allen Ebenen der Organisationen.

Die Rechtsnormen in der Kinderbetreuung werden durch über 30 Gesetze, Verordnungen, Richtlinien und Leitlinien definiert. In der Gesamtheit sind die Inhalte auf über 2.800 Seiten dokumentiert. Ständig kommen neue Anforderungen z.B. im Hygienemanagement, im Datenschutz und der Cybersicherheit dazu. Die Verantwortlichen und Mitarbeitenden werden in der Gesamtheit deutlich überfordert (wodurch es zu Verstößen gegen § 3, 7, 8, 13 ArbSchG; BGV A 1; BGR A1; BGI 527 kommen kann). Folglich ergeben sich komplexe Fragen der persönlichen Haftung für das Management der Träger (siehe Kapitel 8 „Rechtsfolgen bei Nichteinhaltung der Rechtsnormen“).

Es ist davon auszugehen, dass der kritische Verantwortungsumfang der Beschäftigten in den meisten Kinderbetreuungseinrichtungen deutlich überschritten wird.

Die 4 „Pain Points“ in der Kinderbetreuung 2022

1 – Personalnotstand, kombiniert mit zunehmender Bürokratie und Regulatorik

In der Kinderbetreuung in Deutschland sind mehr als 30 Gesetze, Verordnungen und Richtlinien verpflichtend einzuhalten.

2 – Lücken in Schulungen und im Coaching der Mitarbeitenden (Rechtskonformität)

Seit 2006 wurden in der Kinderbetreuung über 300.000 Mitarbeitende eingestellt. Es fehlt an Schulungen für neue und bestehende Mitarbeitenden.

3 – Fehlende professionelle IT-Strukturen bei starkem Digitalisierungs-Druck

Entpsrechend einer repräsentativen Studie von KITA-Software ist von mehr als 60% der Module wegen fehlender Rechtskonformität abzuraten.

Der „Faktor Mensch“ macht über 70% der Sicherheits- und Qualitätsanforderungen aus

4 – Schwächen im Sicherheitsmanagement (Arbeitsschutz, Datenschutz, Cyberschutz, QM) →HAFTUNG

In der Kinderbetreuung in Deutschland sind mehr als 30 Gesetze, Verordnungen und Richtlinien verpflichtend einzuhalten.

Die Digitalisierung in der Kinderbetreuung macht Sicherheits- und Qualitätsmaßnahmen erforderlich

Digitale Ökosysteme können pragmatische und preisgünstige Lösungen sofort bieten

2 Kinderbetreuung in Deutschland

In Deutschland übernehmen die nicht-familiäre Kinderbetreuung in Kindergärten (KIGA) und Kindertagesstätten (KITA) öffentliche und freie Träger.

Zum 01. März 2021 gab es in Deutschland insgesamt 58.500 Kinderbetreuungseinrichtungen. Davon befanden sich rund 39.200 in freier sowie etwa 19.300 in öffentlicher Trägerschaft:

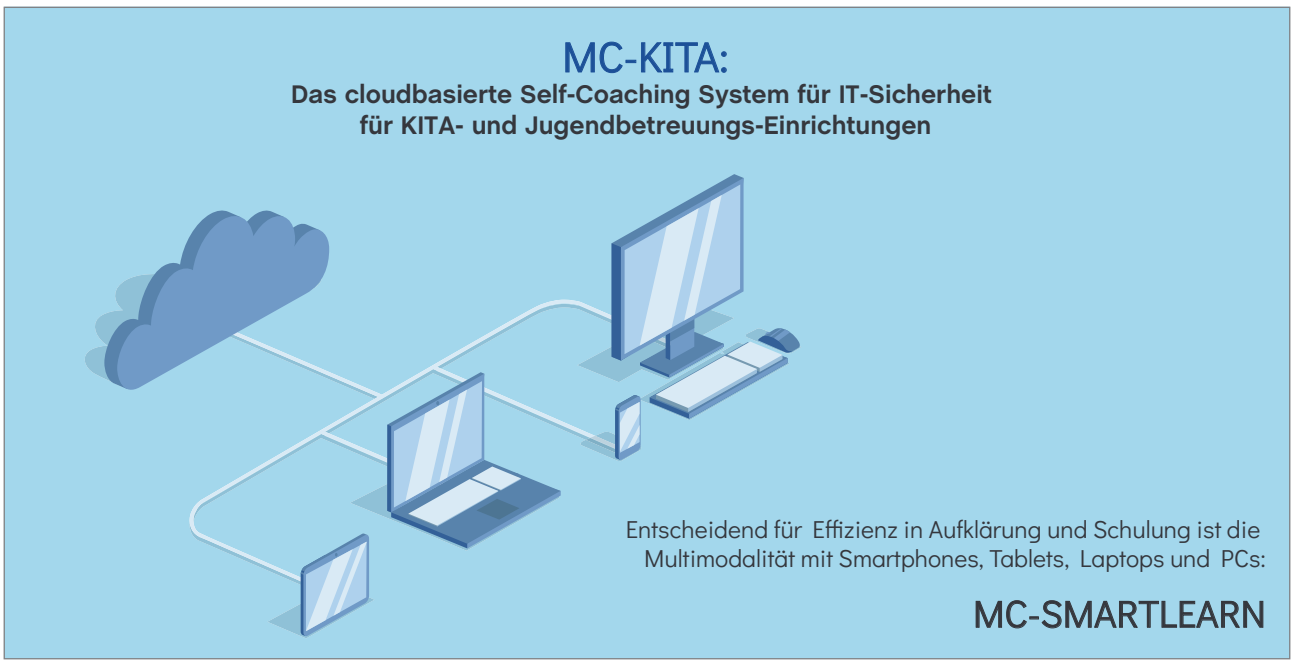
- Der „Markt“ der Kinderbetreuung steht vor großen Herausforderungen.
  Es bestehen Personalengpässe in vielen Einrichtungen.
  Nach unterschiedlichen Umfragen fehlen bis 2025 zwischen 30.000 – 70.000 Fachkräfte.
- Auf der anderen Seite ist der Personalbestand in der externen Kinderbetreuung von ca. 340.000 Mitarbeitenden im Jahr 2006 bis zum Jahr 2021 mit über 700.000 Beschäftigten mehr als verdoppelt worden. Insider sehen damit verbunden große Lücken im Coaching der Teams in KITAs/KIGAs im Qualitätsmanagement (Arbeitssicherheit und Unfallverhütung, Hygienemanagement und Infektionsschutz sowie Notfallmanagement).
- Um die Arbeitssituationen zu verbessern, wird bei allen Trägerorganisationen auf die Digitalisierung gesetzt. Software wird insbesondere in der Verwaltung und auch in der Schulung der Kinder eingesetzt. Angeboten werden etwa 40 spezielle Softwarepakete für die Administration (z.B. Personalplanung, Kommunikation, Abrechnungen etc.). Insgesamt wird geschätzt, dass ca. 40% der Einrichtungen professionelle digitale Systeme einsetzen (22.000+ Einrichtungen).
- Fachleute prognostizieren, dass jährlich etwa 15-20% der Kindergärten und KITAs in die Digitalisierung investieren. Im Jahr 2025 wird voraussichtlich 90-95% digital verwaltet.

3 Wandel durch Digitalisierung

3.1 Personalanforderung für die Digitalisierung

Die Einführung von IT-Systemen in der Kinderbetreuung stellt einen Paradigmenwechsel für die Arbeitsstrukturen und Abläufe dar. In vielen Fällen stehen keine eigenen internen Kapazitäten und Qualifikationen in den Einrichtungen zur Verfügung. Deshalb sind Dienstleistende vor Ort (DLO) einzusetzen. Aus finanziellen und rechtlichen Gründen ist die Auswahl des IT-Partners und die Vertragsgestaltung sorgfältig durch Fachleute zu prüfen.

Siehe auch Kapitel 6 zu Test von KITA-Software.



Die IT-Infrastruktur in KITA/KIGA wird zukünftig bevorzugt auf mobilen Endgeräten basieren und cloudbasierte Software-Anwendungen nutzen. Die Vorteile bestehen in günstigen Konditionen für SaS Angebote (Software as a Service) und in der Mobilität der Anwendungen mit Smartphones und Tablet Computern.

3.2 Rechtsgrundlagen des Digitalisierungsprozesses

In der Gesundheitsversorgung gibt es inzwischen konkrete Anforderungen der Digitalisierung. Dazu gehören u.a. die elektronische Patientenakte, das elektronische Medikamentenrezept und die digitale Arbeitsunfähigkeitsbescheinigung.

Vergleichbare Rechtsnormen gibt es in der Kinderbetreuung noch nicht. Die über 30 Gesetze, Richtlinien, Verordnungen und Leitlinien in der Kinderbetreuung lassen sich aber realistisch nur in digitalen Strukturen umsetzen. Die Verantwortung dafür liegt nach dem Arbeitsschutzgesetz beim Arbeitgeber (§§ 3, 8, 13 ArbSchG, BGV A 1). Insofern ist mittelfristig die Digitalisierung mit professionellen Lösungen alternativlos.

3.3 Budgets für die Digitalisierung

In einer KITA oder einem Kindergarten arbeiten statistisch durchschnittlich 10–14 Beschäftigte in Voll- und Teilzeit. Die gesamten Personalkosten pro Einrichtung betragen zwischen 450.000–500.000 Euro p.a. und in der gesamten Branche ca. 24,3–27,0 Mrd. Euro.

Durch die Digitalisierung kann die Produktivität in der Kinderbetreuung um schätzungsweise 5–6% gesteigert werden (weniger Papier, weniger Doppelarbeiten, Entlastung der Mitarbeitenden).
Die Aufwendungen für die Digitalisierung betragen nach Daten vergleichbarer KMU Strukturen etwa 1,25–1,50% des Jahresumsatzes.

