Leitfaden
zur Einführung
einer Kita-App
in Kindertagesstätten

Herausgeber

Evangelisch-lutherische Landeskirche Hannovers
Das Landeskirchenamt
Referat 73 (Datenschutz)
Referat 52 (Kindertagesstätten)
Rote Reihe 6
30169 Hannover

Name	Position	Telefon	E-Mail
Annegret von Collande	Leiterin Referat Datenschutz	0511 1241-751	anne.voncollande@evlka.de
Arvid Siegmann	Leiter Referat Kindertagesstätten	0511 3604-381	arvid.siegmann@diakonie-nds.de

Dokumentenverantwortung

Dieses Dokument wurde von der Agentur für Datenschutz erarbeitet.

Name	Position	Telefon	E-Mail
Karoline Tancredi	Beraterin im Datenschutzrecht	0176 87858879	Karoline.Tancredi@agenturfuerdatenschutz.de

Versionsübersicht

Version	Datum	Beschreibung
1.0	08.12.2023	Erster Entwurf
1.1	22.01.2024	Abgestimmter Entwurf
2.0	05.04.2024	Abgestimmte Fassung

Vorwort

In den Kindertagesstätten der evangelischen Kirche schreitet der Prozess der Digitalisierung in großen Schritten voran. Immer mehr geraten Kita-Apps unterschiedlicher Funktionsumfänge in den Fokus. Dabei sind neben der Auswahl einer geeigneten Kita-App (mit dem gewünschten Funktionsumfang) auch rechtliche Aspekte zu beachten und vor Einführung der Kita-App umzusetzen. Dieser Leitfaden soll Ihnen einen ersten Eindruck über die zu treffenden datenschutzrechtlichen und IT-technischen Maßnahmen geben, die vor Einführung der App ergriffen werden sollten.

Dieses Papier richtet sich sowohl an die pädagogischen und betriebswirtschaftlichen Leitungen sowie an die Leitungen der Kindertagesstätten. Gleichzeitig soll das Papier den örtlichen Datenschutzbeauftragten als Hilfestellung dienen, die Einführung einer Kita-App datenschutzgerecht und sachkundig zu begleiten.

Weiterhin soll durch diesen Leitfaden die Komplexität der Einführung einer Kita-App aufgezeigt werden. Erfahrungsgemäß ist aktuell von mindestens einem Jahr Umsetzungsdauer von der ersten Zusammenkunft der Akteure bis zum finalen Einsatz der Kita-App zu rechnen.

Inhaltsverzeichnis

A DATENSCHUTZ-BASICS

I PERSONENBEZOGENE DATEN

1. Personenbezogene Daten gem. § 4 Nr. 1 DSG-EKD

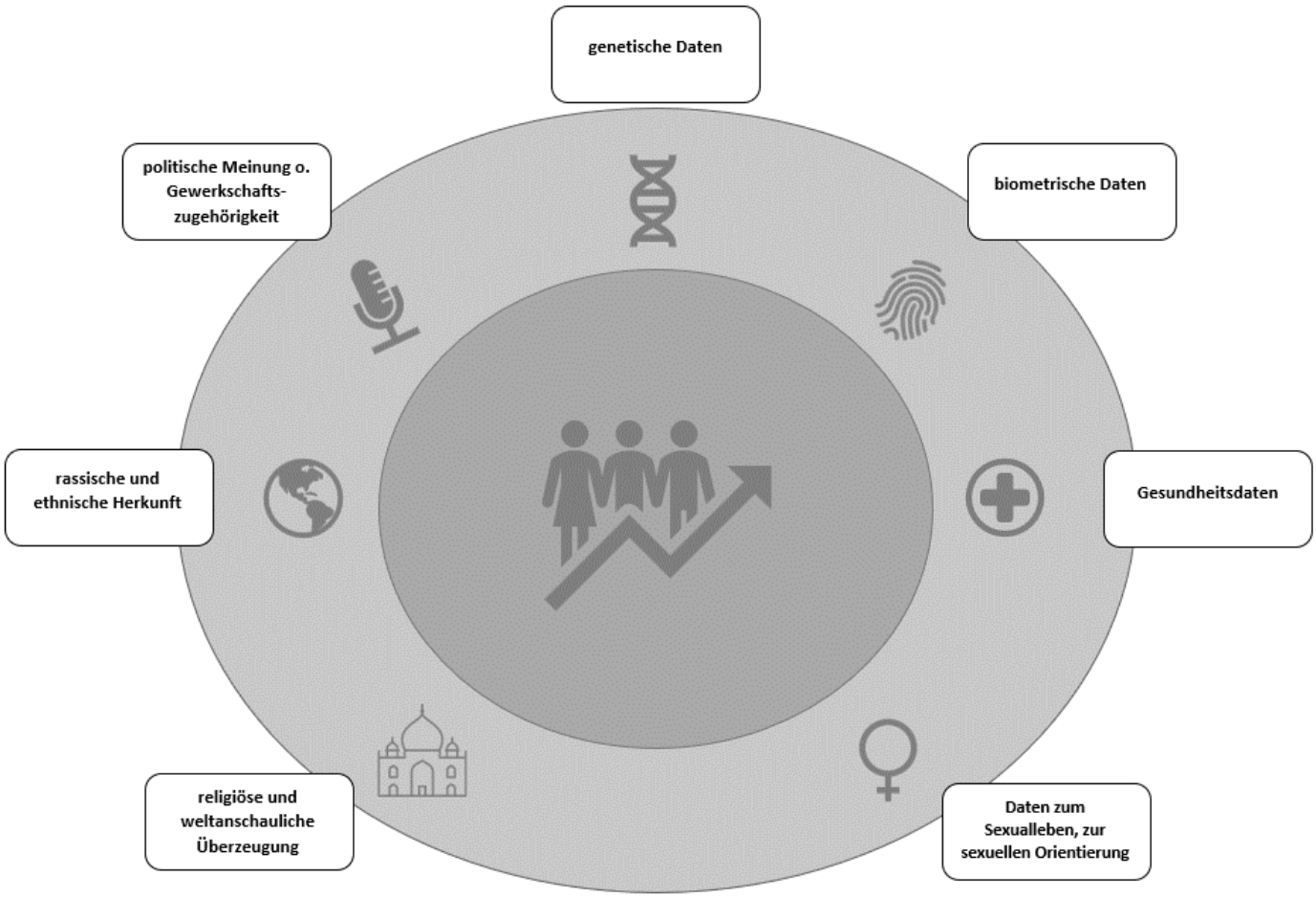
Personenbezogene Daten im Sinne des § 4 Nr. 1 DSG-EKD sind alle Informationen, die sich auf eine identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; identifizierbar ist eine natürliche Person, die direkt oder indirekt insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Um festzustellen, ob die betroffene Person identifizierbar ist, sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen hierfür verwendet werden können. [1]