Insgesamt werden die Träger für KITAs und Kindergärten im Jahr 2025 etwa 300–360 Mio. Euro pro Jahr für Software, Hardware, Providerkosten und IT-Dienstleistungen aufwenden. Grundlagen für die Berechnungen sind Leasing- oder Mietkosten für Hardware und SW-Lizenzen nach SaaS Modellen (Software as a Service).

Im Softwarebudget wird etwa 70% für Verwaltungsanwendungen und 30% für Organisations-, Qualitätsmanagement- und Compliance Anwendungen (ISMS, DSMS, QMS) aufgewendet werden.

3.4 Protokollierung nach DSGVO

Die Protokollierung nach DSGVO dient einerseits den Zwecken zur Erfüllung datenschutzrechtlicher Anforderungen, wie der Erteilung einer datenschutzrechtlichen Auskunft an die betroffene Person (Art. 15 DSGVO i. V. m. der Regelung des jeweils geltenden Landesrechts), andererseits der Gewährleistung der Sicherheit und der Verfügbarkeit des Systems (Art. 32 DSGVO) und dem Nachweis der Rechtmäßigkeit der Verarbeitung der verantwortlichen Stelle.
Außerdem dient die Protokollierung auch der Nachvollziehbarkeit der Verarbeitung bei einer Verletzung des Schutzes von besonderen (sensiblen) Daten (Art. 33, 34 DSGVO).

3.5 IT-Sicherheitsgesetz (IT-SiG 2.0)

Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist ein am 25.07.2015 in Kraft getretenes Gesetz und resultiert nach Angaben des Bundesinnenministeriums aus der im Februar 2011 beschlossenen Cyber-Sicherheitsstrategie.

Am 27.05.2021 wurde das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) im Bundesgesetzblatt verkündet (BGBl. I S. 1122).
Der überwiegende Teil des IT-Sicherheitsgesetzes trat damit am 28.05.2021 in Kraft.

3.6 Dokumentationsanforderungen in der Kinderbetreuung

Im Folgenden werden exemplarisch Anforderungen aufgelistet, die personenbezogene Daten enthalten, zu denen eine Dokumentation unerlässlich ist und die hinsichtlich des Datenschutzes nach DSGVO und BDSG schützenswert zu behandeln sind:

3.6.1 Arbeitsmedizinische Vorsorgekartei

Träger müssen eine Vorsorgekartei mit Angaben führen, wann und aus welchen Anlässen arbeitsmedizinische Vorsorge für Beschäftigte stattgefunden hat. Die Angaben der Vorsorgekartei sind grundsätzlich bis zur Beendigung des Beschäftigungsverhältnisses aufzubewahren und anschließend zu löschen. Bei Beendigung des Beschäftigungsverhältnisses hat der Arbeitgeber der betroffenen Person eine Kopie der sie betreffenden Angaben auszuhändigen.

3.6.2 Bildungs- und Entwicklungsdokumentationen

Die Dokumentation einer kindorientierten Entwicklungs- und Bildungsbegleitung erfolgt vor allem nach dem täglichen wahrnehmenden Beobachten des Kindes. Diese Erkenntnisse werden in Beobachtungs- und Entwicklungsbögen erfasst. Entwicklungs- und Bildungsdokumentationen dienen der Transparenz und erleichtern die Kommunikation zwischen den verschiedenen Akteuren, wie Träger, Personal, Elternschaft und externen Stellen, z. B. dem örtlichen Jugendamt oder dem zuständigen Landesjugendamt. Zudem dient diese Form der Dokumentation nicht zuletzt auch der Sicherheit der betreuten Kinder, da die Aktivitäten und Fördermöglichkeiten dem individuell ermittelten Entwicklungsstand angepasst werden können.

Entwicklungs- und Bildungsdokumentationen sowie die Weiterleitung dieser Daten an Dritte (z. B. eine Grundschule) setzen die schriftliche Zustimmung der Eltern voraus. Die Eltern sind darauf hinzuweisen, dass sie ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können.

Endet die Betreuung eines Kindes in der Kindertageseinrichtung, wird die Entwicklungs- und Bildungsdokumentation den Eltern ausgehändigt (vgl. § 18 Abs. 1 und 2 Kinderbildungsgesetz NRW).

3.6.3 Gefährdungsbeurteilung

Ein zentrales Element des Arbeits- und Gesundheitsschutzes stellt die Gefährdungsbeurteilung dar. Diese besteht aus einer systematischen Feststellung und Bewertung von relevanten Gefährdungen für das Personal und die Kinder. Innerhalb der Dokumentation werden zur Beurteilung und Festlegung von Maßnahmen auch Betriebs- und Geschäftsgeheimnisse festgehalten.

3.6.4 Medikamentengabe

Kinder mit chronischen Erkrankungen, z. B. Allergien, Diabetes, Epilepsie, Hämophilie, angeborene Herzfehler etc., können auf eine regelmäßige Einnahme von Medikamenten angewiesen sein.

Eine Kindertageseinrichtung, die diese Medikamentengabe unterstützt, kommt somit auch in den Besitz von vertraulichen Daten. Informationen über die Erkrankung des Kindes, ärztliche Verordnungen, die Art der Medikation und die Medikamenten-Einzelgaben liegen vor.

3.6.5 Notfall Dokumentation

Der Träger hat Vorkehrungen zu treffen, dass alle Personen, die einer unmittelbaren erheblichen Gefahr ausgesetzt sind oder sein können, möglichst frühzeitig über diese Gefahr und die getroffenen oder zu treffenden Schutzmaßnahmen informiert sind.

Schutzmaßnahmen zur Gefahrenabwehr, Personenrettung und Schadensbegrenzung sind im Vorfeld festzulegen. Hierzu werden Notfallpläne aufgestellt, die unter anderem auch Daten der zu beteiligenden Personen, z. B. private Rufnummern, enthalten können.

3.6.6 Unfall Dokumentation

Arbeits- und Wegeunfälle der Beschäftigten und Unfälle der Kinder sind zu dokumentieren. Bei leichteren Unfällen wie z. B. Schnitt- und Schürfwunden werden der Unfallhergang und die Erste-Hilfe-Leistungen z. B. in einem Meldeblock erfasst.

Bei schwereren Unfällen dient eine Unfallanzeige zur Dokumentation:

Bei Kindern, bei denen nach einem Unfall ein Arztbesuch erforderlich ist, muss eine Unfallanzeige erstellt werden.

Für Beschäftigte, die in Folge des Arbeits- oder Wegunfalls mit einer Arbeitsunfähigkeit von mehr als 3 Kalendertagen ausfallen, muss eine Unfallanzeige erstellt werden.

Die Unfallanzeigen sind der Unfallkasse des jeweiligen Landes zuzuleiten. Falls die verunfallte Person nicht kommunal beschäftigt ist, wird der Unfall der zuständigen Berufsgenossenschaft gemeldet. In der Regel ist dies die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege.

3.6.7 Datenbank zu Kindern mit chronischen Erkrankungen

Kinder mit chronischen Erkrankungen (siehe 3.6.4) benötigen im Notfall eine besondere Behandlung. Abgestimmt mit den Eltern und behandelnden Ärzt*innen sind alle relevanten Informationen digital und strukturiert (Standards nach ePA Vorgaben) zu speichern. Nach Entlassung der Kinder sind die Daten gesichert zu archivieren und nach der Aufbewahrungsfrist zu löschen.

3.6.8 Erfassung der Maßnahmen im Rahmen der Inklusion (Besuchskommission)

Die Inklusionsgesetze auf Landesebene regeln ein umfassendes Monitoring der KITAs und Kindergärten z.B. durch sogenannte Besuchskommissionen. Diese haben die Aufgabe und Berechtigung, in den KITAs und Kindergärten Audits durchzuführen. Dazu sind die Inklusionsmaßnahmen mit Nachweisdokumenten nach QM Gesichtspunkten zu erfassen und zu speichern.

3.6.9 Dokumentation zum Notfallmanagement mit Verantwortungsnachweisen

Das Notfallmanagement ist ein wesentlicher Bestandteil der Sicherheitsmaßnahmen in der KITA. Die Informationen sind so präzise wie möglich zu dokumentieren. Dazu gehören auch Zuständigkeitsdaten und damit persönliche Daten.

3.6.10 Daten zu Abhol-Berechtigten und zu Sorge- und Umgangsrecht bei Scheidungskindern

Das Abholen von Kindern aus der KITA und dem Kindergarten ist ein sensibler Datenbereich. Die Leitung muss dokumentieren, wer abholberechtigt ist und wer im Notfall autorisiert informiert wird.

3.6.11 Schulungs- und Nachweisdokumentation für alle Mitarbeitenden

Die Mitarbeitenden in der Kinderbetreuung müssen zu Rechtsnormen ausführlich und jeweils aktuell informiert und geschult sein. Die Qualifikationen müssen durch Nachweise in der Einrichtung dokumentiert werden.

Die nachzuweisenden Schulungen beziehen sich u.a. auf:

- Arbeitsschutz und Notfallmanagement
- Hygieneplan und Präventionsmaßnahmen
- Datenschutz (nach DSGVO komplett)
- Informationssicherheit und Cyberschutz (nach BSI)
- Inklusionsmanagement
- Qualitätsmanagement

Die rechtlichen Verpflichtungen sehen in den meisten Fällen regelmäßige jährliche Aktualisierungen der Schulungs- und Aufklärungsmaßnahmen vor. Deshalb ist die digitale Verwaltung mit Erinnerungsfunktionen empfehlenswert.

Die bei den verschiedenen Dokumentationsformen verarbeiteten personenbezogenen Daten müssen vor Missbrauch geschützt werden. Das bedeutet, dass diese gegen den Zugriff Unbefugter zu sichern sind.

4 Definitionen

4.1 IT-Sicherheit

Die IT-Sicherheit bezieht sich in der Kinderbetreuung auf den Schutz der IT-Infrastruktur von KITAs, Kindergärten und andere Betreuungseinrichtungen mit dem Ziel, wirtschaftlichen Schaden und Datenschutzverstöße zu verhindern. Es finden Werkzeuge wie Antivirenprogramme, Spamfilter und Passwortmanager ihre Anwendung.

4.2 Informationssicherheit

Die Informationssicherheit beinhaltet die IT-Sicherheit, erweitert diesen Begriff jedoch um die Sicherheit von nicht technisch gespeicherten und elektronisch verarbeiteten Daten. Um das Erreichen von Informations- und IT-Sicherheit messbar zu machen, werden sogenannte Schutzziele definiert.

Allgemeine Schutzziele sind dabei:

- Die Vertraulichkeit von Daten, dass keine Daten von unberechtigten Personen gelesen oder verändert werden dürfen, beispielsweise durch Richtlinien, Nutzergruppen und der Anwendung des sogenannten Need-to-know-Prinzips.
- Die Integrität von Daten, dass keine Daten unbemerkt verändert werden dürfen und jede Veränderung beispielsweise durch Logs nachvollziehbar belegt werden kann. Auch die Konsistenz von Daten, also der Abhängigkeit der Daten untereinander zählt zum Schutzziel Integrität.
- Die Verfügbarkeit von Daten, die in definierten Zeiträumen gewährleistet sein muss (beispielsweise Aufbewahrungsfristen medizinischer Daten und Informationen). Dieses Schutzziel wird unter anderem durch das Erstellen von regelmäßigen Datensicherungen (Backups), redundanter Datenhaltung und Langzeit-Archivierung erreicht.

4.3 Cyber-Sicherheit

Die Cyber-Sicherheit wird häufig entweder der Informationssicherheit gleichgesetzt oder dieser übergeordnet. Sie beinhaltet dann nicht nur die Sicherheit von Daten und der IT-Infrastruktur einer einzelnen Organisation, sondern bezeichnet den Sicherheitsbegriff umfassender bis hin zur nationalen oder globalen Sicherheit. Damit ist Cyber-Sicherheit als Prozess zur Implementierung von Kontrollen zu verstehen, mit dem die Eintrittswahrscheinlichkeit von Datenschutzverletzungen aus einem Cyber-Angriff reduziert werden kann.

Zusammenfassung für den Bereich der Kinderbetreuung:

IT-Sicherheit bezieht sich auf ein soziotechnisches System, in dem Informationen mit Hilfe von Informationstechnik (IT) erfasst, gespeichert und verarbeitet werden. IT-Sicherheit erhält durch die höheren Dokumentationspflichten der Kinderdaten eine deutlich größere Bedeutung.

Dagegen ist Informationssicherheit umfassender definiert und umfasst auch auf Papier dokumentierte Daten und Informationen.

4.4 Übergeordnete Definitionen

Art. 32 DSGVO Sicherheit der Verarbeitung

Stand der Technik

Der Terminus „Stand der Technik“, der in Art. 32 DSGVO verwendet wird, unterliegt einer ständigen Entwicklung. In der Rechtsprechung existieren verschiedene Definitionen wie z.B.

§ 3 Abs. 10 GefStoffV

Der ‚Stand der Technik’ ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Gesundheit und zur Sicherheit der Beschäftigten gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt worden sind.

Eintrittswahrscheinlichkeit und Schwere eines Risikos

Bei der Risikobetrachtung in der Informationssicherheit ist die Sichtweise auf die Kinder einerseits und auf die Verantwortlichen andererseits zu betrachten:

- **Risiken für Kinder**
  - Risiken der Sicherheit
  - Risiken der Versorgungsqualität
  - Risiken der Verletzung der Privatsphäre
- **Risiken für die Verantwortlichen (Träger und Leitung)**
  - Berufsrechtliche Risiken
  - Datenschutzrechtliche Risiken
  - Berufsrechtliche Risiken
  - Versicherungsrelevante Risiken

5 IT-Sicherheitsbereiche

Die IT-Infrastruktur in der Kinderbetreuung befindet sich in vielen Einrichtungen im Aufbau. Deshalb fehlen noch Standards für IT-Planungen für KITAs/KIGAs. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für Informationssicherheit und Cyberschutz Empfehlungen veröffentlicht, die in den Kinderbetreuungs-Einrichtungen angewendet werden können (z.B. BSI Grundschutz).
Für die Sicherheit sensibler Gesundheitsdaten hat das BSI in Kooperation mit der Kassenärztlichen Bundesvereinigung (KBV) eine Sicherheitsrichtlinie nach § 75b SGB V veröffentlicht. Die Inhalte können im Bereich der sensiblen Gesundheitsdaten (5.2.) in der KITA angewendet werden.

5.1 Datapoints Versicherer

In der KITA sind umfangreiche persönliche Daten zu Mitarbeitenden und Stellenbewerber*innen zu speichern und zu verwalten:

- Personalkartei für alle Mitarbeitenden
- Schulungs- und Nachweisdokumentation
- Bewerbungsmanagement für neue Mitarbeitende

5.2 ISAK Sozialwirtschaft

In den Bereich der professionellen Betreuung von Kindern gehört auch die Erhebung und Speicherung von sensiblen „besonderen Daten“ nach Art. 9 DSGVO:

- Informationen zu chronischen Erkrankungen und Behandlungsprozessen nach Health IT Standards (SNOMED, ICD)
- Informationen zu Notfallversorgungen in medizinischen Notfällen inkl. Benachrichtigungen
- Informationen zur Medikamentenabgabe mit PZN
- Abholberechtigungen und Informationen zu Sorgerechtsvereinbarungen
- Beobachtungsbogen/Beurteilung für Kinder

Die o.g. Daten sind besonders zu schützen. Außerdem sind genaue Informationen zu Löschprozessen nach Art. 17 DSGVO festzulegen.

ISAK = Informationssicherheits-Ausschöpfungskennzahl

Der ISAK Parameter visualisiert, in welchem Umfang die Möglichkeiten zur Gewährleitung der Informationssicherheit ausgeschöpft werden. Dazu werden Fragen zur einrichtungsinternen Sicherheitsstruktur und zu Sicherheitsprozessen beantwortet, Anwendungsprofile des **MCSS-Systems** protokolliert und nach globalen Risikobewertungen (Eintrittswahrscheinlichkeit und Schadensauswirkung) klassifiziert.

ISAK gibt Auskunft über den relativen Status der IT-Sicherheit und des Cyberschutzes.
Der Parameter hat eine Bandbreite zwischen 0,5 (ungenügend) und 1,2 (sehr gut) und ist die wesentliche Kennzahl der regelmäßigen Quartals- oder Halbjahresberichte.

ISAK von 0,6 kennzeichnet eine unzureichende Schutzsituation im Bereich der Informationssicherheit

ISAK von 1,2 repräsentiert die maximale Ausschöpfung relevanter technischer und organisatorischer Schutzmaßnahmen

6 KITA-Software im Sicherheitstest

KITA Software wird immer häufiger in der Kinderbetreuung genutzt. Allerdings zeigt eine Studie, welche Risiken damit verbunden sein können:

Aus T-Online News:

Kita-Apps: Studie warnt vor Sicherheitslücken

Von ella, dpa | 07.07.2022, 18:31

IT-Sicherheitsexperten haben in einer Studie 42 Kita-Apps vor allem aus Europa und den USA untersucht und dabei teilweise gravierende Sicherheitsmängel entdeckt. Ohne Einverständnis griffen mehrere Apps Daten ab und teilten diese mit Drittanbietern, bei einigen Apps war es den Forschern sogar möglich, auf Fotos von Kindern zuzugreifen. Das geht aus einem am Donnerstag veröffentlichten Papier hervor, für das unter anderem Wissenschaftler der Ruhr-Universität Bochum, des Max-Planck-Instituts für Sicherheit und Privatsphäre sowie Experten der IT-Sicherheitsfirma Aware7 aus Gelsenkirchen kollaborierten.

Kitas können mit solchen Apps beispielsweise Zeitpläne organisieren, Eltern können darüber mit Erzieherinnen und Erziehern kommunizieren oder Berichte über die Kindesentwicklung abrufen. Die 42 untersuchten Apps kamen insgesamt auf drei Millionen Downloads, aber gut zwei Drittel davon entfielen allein auf zwei Apps aus den USA.
Fast eine halbe Million Downloads verzeichnen die 16 auf dem deutschen Markt verfügbaren Apps, auch wenn die Downloads nicht alle von deutschen Nutzern kommen müssen. Dennoch werden Apps auch in Deutschland durchaus genutzt, so etwa künftig in den 42 Wiesbadener Kindertagesstätten, wie die Stadt am Donnerstag mitteilte.

Acht Apps, darunter vier deutsche, wiesen nach dem Ergebnis der Studie „gravierende Sicherheitsprobleme“ auf. Es war für Angreifer teilweise dort möglich, private Fotos der Kinder einzusehen. Indem sie selbst erstellte Konten hackten, fanden die Wissenschaftler die Schwachstellen.

Für gezielte Werbekampagnen sammeln und verkaufen fast alle Apps Daten an Drittanbieter wie Amazon, Facebook, Google oder Microsoft. Ein Kita-App-Anbieter legt beispielsweise offen, dass die durchschnittliche Anzahl der gewechselten Windeln pro Tag errechnet wird.