Beispiele für personenbezogene Daten gem. § 4 Nr. 1 DSG-EKD:

[1] Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, Rn. 13;

2. Besondere Kategorien personenbezogener Daten gem. § 4 Nr. 2 DSG-EKD

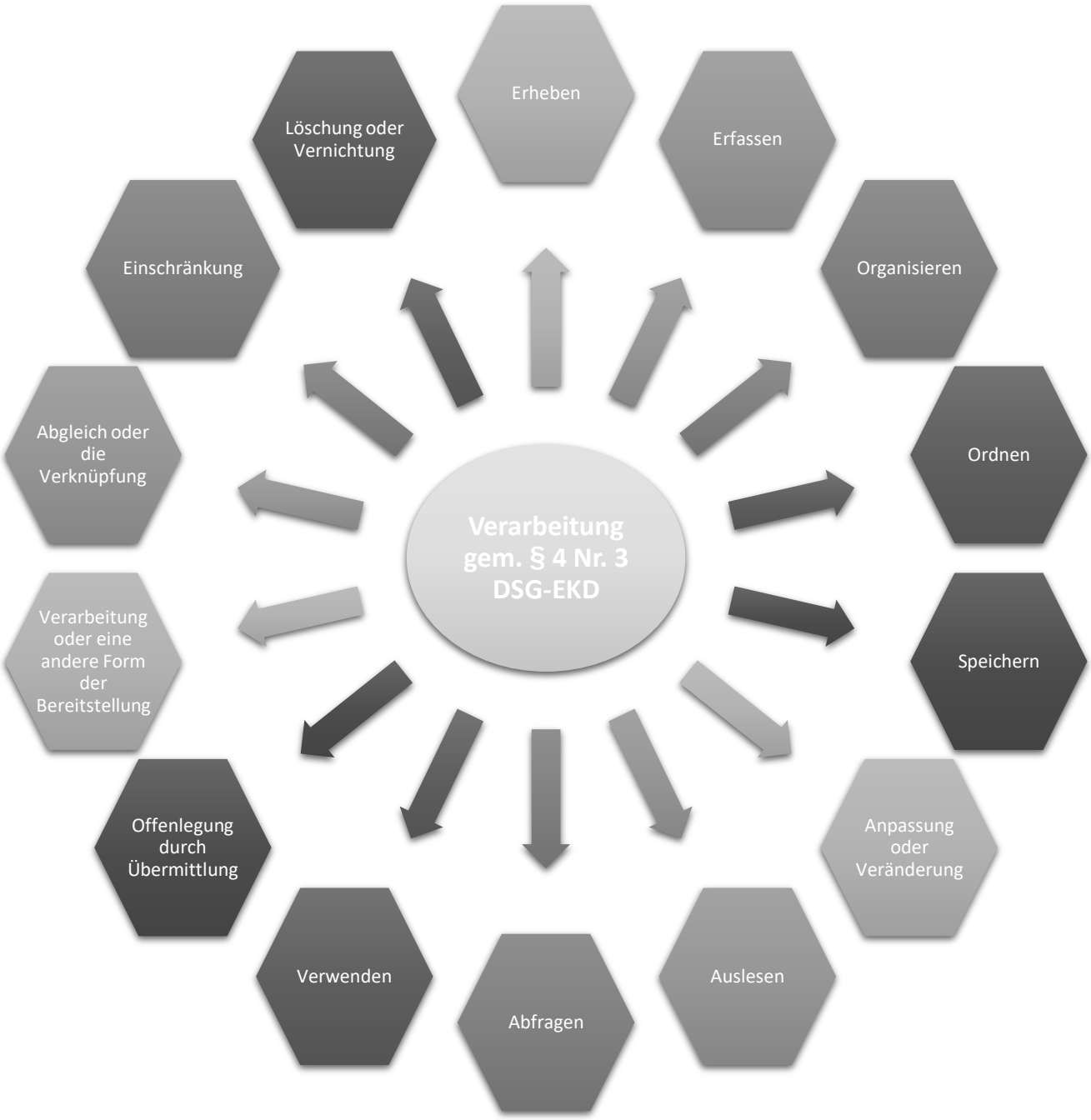
Neben den personenbezogenen Daten gem. § 4 Nr. 1 DSG-EKD bestehen die besonderen Kategorien personenbezogener Daten gem. § 4 Nr. 2 DSG-EKD. Diese sind als besonders schützenswert zu erachten, weil Sie aufgrund Ihrer Sensibilität ein hohes Potenzial für Diskriminierung bieten. § 13 Abs. 1 DSG-EKD normiert für die Verarbeitung der besonderen Kategorien personenbezogener Daten ein Verarbeitungsverbot. Danach ist die Verarbeitung personenbezogener Daten grundsätzlich verboten, außer es liegt einer der Erlaubnistatbestände aus § 13 Abs. 2 Nr. 1 bis 10 DSG-EKD vor.



II VERARBEITUNG GEM. § 4 NR. 3 DSG-EKD

§ 4 Nr. 3 DSG-EKD definiert den Begriff der „Verarbeitung“ als jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe in Zusammenhang mit personenbezogenen Daten. [2]

[2] Taeger/Gabel/Arning/Rothkegel DS-GVO Art. 4, Rn. 60-61;



Die Definition der Verarbeitung enthält 3 Voraussetzungen:

1) Ausführung eines Vorgangs oder einer Vorgangsreihe;
2) in automatisierter oder nicht automatisierter Weise;
3) im Zusammenhang mit personenbezogenen Daten.

1. Ausführung eines Vorgangs oder einer Vorgangsreihe

Ein ausgeführter Vorgang oder eine Vorgangsreihe setzt eine Handlung voraus, die zur Folge hat, dass etwas mit den Daten geschieht bzw. ein Umgang mit ihnen erfolgt. [3]

2. In automatisierter oder nicht automatisierteer Weise

Eine ganz oder teilweise automatisierte Verarbeitung liegt bereits dann vor, wenn eine Datenverarbeitungsanlage eingesetzt wird. Erfasst ist jede Form der Datenverarbeitungsanlage, also Computer jeder Größenordnung, Smartphones, Überwachungsanlagen, digitale Kopierer und Scanner etc. [4] Demgegenüber liegt ein nicht automatisierter Vorgang vor, wenn er ohne Hilfe von Datenverarbeitungsanlagen, also i.d.R. manuell erfolgt. [5] Soweit der Vorgang nicht automatisiert erfolgt, ist aber darauf zu achten, dass der Anwendungsbereich des DSG-EKD bei der nicht automatisierten Verarbeitung gem.§ 2 Abs. 1 DSG-EKD nur dann eröffnet ist, wenn personenbezogene Daten verarbeitet werden, die in einem Dateisystem i.S.d. § 4 Nr. 8 DSG-EKD gespeichert sind oder gespeichert werden sollen. [6]

3. Im Zusammenhang mit personenbezogenen Daten

Des Weiteren muss der/die (nicht) automatisierte Vorgang/Vorgangsreihe im Zusammenhang mit personenbezogenen Daten erfolgen. Dies ist der Fall, wenn die (nicht) automatisierte Handlung personenbezogene Daten i.S.d. § 4 Nr. 1 DSG-EKD betrifft. [7]

III RECHTMÄSSIGKEIT DER VERARBEITUNG

Der Grundsatz der Rechtmäßigkeit gem. § 5 Abs. 1 Nr. 1 DSG-EKD fordert, dass Daten ausschließlich auf eine rechtmäßige Weise verarbeitet werden dürfen. Dementsprechend fordert der Grundsatz der Rechtmäßigkeit, dass eine Datenverarbeitung ausschließlich aufgrund einer Rechtsgrundlage zu erfolgen hat.

[3] Taeger/Gabel/Arning/Rothkegel DS-GVO Art. 4, Rn. 62;
[4] Ziekow in Wagner (Hrsg.) EKD-Datenschutzgesetz § 2, Rn. 26;
[5] Taeger/Gabel/Arning/Rothkegel DS-GVO Art. 4, Rn. 63;
[6] Taeger/Gabel/Arning/Rothkegel DS-GVO Art. 4, Rn. 65;
[7] Taeger/Gabel/Arning/Rothkegel DS-GVO Art. 4, Rn. 66;

Die Rechtsgrundlagen der Datenverarbeitung sind in § 6 DSG-EKD aufgeführt:

Rechtsvorschrift **§ 6 Nr. 1 DSG-EKD**	• Die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten ergibt sich aus einer Rechtsvorschrift.
Einwilligung **§ 6 Nr. 2 DSG-EKD**	• Die Verarbeitung der personenbezogenen Daten ist rechtmäßig, wenn diese auf einer freiwilligen, bestimmten, informierten, zweckgebundenen und unmissverständlich erklärten Einwilligung beruht.
Erfüllung einer Aufgabe der verantwortlichen Stelle **§ 6 Nr. 3 DSG-EKD**	• Die Verarbeitung ist zur Erfüllung der Aufgaben der verantwortlichen Stelle, einschließlich der kirchlichen Aufsicht erforderlich.
Sonstige Aufgabe im kirchlichen Interesse **§ 6 Nr. 4 DSG-EKD**	• Die Verarbeitung ist für die Wahrnehmung einer sonstigen Aufgabe erforderlich, die im kirchlichen Interesse liegt.
Erfüllung eines Vertrages oder vorvertragliche Maßnahmen **§ 6 Nr. 5 DSG-EKD**	• Die Verarbeitung ist zur Erfüllung eines Vertrages oder für vorvertragliche Maßnahmen (Bewerbungsverfahren) notwendig.
Erfüllung einer rechtlichen Verpflichtung **§ 6 Nr. 6 DSG-EKD**	• Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung, der die kirchliche Stelle unterliegt, erforderlich. Die rechtliche Verpflichtung wird dabei durch Unionsrecht oder kirchliches Recht festgelegt.
Lebenswichtige Interessen **§ 6 Nr. 7 DSG-EKD**	•Die Verarbeitung ist rechtmäßig, soweit dies erforderlich ist, um lebenswichtige Interessen der betroffenen Person zu schützen.
Berechtigtes Interesse **§ 6 Nr. 8 DSG-EKD**	• Die Verarbeitung beruht aufgrund eines berechtigten Interesses des Verantwortlichen. Das Interesse umfasst das rechtliche, tatsächliche, wirtschaftliche oder ideelle Interesse des Verantwortlichen und erfordert eine Interessenabwägung.

IV. GRUNDSÄTZE DER VERARBEITUNG

Prinzipiell sind personenbezogene Daten nach den normierten Grundsätzen gem. § 5 DSG-EKD zu verarbeiten.

1. Grundsatz der Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Der Grundsatz der Rechtmäßigkeit erfordert, dass für jeden Datenverarbeitungsvorgang eine Rechtsgrundlage gegeben ist. Dieses Strukturprinzip wird auch als „Verbot mit Erlaubnisvorbehalt“ bezeichnet.[8]
Nach dem Grundsatz der Verhältnismäßigkeit dürfen bei der Beurteilung einer Verarbeitung personenbezogener Daten nur solche gesammelt und verarbeitet werden, die für die Zwecke der Verarbeitung angemessen und erheblich sind. Eine Erheblichkeit ist zu bejahen, wenn die Daten für den Zweck relevant sind, sie also geeignet und erforderlich sind. Die Datenverarbeitung ist angemessen, wenn sie verhältnismäßig im inneren Sinn ist.

Der Grundsatz nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, von der Durchführung einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden.

Der Grundsatz der Transparenz setzt voraus, dass alle Informationen zu den personenbezogenen Daten in leicht zugänglicher, verständlicher sowie in klarer und einfacher Sprache abgefasst sind.[9]

2. Grundsatz der Zweckbindung

Nach dem Grundsatz der Zweckbindung dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

3. Grundsatz der Datenminimierung

Die Datenverarbeitung muss nach dem Zweck angemessen und erheblich sein, zudem muss sie auf das für die Zwecke der Datenverarbeitung notwendige Maß beschränkt werden.[10]

4. Grundsatz der Richtigkeit

Nach dem Grundsatz der Richtigkeit müssen Daten sachlich richtig und auf dem neusten Stand sein.

[8] Gola/Heckmann/Pötters DS-GVO Art. 5, Rn. 7;
[9] Gola/Heckmann/Pötters DS-GVO Art. 5, Rn. 11;
[10] Gola/Heckmann/Pötters DS-GVO Art. 5, Rn. 22;

5. Grundsatz der Speicherbegrenzung

Nach dem Grundsatz der Speicherbegrenzung dürfen personenbezogene Daten, die die Identifizierung der betroffenen Person ermöglichen, nur so lange gespeichert werden, wie es für die Zweckerreichung erforderlich ist. Der Grundsatz der Speicherbegrenzung konkretisiert den Grundsatz der Zweckbindung und das Verhältnismäßigkeitsprinzip in zeitlicher Hinsicht.[11]

6. Grundsatz der Integrität und Vertraulichkeit

Nach dem Grundsatz der Integrität und Vertraulichkeit muss eine angemessene Sicherheit der personenbezogenen Daten durch technische und organisatorische Maßnahmen vor der unbefugten und unrechtmäßigen Verarbeitung, vor dem unbefugten und unbeabsichtigten Verlust, vor der unbeabsichtigten Zerstörung oder unbeabsichtigten Schädigung gewährleistet werden. Der Grundsatz der Integrität und Vertraulichkeit wird durch die in § 27 DSG-EKD aufgeführten technischen und organisatorischen Maßnahmen konkretisiert.