Studien-Mitautor Maximilian Golla sagte, dass sich ein „erschreckendes Bild“ in den Datenschutzerklärungen ergeben habe. Vor der Veröffentlichung wies das Team alle Hersteller auf Schwachstellen hin. Golla sagte, dass nur sechs der 42 überhaupt reagiert hätten.

Die Untersuchung beschränkt sich dabei auf Android-Apps, aber die Studienautoren vermuten, dass das Ergebnis bei anderen Anbietern wie Apple vergleichbar wäre.
Den Studienautoren zufolge waren zwölf der untersuchten Apps, darunter vier deutsche, unbedenklich und können laut den Experten empfohlen werden.

Die Studie macht deutlich, wie wichtig ein professionelle ISMS (Informationssicherheitssystem) und DSMS (Datenschutzmanagementsystem) ist. Informationen dazu veröffentlichte das Bundesamt für die Sicherheit in der Informationstechnik (BSI).

7 Mögliche Rechtsfolgen bei Nichterfüllung der Normen

7.1 Datenschutzrechtliche Folgen

Die negativen Rechtsfolgen aus Datenschutzverstößen aufgrund von Missachtung der geltenden Regelungen sind wahrscheinlicher als die Rechtsfolgen nach Berufsrecht. Die Abschreckung steht häufig im Vordergrund der Begründung.

Es wird darauf hingewiesen, dass die Regelungen auch der Konkretisierung der Pflichten nach Art. 32 DSGVO dienen (siehe 2.1. Definitionen und Geltungsbereiche).

7.1.1 Bußgeldverfahren nach Art. 83 DSGVO

Bei Verstößen gegen Art. 32 DSGVO können erhebliche Bußgelder verhängt werden.
Nach Art. 83 der DSGVO können Bußgelder bis zu 2% des Jahresumsatzes der Betreuungs-Einrichtung verhängt werden. Das sind für eine durchschnittliche Einrichtung etwas 10.000 Euro (die maximale Höhe beträgt 10 Millionen Euro, was aber in der Kinderbetreuung nicht relevant ist).

7.1.2 Schadensersatzzahlungen nach Art. 82 DSGVO

Eine unzureichende IT-Sicherheit in KITAs und Kindergärten kann zu erheblichen Schadensersatzzahlungen an die Eltern führen. Nach Art. 82 der DSGVO können durch Datenschutzverstöße geschädigte Personen Schadensersatzansprüche geltend machen. Dies gilt sowohl für materielle wie auch für immaterielle Schadensereignisse.

Fachleute sehen in den potenziellen Schadensersatzforderungen erhebliche Gefahren.
Dabei wird darauf hingewiesen, dass die zivilrechtlichen Ansprüche im Kontext der EU-Datenschutz-Grundverordnung abschreckende Wirkungen erzielen sollen. Da bislang keine gefestigte Rechtsprechung vorliegt, ist die Bandbreite der Zahlungen schwer einzuschätzen bzw. zu limitieren.
Ein weiteres Risiko ergibt sich aus der möglichen Beweislastumkehr, die Juristen im Kontext der Rechenschaftspflicht nach Art. 5 DSGVO als wahrscheinlich ansehen.

Fazit: Die Eintrittswahrscheinlichkeit ist nicht zu unterschätzen und auch die Schadenshöhe aus Sicht der Leitung und der Träger ist schwer kalkulierbar.

7.1.3 Meldepflichten nach Art. 33 DSGVO

Ein weiteres finanzielles Risiko ergibt sich aus § 33 DSGVO. Danach müssen die Verantwortlichen eine konkrete Datenschutzverletzung innerhalb von 72 Stunden nach Kenntnisnahme an die zuständige Datenschutz-Aufsichtsbehörde melden.

Bei der Meldepflicht einer Datenschutzverletzung kommt es nicht darauf an, ob die Leitung für einen Vorfall selbst verantwortlich ist. Ist der/die Auftragsverarbeitende (z.B. der/die Dienstleistende für die externe Datensicherung) involviert, so muss diese/r unverzüglich die Meldung des Vorfalls an die Einrichtungsleitung veranlassen. Somit kommt es bei der Meldepflicht nicht auf die Schuldfrage an.

Für die Meldeprozesse sind genaue Vorschriften veröffentlicht. Die Anforderungen ergeben sich aus Art. 34 DSGVO. Hinzu kommt die Regelung zur Benachrichtigung der betroffenen Personen.

Unterschieden wird nach einer Einzelbenachrichtigung und nach einer öffentlichen Benachrichtigung (z.B. in der Tagespresse). Aus letzterer kann sich ein erheblicher Reputationsschaden ergeben, der nur sehr schwer kalkuliert werden kann.

Meldepflichtverletzungen bei einer Datenschutzverletzung sind nicht selten. Bei Verlust großer Mengen von Personendaten, oder wenn Datensicherungsmedien mit sensiblen Daten öffentlich zugänglich werden, können Schäden im 6-stelligen Euro-Bereich entstehen.

7.2 Versicherungsrelevante Folgen

Im Bereich der IT-Sicherheit sind 3 Versicherungsbereiche relevant:

- Cyber-Versicherung
- Haftpflicht- und Berufshaftpflichtversicherung
- Betriebsunterbrechungs-Versicherung (BU)

Die steigende Gefährdung der Informationssicherheit in der Kinderbetreuung leitet einen Paradigmenwechsel auch für Versicherungen in der Personenbetreuung ein. Im Mittelpunkt steht die Digitalisierung mit den neuen Errungenschaften der computergestützten Betreuung von Kindern, aber auch mit zusätzlichen Risiken für IT-Sicherheit und Datenschutz.

Mögliche Folgen für Versicherte:

Kündigung des Versicherungsvertrags

Verletzt der/die Versicherungsnehmende vorsätzlich oder grob fahrlässig eine Obliegenheit, die er/sie vor Eintritt des Versicherungsfalls gegenüber der Versicherung zu erfüllen hat, so kann die Versicherung innerhalb eines Monats, nachdem sie von der Verletzung Kenntnis erlangt hat, den Vertrag fristlos kündigen.

Die Versicherung hat kein Kündigungsrecht, wenn der/die Versicherungsnehmende nachweist, dass er/sie die Obliegenheit weder vorsätzlich noch grob fahrlässig verletzt hat.

Leistungsfreiheit bei Obliegenheitsverletzungen

Verletzt der/die Versicherungsnehmende eine Obliegenheit vorsätzlich, so ist die Versicherung von der Verpflichtung zur Leistung frei. Bei grob fahrlässiger Verletzung der Obliegenheit ist die Versicherung berechtigt, ihre Leistung in dem Verhältnis zu kürzen, das der Schwere des Verschuldens des/der Versicherungsnehmenden entspricht.

Verletzt der/die Versicherungsnehmende eine nach Eintritt des Versicherungsfalls bestehende Auskunfts- oder Aufklärungsobliegenheit, so ist die Versicherung nur dann vollständig oder teilweise leistungsfrei, wenn sie die/den Versicherungsnehmende/n durch gesonderte Mitteilung in Textform (z. B. E-Mail, Telefax oder Brief) auf diese Rechtsfolge hingewiesen hat.

7.3 Förderrechtliche Folgen

Werden Fördermittel für die Digitalisierung in Anspruch genommen, so sind bei Nichteinhaltung der geforderten Nachweise Rückzahlungen und Sanktionen aufgrund von nicht korrekter Verwendung vorgesehen.

7.4 Risikoübertragung an Dienstleistende und Versicherungen

Der Gesetzgeber geht davon aus, dass in der Kinderbetreuung nicht immer ausreichende personelle Kapazitäten und Qualifikationen zur Umsetzung aller rechtlichen Anforderungen zur Verfügung stehen. Es ist deshalb vorgesehen, dass die Umsetzung des Risikomanagements auch an Dritte, wie qualifizierte Dienstleistende und spezialisierte Versicherungen mit entsprechenden Assistance Leistungen übertragen werden können.

8 Lösungen in der Umsetzung der Rechtskonformität

Wie dargestellt haben die Verantwortlichen und Mitarbeitenden in der Kinderbetreuung umfangreiche Rechtsnormen einzuhalten. Mit herkömmlichen analogen Mitteln wie Checklisten und Anweisungen auf Papier lassen sich die komplexen Anforderungen der etwa 30 Rechtsnormen nicht umsetzen. Diese Anforderungen stellen ohne digitale Hilfsmittel eine Überforderung nach dem Arbeitsschutzgesetz dar.

Bislang werden die unterschiedlichen Anforderungen an Qualitätsmanagement, Hygienemanagement, Sicherheits- und Notfallmanagement etc. in unterschiedlichen Systemen umgesetzt und auch von unterschiedlichen Aufsichtsbehörden kontrolliert. Tatsächlich haben die prozessorientierten Anforderungen viele Gemeinsamkeiten, die im Sinne der Nutzung von Synergien angewendet werden können.

Ein kombiniertes QM-System mit Datenschutz-, Informationssicherheit-, Hygiene- und Notfallmanagementsystem kann erhebliche Ressourcen sparen, da verschiedene Funktionen in der Organisation digital kombiniert werden können.

8.1 Organisatorische Maßnahmen

In den wichtigen Prozessbereichen in der Kinderbetreuung werden technische, organisatorische und auch rechtliche Maßnahmen umgesetzt. Dementsprechend bietet sich eine Synchronisierung der organisatorischen Strukturen und Prozesse in einer modernen digitalen Organisation an.

8.1.1 Verantwortungsbereiche und Rollen

Der erste Schritt eines konsolidierten und synchronisierten Prozessmanagements in KITAs/KIGAs ist die Definition der Verantwortungsbereiche und Rollen.

Es bietet sich an verschiedene Rollen unter Synergiegesichtspunkten zusammen zu fassen. Allerdings ist gerade in kleineren Organisationen darauf zu achten, dass keine Überforderung im Sinne des Arbeitsschutzes gegeben ist. In kleineren Einrichtungen ist es empfehlenswert externe Rollen zu definieren und zu vergeben. Das gilt z.B. für die Bereiche der Datenschutzbeauftragten (DSG) und der Informationssicherheitsbeauftragten (ISB).

Ebenso können Rollen in der Personensicherheit, dem Hygienemanagement und der Notfallplanung zusammengelegt werden.

Bei der Erstellung des gesetzlich verpflichtenden Hygieneplans ist im Regelfall externe Unterstützung durch Fachkräfte zu empfehlen.

8.1.2 Notfallplan und Notfallmanagement

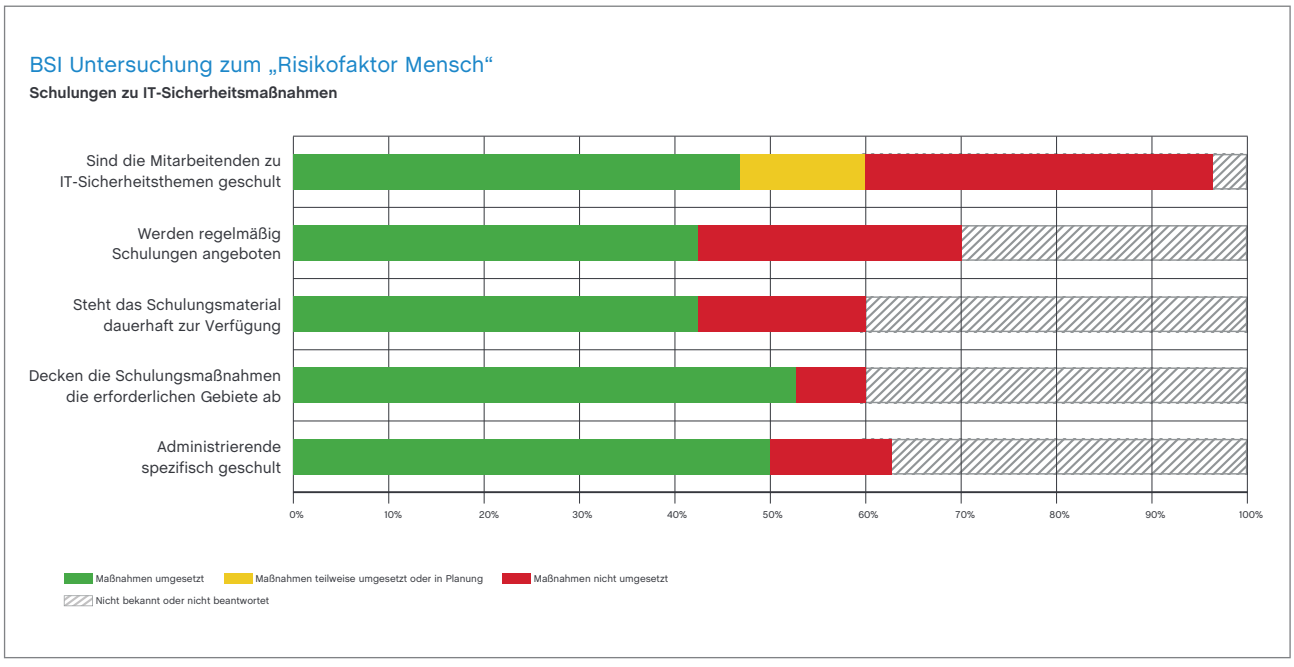
Die Bezeichnung Notfallmanagement wird in den Rechtsnormen unterschiedlich definiert. Im Rahmen des Qualitätsmanagements wird das Notfallmanagement häufig im Kontext der Personensicherheit definiert (z.B. Brand- und Unwetterschutz).

In den Rahmenbedingungen der IT-Sicherheit und des Cyberschutzes bezieht sich Notfallmanagement auf die Wiederherstellung der arbeitsfähigen IT-Infrastruktur nach einem Störfall. Dies ist besonders relevant bei kritischen Datenbeständen z.B. bei der Speicherung von Daten von Medikamentenabgabe und der Handlungsanweisungen für chronisch kranke Kinder.

In kleineren Einrichtungen kann das Notfallmanagement konzertiert betrachtet werden. Dies ist insbesondere im Zusammenhang mit dem übergeordneten Versicherungsmanagement (Haftpflicht-, Cyber- und Betriebsunterbrechungsversicherung) sinnvoll.

8.1.3 Awareness Coaching aller Mitarbeitenden

Für alle Prozessbereiche in der Kinderbetreuung gilt, dass bis zu 70% der Stör- und Schadensfälle auf den Faktor Mensch zurückzuführen sind. Dies wird durch Untersuchungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Gesamtverbands der deutschen Versicherungen (GDV) dokumentiert. Danach sind über 50% der Mitarbeitenden nicht ausreichend ausgebildet oder unvollständig informiert, wenn es z.B. um Pflichten für Informationssicherheit und Cyberschutz geht. Zur Gewährleistung der Rechtskonformität ergibt sich die Notwendigkeit einer konsolidierten Schulungs- und Coachingplanung. Ein übergeordnetes Curriculum (Schulungsplan mit Ausweis der Ausbildungsziele) kann je nach Reifegrad der KITA/KIGA auf 12–24 Monate ausgerichtet sein.



Da Zeitkapazitäten für klassisches Präsenzschulungen fehlen, werden immer häufiger E-Learning-Konzepte eingesetzt. So können die strukturierten Lerninhalte über mobile Endgeräte wie Smartphones und Tabletcomputer angeboten werden. Diese werden unter wissenschaftsbasierten Konzepten mit Multiple Choice Befragungen, Wissenstests und Erklär- bzw. Schulungsvideos ausgestaltet.

8.1.4 Digitale Managementsysteme

Herkömmliche Organisationsmittel wie analoge Dokumentensammlungen sind für ein zeitgemäßes Prozessmanagement ungeeignet. Es empfiehlt sich ein digitales, idealerweise cloudbasiertes System, das die Verfügbarkeit aller Prozessbeschreibungen, Verfahrensanweisungen und internen Regelungen für alle Mitarbeitenden gewährleistet und zur Verfügung stellt.

Datenschutzmanagement

- Kenntnisse der Rechtsnormen
- Datenschutzleitlinien & Richtlinien
- AV-Verträge
- Zustimmung zur Datenverarbeitung
- Weitergabe von Personendaten
- Geheimhaltung & Schweigepflicht
- Verbale Kommunikation im Datenschutz
- Verhalten bei Datenpannen

Informationssicherheits- und Cyberschutzmanagement

- Kenntnisse der Rechtsnormen
- Anwendung von Passwörtern
- Einsatz von Firewalls und Virenschutz
- Prävention Phishing Angriffe
- Privatnutzung Internet/eigene Geräte (Einsatz Internet-Anwendungen)
- Zutrittskontrolle, Zugangskontrolle, Zugriffs- und Weitergabekontrolle
- Kommunikation im Team
- Notfallmanagement IT-Sicherheit

Qualitätsmanagement

- Grundlagen QM
- Verantwortlichkeiten und Zuständigkeiten in der Einrichtung
- Mission und Vision
- Erhebung des Ist-Zustands hinsichtlich QM
- Wichtige Prozessbeschreibungen/Verfahrensanweisungen
- Teamkommunikation und -besprechungen
- QM und Rechtskonformität
- Optimierungsmanagement und PDCA

Notfallmanagement (übergeordnet)

- Zuständigkeiten im Notfall
- Brand- und Katastrophenschutz
- Evakuierungsplanung
- Notfallpartner KITA/KIGA
- Trauerbegleitung in KITA/KIGA
- Dokumentation & Nachbearbeitung von Notfällen

Hygiene- und Infektionsschutzmanagement

- Rechtliche Grundlagen zum Infektionsschutz
- Hygieneplan in der KITA nach §36 IfSG
- Hygieneplan in der Pandemie (Corona)
- Reinigungsplan in KITA und KIGA
- Hygiene im Sandkasten
- Umgang mit infizierten Kindern

Arbeitssicherheitsmanagement

- Aushangpflichtige Gesetze und gesetzliche Regelungen
- Verantwortungsbereiche in der Arbeitssicherheit (Sicherheitsbeauftragte)
- Gefährdungsbeurteilung der Arbeitsplätze in KITAs/KIGAs
- Sicherheit und Unfallschutz im Innenbereich
- Sicherheit und Unfallschutz im Außenbereich
- Verantwortungsbereiche Träger und Leitung

Gesundheitsmanagement

- Erfassung und Speicherung von Gesundheitsdaten
- Betreuung von Kindern mit chronischen Krankheiten
- Leitlinien für den KITA-Regelbetrieb in Corona Zeiten
- Umgang mit Erkältungs- und Krankheitssymptomen bei Kindern
- Erste Hilfe und Erstversorgung
- Splitterentfernung und Wundversorgung

Inklusionsmanagement

- Rechtsnormen und Definitionen zur Inklusion in der Kinderbetreuung
- Aufklärung der Mitarbeitenden zur Inklusion
- Bedarfsplanung für Inklusion in der Einrichtung
- Auditdurchführung für Inklusionsmaßnahmen
- Index für Inklusion in der Kinderbetreuung
- Klassifizierung und Dokumentation der Behinderungen

Nachhaltigkeitsmanagement

- Nachhaltiger Umgang mit Wasser
- Nachhaltiger Umgang mit Energie
- Umweltfreundliche Mobilität
- Nachhaltige Ernährung
- Abfallentsorgung und Umweltschutz
- Nachhaltiger Umgang mit der Natur

8.1.5 Key Risk Indicators (KRI) und Key Performance Indicators (KPI)

Die Träger der Kinderbetreuungs-Einrichtungen, vertreten durch Direktor*innen, Vorstände, Geschäftsführung, verantworten die Rechtskonformität in den Organisationen. Bei der Vielzahl von Gesetzen, Richtlinien, Verordnungen und Vorschriften ist es aber unmöglich, mit herkömmlichen Mitteln den Überblick zu haben. Hilfreich ist bei dieser Gemengelage zwischen Risiken, Personalnot und Budgetrestriktionen ein Frühwarnsystem für Sicherheitsgefahren und (persönliche) Haftungsrisiken.