7. Rechenschaftspflicht

Der für die Verarbeitung Verantwortliche ist gem. § 5 Abs. 2 DSG-EKD für die Einhaltung der Grundsätze verantwortlich und muss die Einhaltung entsprechend nachweisen können.

V GEMEINSAM VERANTWORTLICHE STELLE GEM. § 29 DSG-EKD

§ 29 DSG-EKD konkretisiert, was unter einer gemeinsam verantwortlichen Stelle zu verstehen ist.
Legen zwei oder mehr verantwortliche Stellen gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, so sind sie gemeinsam verantwortliche Stellen.

1. Abgrenzung zwischen einer Auftragsverarbeitung gem. § 30 DSG-EKD und einer gemeinsamen Verantwortlichkeit gem. § 29 DSG-EKD

Bei einer Auftragsverarbeitung entscheidet der Verantwortliche (Auftraggeber) über den Zweck der Verarbeitung. Der Auftragnehmer ist ggü. dem Auftraggeber weisungsgebunden. Die Rechtsgrundlage für die Verarbeitung liegt im Verantwortungsbereich des Auftraggebers. Die Gesamtverantwortung des Auftraggebers umfasst auch die Datenverarbeitung des Auftragsverarbeiters.

Anders gestaltet sich die Verantwortung bei einer gemeinsamen Verantwortlichkeit. Jeder Verantwortliche benötigt für die Verarbeitung eine eigene Rechtsgrundlage. Die Verantwortlichen entscheiden gemeinschaftlich über die Zwecke und Mittel der

[11] Gola/Heckmann/Pötters DS-GVO Art. 5, Rn. 26;

Verarbeitung.[12] Bei einer rechtswidrigen Datenverarbeitung liegt dementsprechend auch eine gemeinsame Haftung vor.

2. Vereinbarung zur gemeinsamen Verantwortlichkeit

Gem. § 29 Abs. 1 DSG-EKD muss eine Vereinbarung zwischen den zwei Stellen geschlossen werden. Das Gesetz gibt die Form der Vereinbarung nicht explizit vor, in Hinblick auf etwaige Informationspflichten gegenüber der betroffenen Person sollte jedoch mindestens eine Regelung in Textform geschlossen werden.

Nachfolgendes wird empfohlen, in die Vereinbarung mit aufzunehmen:

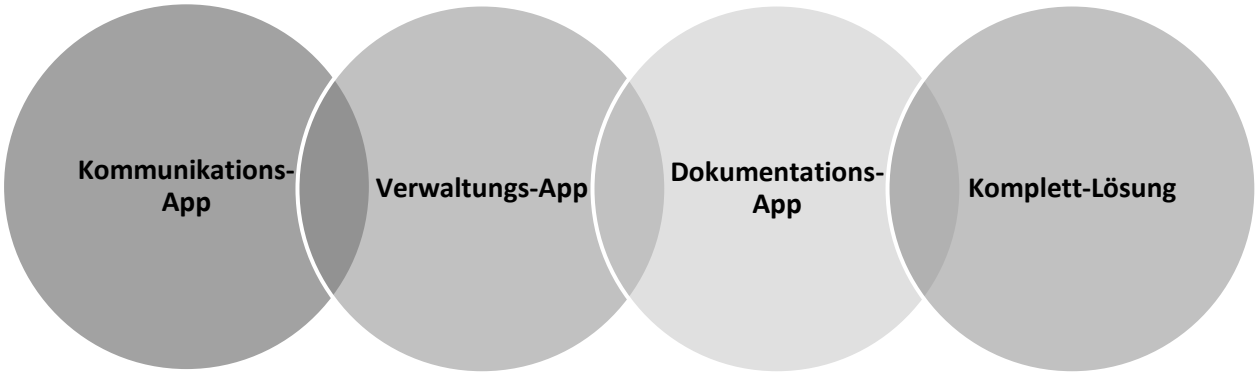
a) Beschreibung der Datenverarbeitung
b) Beziehungen und Funktionen aller gemeinsam Verantwortlichen
c) Rechtsgrundlagen der Datenverarbeitung
d) Umgang mit Betroffenenrechten
e) Verschriftlichung der technischen und organisatorischen Maßnahmen
f) Verschriftlichung von Verarbeitungsverzeichnissen
g) Vorgehensweise bei Anfertigungen von Datenschutz-Folgenabschätzungen
h) Umgang mit Datenschutzverletzungen (Feststellung, Behandlung und Meldung)
i) Auflistung der jeweiligen Ansprechpartner für den Datenschutz
j) Anforderungen an die gegenseitige Übermittlung von Informationen
k) Regelungen zum Haftungsausgleich im Innenverhältnis

B AUSWAHL EINER KITA-APP

Die Auswahl einer Kita-App gestaltet sich bei der Quantität der auf dem Markt befindlichen Kita-Apps durchaus schwierig.

Auswahlkriterien
Bei der Auswahl einer App sind verschiedene Kriterien zu berücksichtigen. Was sollte die zukünftige App können, wobei soll die App unterstützen?
Eine Unterscheidung sowie Selektion kann anhand der gewünschten Funktionen bzw. des gewünschten Funktionsumfangs getroffen werden. Grob lassen sich die Apps in die nachfolgenden vier Kategorien einteilen:

[12] Naumann in Wagner (Hrsg.) EKD-Datenschutzgesetz § 29, Rn. 7;



I KOMMUNIKATIONS-APP

Kommunikations-Apps bieten einen sicheren Kommunikationskanal zwischen den Pädagog:innen und den Personensorgeberechtigten sowie einen Kommunikationskanal innerhalb des Kindertagesstätten-Teams. Diese Art von App dient dem reinen Informationsaustausch der oben aufgezählten Konstellationen. Darüber hinaus sind in der Regel die nachfolgend genannten Funktionen in den Kommunikations-Apps enthalten:

- Kalender (Aktionen, Termine, Schließzeiten)
- Speiseplan
- Chatfunktion zum direkten Austausch zwischen der Kindertagesstätte und den Personensorgeberechtigten
- Abmeldung des Kindes (Urlaub, Krankheit)

II VERWALTUNGS-APP

Verwaltungs-Apps sind zur Planung und Strukturierung der Verwaltungsaufgaben von Kindertagesstätten nutzbar. Sie sollen den Verwaltungsaufwand weitestgehend digitalisieren sowie durch automatisierte Prozesse minimieren. Die nachfolgend genannten Funktionen sind in der Regel in Verwaltungs-Apps enthalten:

- Anmeldung- und Platzvergabe
- Personalmodul (Personaleinsatzplanung, Personalschlüssel, Dienstpläne, Arbeitszeiterfassung)
- Statistik (Landes- und Bundesstatistik)
- Kinder und Gruppen (Betreuungsverträge, Gruppenübersichten, Gruppentagebücher)
- Förderung (Förderanträge und Bescheide)

- Finanzmodule (Verpflegung, Elternbeiträge, Barkasse, Konten und Kostenstellen, Finanzbuchhaltungssoftware inkl. Schnittstelle)
- Verwaltungsmodul (Stammdaten, Adressverwaltung, Einrichtungskalender, Dokumentenbibliothek, Inventarverwaltung, Listen und Auswertungen)

III DOKUMENTATIONS-APP

Dokumentations-Apps bieten die Möglichkeit, die Bildungs- und Entwicklungsdokumentation der Kinder in digitaler Form zu erstellen. Teilweise sind auch digitale Beobachtungsbögen (Lisbet, Sismik, Seldak, Perik etc.) zur Nutzung und Bearbeitung hinterlegt. Auch die Zusammenstellung eines ePortfolios ist in einigen Apps möglich.

IV KOMPLETTLÖSUNG

Komplettlösungen bieten eine Kombination aus einem Kommunikationsmodul, einem Dokumentationsmodul sowie einem Verwaltungsmodul. Sie schaffen somit eine einheitliche Lösung für die Belange der Personensorgeberechtigten sowie der Mitarbeiter:innen und ggf. der übergeordneten Verwaltungseinheit.

Eine Entscheidungshilfe bietet die vom Staatsinstitut für Frühpädagogik (IFP), München, herausgegebene Expertise (2. überarbeitete Auflage, August 2021)[13]. Die IFP-Expertise gibt einen Überblick über aktuell am Markt verfügbare Softwarelösungen für mittelbare pädagogische Kitaaufgaben und über die Datenschutz-Anforderungen an die Konzeption und Anwendung webbasierter KitaApps.

C DATENSCHUTZRECHTLICHE ÜBERPRÜFUNG DER KITA-APP

I AUFTRAGSVERARBEITUNG

Die Verarbeitung von personenbezogenen Daten im Auftrag ist in § 30 DSG-EKD geregelt.

1. Was ist eine Auftragsverarbeitung?

Eine Auftragsverarbeitung ist immer dann gegeben, wenn personenbezogene Daten im Auftrag durch eine *andere Stelle oder Person* verarbeitet werden. Die andere Stelle wird in diesem Zusammenhang als Auftragsverarbeiter bezeichnet. Die Verantwortung über eine ordnungsgemäße Verarbeitung der personenbezogenen Daten verbleibt jedoch beim Auftraggeber. Die andere Stelle fungiert in diesem Zusammenhang als „verlängerter Arm“ des Auftraggebers. Charakteristisch für eine Auftragsverarbeitung ist eine strenge Weisungsgebundenheit des Auftragsverarbeiters.[14]

[13] Expertise - Apps und Softwarelösungen zum digitalen Austausch zwischen Eltern und Kita/Schule (bayern.de)

[14] Schneedorf in Wagner EKD-Datenschutzgesetz § 30, Rn. 3;

2. Wer ist bei einer Auftragsverarbeitung für den Datenschutz verantwortlich?

Bei einer Auftragsverarbeitung stellt sich die Frage, wer für den Schutz der erhobenen Daten verantwortlich ist. Beauftragen Sie eine andere Stelle oder Person mit der Verarbeitung von personenbezogenen Daten, so tragen Sie für die Einhaltung der datenschutzrechtlichen Vorgaben beim Auftragsverarbeiter die Verantwortung.

3. Wann wird ein Auftragsverarbeitungsvertrag benötigt?

Ein Vertrag zur Auftragsverarbeitung wird dann benötigt, wenn eine externe Stelle oder Person im Zuge eines Auftrages Zugriff auf personenbezogene Daten von Dritten erhält. Bereits *vor der ersten Verarbeitung* ist mit der verarbeitenden Stelle ein Auftragsverarbeitungsvertrag zu schließen, der die Rechte und Pflichten der jeweiligen Partei festlegt.

4. Was ist in einem Auftragsverarbeitungsvertrag zu regeln?

Der Regelungsinhalt eines Auftragsverarbeitungsvertrages wird durch § 30 Abs. 3 DSG-EKD konkretisiert. Demzufolge müssen die nachfolgenden Inhalte von einem Auftragsverarbeitungsvertrag erfasst sein:

a) der Gegenstand und die Dauer des Auftrags;

b) der Umgang, die Art und der Zweck der vorgesehenen Verarbeitung, die Art der Daten und der Kreis der Betroffenen;

c) die nach § 27 DSG-EKD zu treffenden technischen und organisatorischen Maßnahmen sowie ihre Kontrolle durch den Auftragsverarbeiter;

d) die Berichtigung, Löschung und Sperrung von Daten;

e) die Verpflichtung der Beschäftigten des Auftragsverarbeiters auf das Datengeheimnis;

f) ggf. die Berichtigung zur Begründung sowie die Beendigung von Unterauftragsverhältnissen;

g) die Kontrollrechte der beauftragten kirchlichen Stelle und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters;

h) der Umfang der Weisungsbefugnis, die sich die beauftragende kirchliche Stelle ggü. dem Auftragsverarbeiter vorbehält;

i) die Rückgabe überlassener Datenträger und die Löschung beim Auftragsverarbeiter gespeicherter Daten nach Beendigung des Auftrags.

5. Serverstandorte

Es ist zwingend darauf zu achten, dass der App-Anbieter sowie alle Unterauftragnehmer ihren Hauptsitz sowie die Serverstandorte in der EU bzw. dem EWR haben.

6. Zusatzvereinbarung gem. § 30 Abs. 5 DSG-EKD

Neben dem Abschluss eines Auftragsverarbeitungsvertrags auf Grundlage des DSG-EKD besteht gem. § 30 Abs. 5 DSG-EKD die Möglichkeit, auch Auftragsverarbeitungsverträge mit Auftragsverarbeitern unter den Voraussetzungen des Art. 28 DSGVO abzuschließen, soweit der Auftragsverarbeitungsvertrag alle erforderlichen Vertragsbestandteile (siehe oben) enthält. Dazu ist in Kombination mit dem Auftragsverarbeitungsvertrag eine Zusatzvereinbarung (ehemals Unterwerfungserklärung) mit dem Auftragsverarbeiter abzuschließen. Ein entsprechendes Muster stellt die Landeskirche Hannovers unter (https://www.landeskirche-hannovers.de/landeskirche/landeskirchenamt/abteilungen/abteilung-7/datenschutz)
zur Nutzung zur Verfügung.