Dazu sind KRI- und KPI-Modelle geeignet, die die Risiken und Konformitätsparameter relativieren und mit Dashboards visualisieren können.

8.1.5.1 Key Risk Indicators (KRIs)

KRIs werden von Organisationen verwendet, um zu bestimmen, welchem Sicherheits-Risiko sie ausgesetzt sind.

KRIs sind eine Möglichkeit, die größten Risiken, denen eine Einrichtung ausgesetzt ist, zu quantifizieren und zu überwachen. Durch die Messung der Risiken und ihrer potenziellen Auswirkungen auf die Sicherheit der Versorgung und der Sicherheit sind die Verwaltungen der KITAs, Kindergärten und Betreuungseinrichtungen in der Lage, Frühwarnsysteme zu schaffen, die es ihnen ermöglichen, wichtige Risiken zu überwachen, zu verwalten und zu mindern.

Effektive KRIs helfen:

- die größten IT-Risiken zu identifizieren
- diese Risiken und ihre Auswirkungen zu quantifizieren
- eine regelmäßige Risikoberichterstattung und Risikoüberwachung intern und extern (gegenüber Versicherern und Aufsichtsbehörden) zu ermöglichen

8.1.5.2 Key Performance Indicators (KPI)

Key Performance Indicators (KPIs) sind die Maßstäbe und Messungen, die eine Einrichtung verwendet, um zu verstehen, wie gut eine Organisation im Hinblick auf ihre strategischen und sicherheitsrelevanten Ziele abschneidet.

Sobald eine Einrichtung die Sicherheits-Ziele identifiziert hat, dienen KPIs als Überwachungs- und Entscheidungshilfen, die bei der Beantwortung der wichtigsten Leistungsfragen der Einrichtung helfen.

8.1.5.3 Die Beziehung zwischen KPIs und KRIs

Während KPIs Organisationen dabei helfen zu verstehen, wie gut sie in Bezug auf ihre strategischen Pläne abschneiden, helfen ihnen KRIs, die damit verbundenen Risiken und die Wahrscheinlichkeit, in Zukunft keine guten Ergebnisse zu erzielen, zu verstehen.
Dies bedeutet, dass KRIs die Kehrseite der KPIs sein können.

Drei Beispiele, die diesen Zusammenhang verdeutlichen:

- Eine Einrichtung kann einen KPI zur Messung der IT-Systemleistung und einen ergänzenden KRI zur Verfolgung der IT-Anfälligkeit für Cyberangriffe einrichten.
- Eine Einrichtung erstellt einen KPI, um die Qualität und Sicherheit zu überwachen, da dies wichtige Ziel sind. Ein mit dem gleichen Ziel verknüpfter KRI könnte die Risiken des Verlusts an Zufriedenheit der Eltern und Kinder überwachen.
- Eine Einrichtung kann Mitarbeitendenengagement oder Mitarbeitendenzufriedenheit als wichtige KPIs messen und die Wahrscheinlichkeit des Verlustes wichtiger Mitarbeitender und die Risiken für seine Arbeitgebermarke als KRIs überwachen.

KPIs und KRIs sind nicht dasselbe: KRIs helfen, Risiken zu quantifizieren, während KPIs helfen, die Versorgungsleistung zu messen.

Große Vorteile der Digitalisierung in der Kinderbetreuung bestehen in der Visualisierung von Schwachstellen und Optimierungspotenzialen. Dazu geeignet sind besonders grafisch dargestellte Indikatoren. Mit innovativer Software lassen sich Key Risk Indicators (KRI) und Key Performance Indicators (KPI) in Dashboards darstellen, intuitiv bewerten und in konkreten Maßnahmen umsetzen.
So können begrenzte finanzielle und personelle Ressourcen mit dem höchsten Wirkungsgrad eingesetzt werden.

8.1.6 Inventarisierung und laufende Dokumentation der IT-Umgebung

Die Digitalisierung in KITAs und Kindergärten steht noch am Anfang der Entwicklung. In den wenigsten Einrichtungen besteht ein professionelles Gesamtkonzept mit kompatiblen Datenmodellen und Schnittstellen für den Datenaustausch.

Die Standardanwendungen

- Personalverwaltung mit Personendatenbank (DSGVO relevant)
- Gruppen- und Einsatzplanung (DSGVO relevant)
- Buchhaltung mit Schnittstellen zu externen Partnern
- Abrechnung und Finanzplanung
- Datenverwaltung Kinderkonten (z.B. Chronische Erkrankungen, Medikamentenabgabe) (DSGVO relevant)
- Verpflegungsmanagement mit Catering-Planung (DSGVO relevant)
- Qualitätsmanagement mit Prozessverwaltung (z.B. ISO 9001)

Alle Anwendungen sind in einer IT-Inventur zu dokumentieren

- Netzwerk mit Hardware und mobilen Endgeräten
- SW Anwendungen
- Digitale Schnittstellen
- Internet-Anwendungen

Für digitalisierte KITAs und Kindergärten empfiehlt sich der Abschluss einer professionellen Cyberversicherung, die auch mit einem integrierten Assistenz-System verbunden sein kann. Zu den Obliegenheiten der Versicherten gehört eine IT-Inventarisierung nach o.g. Auflistung. Im Regelfall sind Dienstleistende vor Ort einzubeziehen, die auch als Informationssicherheitsbeauftragte (ISB) fungieren können.

8.1.7 Benchmarking und Monitoring

Der Status einer Prozessorganisation ist nur dann aussagekräftig, wenn ein Benchmarking als Steuerungssystem für das Management der Organisation (Träger und Leitung) und die risikotragenden Versicherungen transparent eingerichtet ist. Ein erster Schritt in die richtige Richtung ist die Messung des digitalen Reifegrades. Diese ist bislang allerdings auf Investitionsbedarf und weniger auf Risikobeherrschung ausgerichtet.

Ein solches übergeordnetes Benchmarking wird mit dem ISAK-System (Informationssicherheits-Ausschöpfungskennzahl der **MCSS AG**) angeboten. Die allgemeinen Datenpunkte entsprechen dem Fragenkatalog zu Cyber-Risiken des GDV.

8.2 Technische Maßnahmen

Zu den technischen Maßnahmen im Sinne der Informationssicherheit und des Cyberschutzes werden alle Anforderungen gezählt, die in einem ISMS nach BSI-Standard definiert sind.

Eine Mindestanforderung für KITAs und Kindergärten kann auch nach der Standardvorgabe des VdS 10000 und 10010 abgeleitet werden.

8.2.1 Schutzmaßnahmen mit Datensicherungen, Virenschutz, Firewall etc.

Mit der IT-Sicherheitsrichtlinie nach § 75b SGB V hat das BSI in Kooperation mit der Kassenärztlichen Bundesvereinigung (KBV) genaue Anforderungen für den Gesundheitsbereich (ärztliche Praxen) definiert. Die allgemeinen Anforderungen einer Einzelpraxis können analog auf KITAs und Kindergärten übertragen werden.

8.2.2 Pen-Testing

Das deutsche Bundesamt für Sicherheit und Informationstechnik (BSI) hat ein Klassifikationsschema entwickelt, anhand dessen sich ein Penetrations-Test (Pen-Test) beschreiben lässt.
Im Wesentlichen werden sechs verschiedene Kriterien auch für kleine und mittlere Unternehmen (KMU) betrachtet:

- Informationsbasis
- Aggressivität
- Umfang
- Vorgehensweise
- Technik
- Ausgangspunkt

Anhand dieser Kriterien wird zusammen mit dem Träger ein individueller Test zusammengestellt.

9 Visionen und Prognosen

Die Kinderbetreuung wird von der Gesellschaft als zunehmend wichtig wahrgenommen.
Durch die Pandemie wurde eine gesicherte und sichere Betreuung der Kinder (z.B. bis zu 8 Jahren) intensiv in der Öffentlichkeit reflektiert.

Die Anforderungen an eine zeitgemäße Betreuung werden durch die Digitalisierung und auch die damit verbundenen Risiken in der Cybersicherheit und im Datenschutz deutlich komplexer. Ein wirtschaftliches Risiko- und Sicherheitsmanagement lässt sich nur durch digitale Instrumente beherrschen. Der „Dschungel“ von über 30 Rechtsnormen auf etwa 2.500 Seiten lässt sich zuverlässig und wirtschaftlich nur noch durch digitale „Navigationssysteme“ beherrschen.