7. Technische und organisatorische Maßnahmen:

Innerhalb des Auftragsverarbeitungsvertrages sind die umgesetzten technischen und organisatorischen Maßnahmen aufzuführen. Gem. § 27 DSG-EKD haben die verantwortliche Stelle und der kirchliche Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können.

Gem. § 30 Abs. 3 DSG-EKD ist der Auftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Das bedeutet im Konkreten, dass die technischen und organisatorischen Maßnahmen dafür ausgelegt sein müssen, die normierten Datenschutzgrundsätze nach § 5 DSG-EKD wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung mit aufzunehmen.

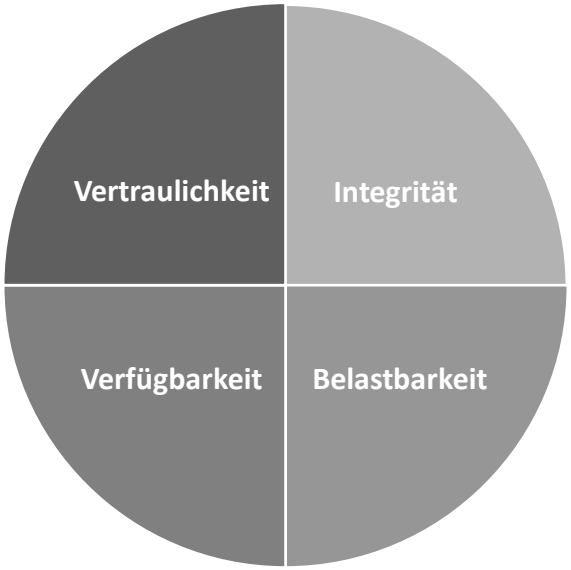
Grundsätzlich sollte zunächst ein Mindestniveau für die technischen und organisatorischen Maßnahmen festgelegt werden. Dieses sollte sich sinnvollerweise am Level des Verantwortlichen selbst orientieren. Darüber hinaus ist hier maßgeblich, welche personenbezogenen Daten durch den Auftragsverarbeiter verarbeitet werden und welchem Schutzniveau diese unterliegen. Gerade bei der Verarbeitung von besonderen Kategorien personenbezogener Daten (bspw. Gesundheitsdaten) sind die Anforderungen an die technischen und organisatorischen Maßnahmen deutlich höher anzusetzen, um ein ausreichendes Schutzniveau für die Daten sicherstellen zu können.

Das Gesetz unterscheidet in § 27 Abs. 1 Nr. 1 – 4 DSG-EKD zwischen verschiedenen Maßnahmen. Dazu zählen:

a) Pseudonymisierung, Anonymisierung und die Verschlüsselung von Daten

Eine ***Pseudonymisierung*** ist lt. der Legaldefinition gem. § 4 Nr. 6 DSG-EKD gegeben, wenn personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. [15]
Bei dem Prozess der ***Anonymisierung*** kann die betroffene Person nicht oder nicht mehr identifiziert werden.[16]
Unter ***Verschlüsselung*** ist ein Vorgang zu verstehen, bei dem eine klar lesbare Information mithilfe eines kryptografischen Verfahrens in eine „unleserliche" Zeichenabfolge umgewandelt wird.[17] Eine Kombination aus Pseudonymisierung und Verschlüsselung soll gewährleisten, dass selbst bei einem unbefugten Zugriff auf Systeme nicht auf personenbezogene Daten zugegriffen oder zumindest ein Personenbezug nicht ohne weiteres hergestellt werde kann.

b) Sicherstellung der Vertraulichkeit, der Integrität, der Verfügbarkeit und der Belastbarkeit von Systemen und Diensten



Die in § 27 Abs. 1 Nr. 2 DSG-EKD geforderten Maßnahmen, sollen zur Sicherstellung der Systeme und Dienste beitragen.

[15] Gola/Heckmann/Pötters; DS-GVO Art. 89; Rn. 10;
[16] Gola/Heckmann/Pötters; DS-GVO Art. 89; Rn. 11;
[17] Simitis/Ernetus BDSG § 9, Rn. 166; Hornung/Schallbruch IT SicherheitsR/Grimm/Waidner, 2021, § 2, Rn. 1;

Das Gewährleistungsziel der ***Vertraulichkeit*** soll sicherstellen, dass kein unbefugter Dritter personenbezogene Daten zur Kenntnis nehmen oder gar nutzen kann. Maßnahmen, um das Gebot der Vertraulichkeit umzusetzen, sind unter anderem eine Zutritts-, Zugriffs-, Zugangs- oder etwa eine Weitergabekontrolle.
Mit dem Gewährleistungsziel der ***Integrität*** soll sowohl eine Unversehrtheit von Daten als auch die Funktionalität von Systemen sichergestellt werden. Zu den anerkannten Maßnahmen in diesem Sinne gehören unter anderem: Einsatz von elektronischen Signaturen oder Prüfziffern, Eingabekontrollen mittels Protokollierung, um feststellen zu können von wem wann welche personenbezogenen Daten eingegeben wurden sowie Berechtigungssysteme für den Zutritt, den Zugang oder den Zugriff zu personenbezogenen Daten innerhalb eines Systems.
Durch das Gewährleistungsziel der ***Verfügbarkeit*** von Daten soll sichergestellt werden, dass die genutzten Systeme und Dienste von den Anwendern stets wie vorgesehen genutzt und somit die personenbezogenen Daten des Betroffenen wie erwartet und vereinbart verarbeitet werden können. Zu den anerkannten Schutzmaßnahmen zur Gewährleistung der Verfügbarkeit gehören die Einrichtung von Back-up-Systemen, Sicherheitsmonitoring-Systeme als auch redundante Systeme, der physische Schutz der Hardware sowie die Etablierung eines Schulungssystems.
Im engen Zusammenhang mit dem Gewährleistungsziel der Verfügbarkeit steht das Gewährleistungsziel der ***Belastbarkeit*** von Systemen. Im Rahmen der Belastbarkeit geht es darum, die Verarbeitung von personenbezogenen Daten auf Dauer sicherzustellen. Was explizit bedeutet, dass die Systeme und Dienste trotz möglicher Störungen und Fehler stets funktionsfähig sind und bleiben.

c) Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen

Das Gewährleistungsziel der Wiederherstellbarkeit steht ebenfalls in einem engen Zusammenhang mit dem Gewährleistungsziel der Verfügbarkeit. Es besteht immer die Möglichkeit, dass Daten beschädigt oder gestohlen werden oder auf eine andere Weise abhandenkommen. Umso wichtiger ist in einem solchen Fall eine rasche Wiederherstellbarkeit der Daten. Folgende Maßnahmen können in diesem Zusammenhang die Wiederherstellbarkeit der Daten gewährleisten:

- Back-ups oder Datensicherungen
- Firewall
- Regelmäßiges Testen der Datenwiederherstellung
- Virenscanner
- Erstellung eines Notfallplans

d) Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit getroffener technischer und organisatorischer Maßnahmen kann ein dreistufiger Aufbau angewandt werden:

da) Überprüfung

Überprüft werden die konkret eingesetzten technischen und organisatorischen Maßnahmen.

db) Bewertung

Erneute Überprüfung der Risikoprognose und des damit korrespondierenden Schutzniveaus. Anschließend findet eine Überprüfung statt, ob die eingesetzten technischen und organisatorischen Maßnahmen das festgestellte Schutzniveau sicherstellen.

dc) Evaluierung

Hier ist anschließend zu überprüfen, ob die Effektivität der Maßnahmen gewährleistet ist. Dies kann, wenn auch nicht ausschließlich, durch Penetrationstests erfolgen.[18]

Die DSK (Datenschutzkonferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder) beschreibt ein entsprechendes Verfahren „Plan-Do-Check-Act-Zyklus“ (PDCA) im Rahmen des Standard-Datenschutzmodells. Des Weiteren bestehen im IT-Grundschutz und der ISO 27001 weitere mögliche Verfahren zur Sicherstellung der oben beschriebenen Gewährleistungsziele.

Entsprechend der dynamischen Veränderungen des Datenschutzrechts sind auch die oben beschriebenen Maßnahmen in regelmäßigen Abständen zu überprüfen, um eine fortwährende Wirksamkeit zu gewährleisten. Nach Ansicht einzelner Aufsichtsbehörden ist die Wirksamkeitsevaluation alle zwei bis drei Jahre durchzuführen. Einer solch statischen Handhabung ist jedoch mit Vorsicht zu begegnen. Bei der Bestimmung des Turnus sind die Kategorien der verarbeiteten Daten sowie die dadurch resultierenden Risiken für die betroffene Person mit einzubeziehen.

[18] Kipker/Reusch/Ritter/Piltz/Zwerschke; DS-GVO Art. 32; Rn. 58;

Essenzielle TOMs bei Nutzung einer Kita-APP

Datenbanken	Für jede Kindertagesstätte ist eine individuelle Datenbank anzulegen, sodass kein Zugriff auf einrichtungsfremde Daten möglich ist.
Rollen- und Berechtigungskonzept	Innerhalb der Kita-App sollte die Möglichkeit eines ausdifferenzierten Rollen- und Berechtigungskonzepts für Mitarbeiter:innen vorhanden sein. Dies sollte jedem Nutzer anhand der jeweiligen Funktion zugeordnet werden können. Die Zuordnung der jeweiligen Rolle sollte der Leitung der Kindertagesstätte obliegen.
Personalisierte Zugänge	Jede Fachkraft sollte ausschließlich über personalisierte Zugänge (Nutzername, Passwort) innerhalb der App arbeiten dürfen. Dabei ist zwingend auf eine Passwortsicherheit zu achten (Mindestlänge, Buchstaben, Zahlen, Sonderzeichen).
Passwortschutz der Hardware	Das Tablet oder ein anderes Endgerät ist ebenfalls mit einem Zugangscode zu sichern, um nur befugten Personen den Zugriff zu gewähren. Auch hier ist auf eine entsprechende Passwortsicherheit zu achten.
2-Faktor-Authentifizierung	Die 2-Faktor-Authentifizierung bietet eine wirksame Möglichkeit zum Schutz der personenbezogenen Daten. Wichtig in Bezug auf die 2-Faktor-Authentifizierung ist, dass die Faktoren aus verschiedenen Kategorien stammen. Eine Kombination aus Wissen (Passwort oder PIN), Besitz (Chipkarte, TAN-Generator) oder Biometrie (z.B. Fingerabdruck) ist zu empfehlen.
Verschlüsselung	Personenbezogene Daten dürfen ausschließlich mittels TLS- oder SSL-Verschlüsselung übermittelt werden.
MDM	Alle mobilen Endgeräte sollten in ein MDM (Mobile Device Management) eingebunden sein. Ein MDM bietet die Inventarisierung und zentrale Verwaltung von mobilen Endgeräten in einer Einrichtung. Geräte können im Falle eines Diebstahls ferngesteuert gesperrt bzw. gelöscht werden, um den Schutz der personenbezogenen Daten zu gewährleisten.
Verschwiegenheitsverpflichtung	Verpflichtung des Auftraggebers und ggf. dessen Unterauftragnehmer auf das Datengeheimnis.

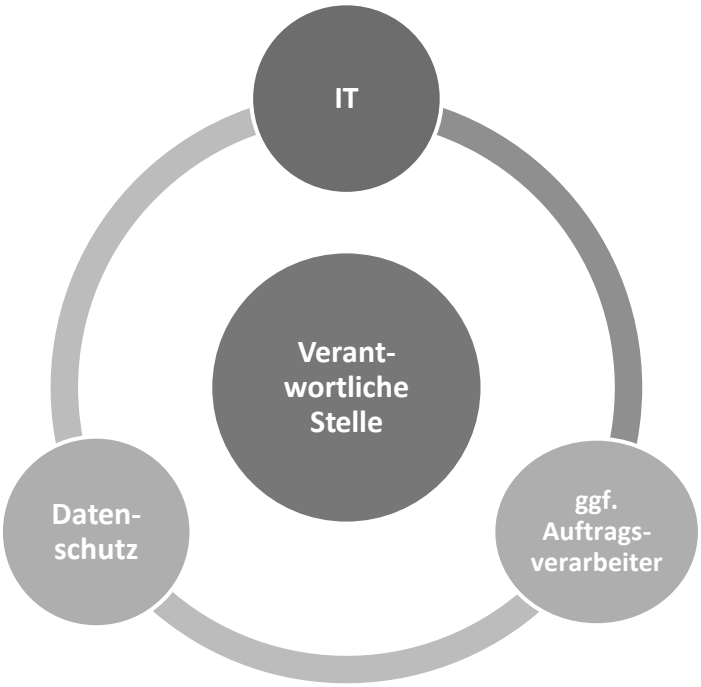
II DURCHFÜHRUNG EINER DSFA (DATENSCHUTZ-FOLGENABSCHÄTZUNG)

Sobald eine Verarbeitung von personenbezogenen Daten ein hohes Risiko für die Rechte natürlicher Personen zur Folge hat, ist durch die verantwortliche Stelle vorab eine Datenschutz-Folgenabschätzung der vorgesehenen Verarbeitungsvorgänge durchzuführen.