10 Rentabilitätsberechnung Compliance Management

Anforderungen	Kosten/ Std.	Standard* Std./Jahr	Ökosystem** Std./Jahr	Standard* Euro/Jahr	Ökosystem** Euro/Jahr	Vorteil Euro/Jahr
Datenschutz nach DSGVO						
Supervisor (für 50 Einrichtungen)	55,00 €	6	4	330,00 €	220,00 €	110,00 €
Leitung der Einrichtung	29,50 €	48	32	1.416,00 €	944,00 €	472,00 €
Mitarbeitende (8 MA)	23,00 €	64	32	1.472,00 €	736,00 €	736,00 €
SUMME		**118**	**68**	**3.218,00 €**	**1.900,00 €**	**1.318,00 €**
Informationssich. / Cyberschutz						
Supervisor (für 50 Einrichtungen)	70,00 €	6	4	420,00 €	280,00 €	140,00 €
Leitung der Einrichtung	29,50 €	24	16	708,00 €	472,00 €	236,00 €
Mitarbeitende (8 MA)	23,00 €	32	16	736,00 €	368,00 €	368,00 €
SUMME		**62**	**36**	**1.864,00 €**	**1.120,00 €**	**744,00 €**
Qualitätsmanagement						
Supervisor (für 50 Einrichtungen)	55,00 €	8	6	440,00 €	330,00 €	110,00 €
Leitung der Einrichtung	29,50 €	64	48	1.888,00 €	1.416,00 €	472,00 €
Mitarbeitende (8 MA)	23,00 €	384	240	8.832,00 €	5.520,00 €	3.312,00 €
SUMME		**456**	**294**	**11.160,00 €**	**7.266,00 €**	**3.894,00 €**
Notfallmanagement						
Supervisor (für 50 Einrichtungen)	55,00 €	6	4	330,00 €	220,00 €	110,00 €
Leitung der Einrichtung	29,50 €	24	16	708,00 €	472,00 €	236,00 €
Mitarbeitende (8 MA)	23,00 €	32	16	736,00 €	368,00 €	368,00 €
SUMME		**62**	**36**	**1.774,00 €**	**1.060,00 €**	**714,00 €**
Hygienemgmt. / Infektionsschutz						
Supervisor (für 50 Einrichtungen)	60,00 €	8	4	480,00 €	240,00 €	240,00 €
Leitung der Einrichtung	29,50 €	32	24	944,00 €	708,00 €	236,00 €
Mitarbeitende (8 MA)	23,00 €	128	64	2.944,00 €	1.472,00 €	1.472,00 €
SUMME		**168**	**92**	**4.368,00 €**	**2.420,00 €**	**1.948,00 €**
Arbeitssicherheitsmanagement						
Supervisor (für 50 Einrichtungen)	55,00 €	6	4	330,00 €	220,00 €	110,00 €
Leitung der Einrichtung	29,50 €	48	32	1.416,00 €	944,00 €	472,00 €
Mitarbeitende (8 MA)	23,00 €	128	64	2.944,00 €	1.472,00 €	1.472,00 €
SUMME		**182**	**100**	**4.690,00 €**	**2.636,00 €**	**2.054,00 €**
Gesundheitsmanagement						
Supervisor (für 50 Einrichtungen)	55,00 €	6	4	330,00 €	220,00 €	110,00 €
Leitung der Einrichtung	29,50 €	48	32	1.416,00 €	944,00 €	472,00 €
Mitarbeitende (8 MA)	23,00 €	128	64	2.944,00 €	1.472,00 €	1.472,00 €
SUMME		**182**	**100**	**4.690,00 €**	**2.636,00 €**	**2.054,00 €**
Inklusionsmanagement						
Supervisor (für 50 Einrichtungen)	55,00 €	6	4	330,00 €	220,00 €	110,00 €
Leitung der Einrichtung	29,50 €	48	32	1.416,00 €	944,00 €	472,00 €
Mitarbeitende (8 MA)	23,00 €	128	64	2.944,00 €	1.472,00 €	1.472,00 €
SUMME		**182**	**100**	**4.690,00 €**	**2.636,00 €**	**2.054,00 €**
Nachhaltigkeitsmanagement						
Supervisor (für 50 Einrichtungen)	55,00 €	4	2	220,00 €	110,00 €	110,00 €
Leitung der Einrichtung	29,50 €	24	16	708,00 €	472,00 €	236,00 €
Mitarbeitende (8 MA)	23,00 €	64	48	1.472,00 €	1.104,00 €	368,00 €
SUMME		**92**	**66**	**2.400,00 €**	**1.686,00 €**	**714,00 €**
Gesamt			600 Stunden eingespart		40% Personalkosten gespart	
Supervisor (für 50 Einrichtungen)		56	36	3.210,00 €	2.060,00 €	1.150,00 €
Leitung der Einrichtung		360	248	10.620,00 €	7.316,00 €	3.304,00 €
Mitarbeitende (8 MA)		1088	608	25.024,00 €	13.984,00 €	11.040,00 €
SUMME		**1504**	**892**	**38.854,00 €**	**23.360,00 €**	**15.494,00 €**

* mit analogen und einfachen digitalen Hilfsmitteln **mit **MC-KITA** (**MCSS** **Ökosystem**)

Die Rentabilitätsstudie basiert auf Daten in der medizinischen Versorgung.
Die Anforderungen an die Kinderbetreuung im Jahr 2022 entsprechen in wichtigen Bereichen den Anforderungen und organisatorischen Rahmenbedingungen in Arztpraxen (Einzelpraxen mit 5-10 Mitarbeitenden). Die Regulatorik für QM, Personensicherheit, Datenschutz, Cyberschutz, Hygienemanagement und Notfallmanagement sind in Arztpraxen und in KITAs/KIGAs direkt vergleichbar.

Das Optimierungspotenzial einer digitalen Gesamtlösung (cloudbasiertes Ökosystem) liegt nach einem Umsetzungszeitraum von 24 Monaten bei bis zu 40%. Die möglichen finanziellen Einsparungen und zeitlichen Entlastungen sind insbesondere für größere Träger in der Kinderbetreuung signifikant. In dem aufgeführten Beispiel können mehr als 600 Stunden jährlich bei einer Kostenersparnis von etwas 15.000 Euro optimiert werden.

Die Einsparungen ergeben sich in 4 Bereichen:

EINSPARPOTENZIALE	
1	Optimierung der Schulungsprozesse aller Mitarbeitenden durch E-Learning mit innovativen wissenschaftsbasierten und synchronisierten Wissensmodulen (z.B. Nutzung von Smartphones & Tablet Computer)
2	Ausschöpfung von Synergien in den einzelnen Arbeitsbereichen durch Zusammenlegung von Abläufen (integrierte PDCA Prozessanalyse z.B. Qualitäts- und Sicherheitsmanagement)
3	Nutzung erprobter Dokumentenvorlagen für Verfahrensanweisungen, Checklisten und Merkblättern (z.B. ISO 9001 kompatible digitale Muster)
4	Laufende Aktualisierung der Anforderungsprofile bei veränderten rechtlichen und technischen Rahmenbedingungen (z.B. zeitnahe und zeitoptimierte Umsetzung neuer RKI-Verordnungen)

11 Zusammenfassung

Die zunehmende Digitalisierung in der Kinderbetreuung bietet viele Potenziale für die optimierte und zeitgemäße Führung von KITAs und Kindergärten. Der Gesetzgeber hat dazu mit zusätzlichen Rechtsnormen neue Rahmenparameter definiert. Damit verbunden ist ein umfassendes „Change-Management“ in den Einrichtungen.

Ein Großteil der über 54.000 Betreuungseinrichtungen ist darauf weder personell noch organisatorisch vorbereitet. Dies wird besonders in der Umsetzung technischer und organisatorischer Maßnahmen zur Informationssicherheit und zum Cyberschutz deutlich.

1. Es gilt die Datenschutz-Grundverordnung (DSGVO) und insbesondere der Art. 32 zur „Sicherheit der Verarbeitung“ von sensiblen Daten in der Kinderbetreuung.

2. Die rechtlichen Rahmenbedingungen haben bei Nichteinhaltung der umfassenden Normen erhebliche negative Folgen. Sanktionen und Schadensersatzverpflichtungen können den Trägern der KITAs und Kindergärten entstehen.

3. Analysen machen deutlich, dass die Mehrzahl der Kindergärten und Kindertagesstätten nur unzureichend auf die zeitgemäßen Anforderungen vorbereitet ist. Die Gründe der Defizite: heterogene und unprofessionelle Infrastrukturen, fehlende Personalkapazitäten und mangelhafte Standardisierung.

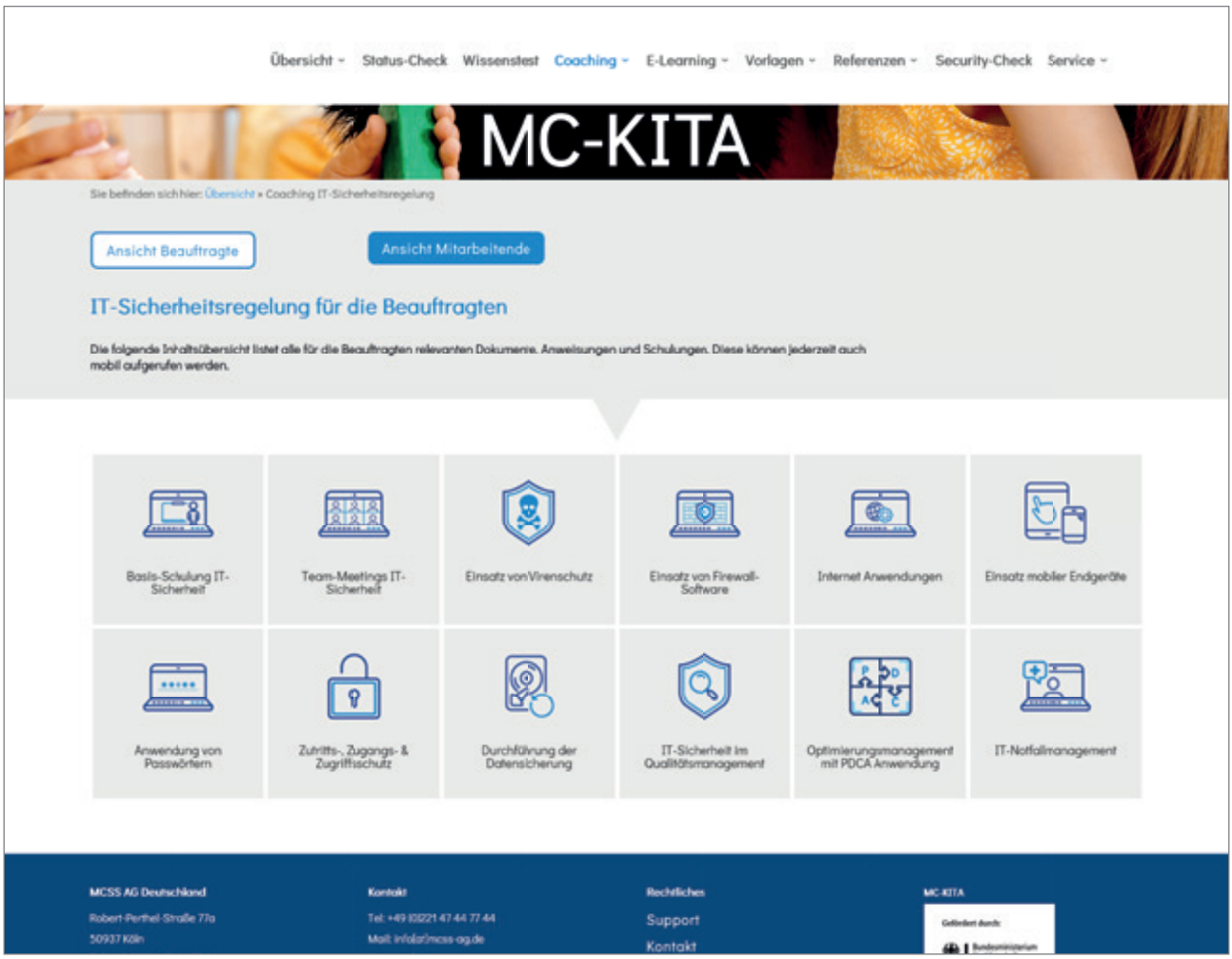
4. Die Gefahren durch Cyberattacken und andere IT-Störfälle sind in den Zeiten der Pandemie deutlich angestiegen und Versicherer berichten von signifikant höheren Schadenssummen. Fachleute befürchten eine weitere Steigerung in der Zukunft, weil die kriminelle Energie der Schadensverursacher mit innovativen technologischen Instrumenten (z.B. künstliche Intelligenz) kombiniert werden.

5. In diesem Umfeld wird Versicherungsmanagement in der Kinderbetreuung zu einem zentralen Baustein der Risikominimierung. „Hidden Cyber“ Strategien stellen Cyber-Versicherungen mit Haftpflicht- und BU-Policen in einen integralen Zusammenhang.

6. Wesentliche Bestandteile des Versicherungsmanagements werden zukünftig sogenannte „Assistance Dienstleistungen“ für die Versicherten sein. Mit digitalen Coaching Systemen und benchmark-basiertem digitalen Monitoring können Schadensrisiken für Versicherte und Versicherer in der nachweislich reduziert werden.

7. Der „Faktor Mensch“ ist ursächlich für bis zu 70% der Schäden durch IT-Sicherheitsvorfälle und Datenpannen verantwortlich. Dazu zeigen Untersuchungen (z.B. GDV), dass durchschnittlich bis zu 50% der Mitarbeitenden nicht oder nur unvollständig über Risiken und notwendige technische und organisatorische Maßnahmen aufgeklärt sind.

8. Der Paradigmenwechsel der KITA-Organisation von analogen zu digitalen Prozessen macht neue und kombinierbare Organisationsinstrumente erforderlich. Das Prozessmanagement für Informationssicherheit, Datenschutz (DSGVO/BDSG) und Qualitätsmanagement kann in einem digitalen System kombiniert werden und damit erhebliche Synergien realisieren (siehe z.B. das digitale **MCSS Ökosystem** im Gesundheitswesen).



9. Cloudbasierte Organisationslösungen, getrennt vom lokalen Netzwerk optimieren die Verfügbarkeit und können das Cyber-Risiko um bis zu 35% reduzieren und damit die Informationssicherheit signifikant erhöhen. (Cloud-Computing-Systeme nach § 19 Abs. 1 S. 1 Nr. 7 KHSFV)

10. Innovative Technologien wie Big Data Analysen, Machine Learning Konzepte bis hin zu KI-Anwendungen (künstliche Intelligenz) werden die Digitalisierung effektiv und im Sinne der Sicherheit und der Qualität gestalten können.

12 Die Autor*innen

Claudia Wente-Waedlich

Claudia Wente-Waedlich, Germanistin und Magister Artium (M.A.), ist Expertin für digitales Qualitätsmanagement und Kommunikation in der ambulanten und stationären medizinischen und sozialen Versorgung.

In ihrer 30-jährigen Berufslaufbahn hat sie mehr als 10.000 Mitarbeitende in Deutschland, den USA, Japan und China in innovativen Digitalisierungsprozessen begleitet.

Ihre Spezialgebiete sind die digitale Wissensvermittlung mit modernen Kommunikations-Strategien wie NLP (Neurolinguistische Programmierung) und die Nutzung von E-Learning Technologien mit Cloudanwendungen.

Claudia Wente-Waedlich war über 15 Jahre im Aufsichtsrat von Health IT- Unternehmen in Deutschland und USA tätig. Aktuell ist sie in der **MCSS AG, Köln** als Aufsichtsratsmitglied für den Bereich Qualitätsmanagement, Coaching und E-Learning verantwortlich.

Sabine Engel

Sabine Engel – Mutter, kreative und staatlich anerkannte Heilerziehungspflegerin. Aus Liebe zu Ihrem Sohn und aus Rebellion gegen die mangelhafte Umsetzung der Inklusion von chronisch Erkrankten und deren Anspruch auf Nachteilsausgleich ist sie Unternehmerin geworden.

Als “Social Entrepreneurin” belegte sie bei GRIID den zweiten Platz, erhielt ein Stipendium beim Social Impact Lab in Duisburg und hat es in den Kreis der 100 innovativsten Projekte Deutschlands geschafft.

Sie sieht sich in der Verantwortung eine gesellschaftlich nachhaltige Verbesserung der Inklusion von chronisch erkrankten Menschen zu erreichen, von haptischen Hilfsmitteln bis hin zur digitalen Unterstützung für Erkrankte und deren Betreuer/Begleiter des alltäglichen Lebens.

Sabine Engel hat aus ihrer langjährigen Tätigkeit als Heilerziehungspflegerin in stationären und ambulanten Bereichen Einblick in und Erfahrung mit Abläufen und Systemen von Einrichtungen. Ihr Anliegen ist es, digitale Strukturen zu nutzen, um ihren Kolleg*innen durch Aufklärung und Vereinfachung die Hilfe zu geben, die sie in der zeitgemäßen Kinderbetreuung und im Umgang mit chronischen erkrankten Kindern benötigen.

Arno Zurstraßen

Arno Zurstraßen, M.A. ist als Fachanwalt für Medizinrecht und Sozialrecht, Mediator und Supervisor in Köln niedergelassen. Mit seiner Erfahrung von über 25 Jahren berät er Ärzt*innen, Zahnärzt*innen, Praxisnetze und ärztliche Berufsverbände mit Schwerpunkt Rechtskonformität und Arzthaftungsrecht.

Die Umsetzung der umfangreichen Rechtsvorschriften für Ärzt*innen mit innovativen Konzepten und professionellen Technologien ist ein besonderes Credo für ihn.

Arno Zurstraßen berät Ärzt*innen auch bei Praxisabgaben oder -verschmelzungen. Dabei stützt er sich auf ein strukturiertes Projektmanagement, das er nach Qualitätsmanagement-Kriterien im Team mit IT-Fachleuten entwickelt hat.

Er ist Autor vieler Publikationen in der Fachpresse und bekannter Referent auf ärztlichen Kongressen.

Als Mitglied des Aufsichtsrats der **MCSS AG, Köln** gewährleistet er die rechtliche Kompatibilität innovativer digitaler Managementsysteme für die medizinische Versorgung.

Christian Schottmüller

Christian Schottmüller studierte Betriebswirtschaftslehre und Jura an der Universität zu Köln.

Seit dem Jahr 2008 ist er in verschiedenen Leitungsfunktionen für die Versicherungswirtschaft tätig und arbeitete dort seit 2014 unter anderem daran mit, Standards für die IT-Sicherheit im präventiven Bereich durch Informationssicherheits-Managementsysteme zu entwickeln. In seiner Laufbahn vermittelte er sein profundes Branchenwissen in zahlreichen Schulungen und Vorträgen.

Im Jahr 2021 übernahm Christian Schottmüller die Verantwortung für die Umsetzung von Cyberschutz und Informationssicherheit im Gesundheitswesen und in der Sozialwirtschaft als Direktor der **MCSS AG, Köln**.

13 Referenzen/Anlagen

- EU-Datenschutzverordnung Art. 32 DSGVO
- BS3-Standard nach BSI
- VdS Standard RL 10000 Informationssicherheit (ISMS) und VdS 10010 (DS)

Anmerkung

Das im Text erwähnte digitale **MCSS-System** (CPTF-S) wurde vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) im Rahmen eines ZIM Forschungs- und Innovationsprojekts gefördert und als Innovationsprojekt des Jahres 2022 vom Bundeswirtschaftsminister ausgezeichnet.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

ZIM
Zentrales
Innovationsprogramm
Mittelstand

MCSS AG
MioCloud
Solution Systems

A Weinsbergstraße 190
50825 Köln
T 0221/47 44 77 44
F 0221/47 44 77 55
E info@mcss-ag.de
W mcss-ag.de