1. Vorbereitende Maßnahmen

a) Zusammenstellung eines DSFA-Teams

Für die Erstellung einer Datenschutz-Folgenabschätzung ist die Zusammenstellung eines fachübergreifenden Teams, bestehend aus der verantwortlichen Stelle, dem Datenschutz, der IT und ggf. dem Auftragsverarbeiter notwendig. Der örtlich Beauftragte für den Datenschutz hat bei der Erstellung der DSFA gem. § 34 DSG-EKD lediglich eine beratende Funktion und kann als Einzelperson nicht für die Erstellung dieser verantwortlich gemacht werden.



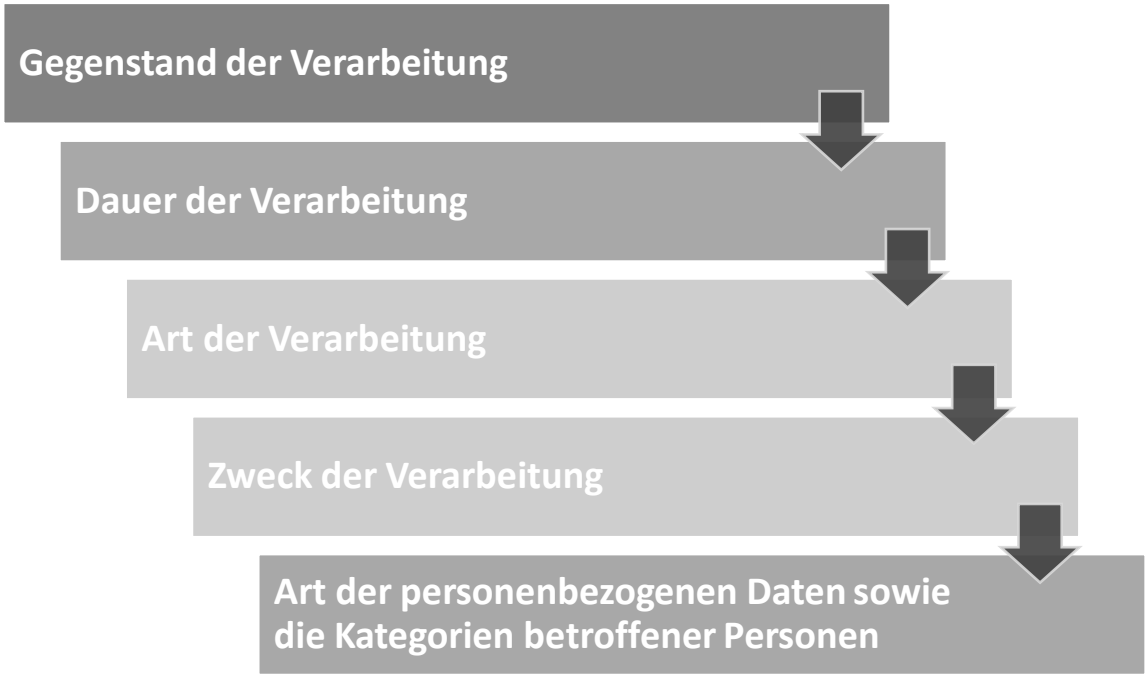
b) Benennung der Verantwortlichen Stelle

„Verantwortliche Stelle“ im Sinne des DSG-EKD ist jede natürliche oder juristische Person, kirchliche oder sonstige Stelle, die ***allein oder gemeinsam*** mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten

entscheidet.[19] Federführend im Prozess der Kita-App-Einführung sind hier die betriebswirtschaftlichen und pädagogischen Leitungen, unter der Entscheidungsbefugnis des Trägers (Kirchenvorstand, Kirchenkreisvorstand, Verbandsvorstand) sowie des geschäftsführenden Ausschusses zu nennen.

c) Beschreibung der Verarbeitung

Zunächst ist die Verarbeitung selbst zu beschreiben:



d) Rechtsgrundlage der Verarbeitung

Als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten der Personensorgeberechtigten, Kindergartenkinder und Abholberechtigten/Notfallkontakte innerhalb der Kita-App kommt ausschließlich die Einwilligung gem. § 6 Nr. 2 DSG-EKD in Betracht.

[19] Eibach in Wagner (Hrsg.) EKD-Datenschutzgesetz, § 4, Rn. 91;

da) Wirksamkeitsvoraussetzungen einer Einwilligung

(1) Freiwilligkeit

Eine Einwilligung ist grundsätzlich nur wirksam, wenn diese freiwillig, d.h. ohne jeglichen Druck oder Zwang abgegeben wurde. Erwägungsgrund 42 der DSGVO verlangt in diesem Zusammenhang eine echte Wahlfreiheit der jeweiligen betroffenen Person. Danach impliziert „frei", dass die betroffene Person eine echte Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erlangen. [20] Von einer Freiwilligkeit ist grundsätzlich nicht auszugehen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein Abhängigkeitsverhältnis besteht. [21] Dies ist beispielsweise dann gegeben, wenn es sich bei dem Verantwortlichen um eine Behörde handelt oder ein Über- bzw. Unterordnungsverhältnis im Rahmen eines Anstellungsverhältnisses gegeben ist.

(2) Transparenz und Informiertheit

Eine Einwilligung ist wirksam erteilt, wenn die betroffene Person ihre Einwilligung „in informierter Weise" erklärt hat. Damit wird der in § 5 Abs. 1 DSG-EKD normierte „Transparenzgrundsatz" konkretisiert. In einer informierten Weise wird eine Einwilligung vom Betroffenen erteilt, wenn

[20] Rubel in Wagner (Hrsg.) EKD-Datenschutzgesetz, § 11, Rn. 25;

[21] Rubel in Wagner (Hrsg.) EKD-Datenschutzgesetz, § 11, Rn. 28;

diesem vor Abgabe der Einwilligungserklärung sämtliche Informationen zur Verfügung gestellt wurden, die notwendig sind, um die Umstände der Verarbeitung sowie die damit einhergehenden Auswirkungen und die Tragweite überblicken zu können. [22]

(3) Bestimmtheit

Eine wirksam erteilte Einwilligung muss „für den bestimmten Fall" erteilt werden. Der betroffenen Person soll durch das Erfordernis der „Bestimmtheit" ein gewisses Maß an Kontrolle gegeben werden. Nur wenn die betroffene Person weiß, wofür ihre personenbezogenen Daten erhoben werden und was konkret mit den Daten geschehen soll, kann diese im Rahmen der informationellen Selbstbestimmung darüber entscheiden, ob sie in die Datenverarbeitung einwilligen möchte oder eben nicht.

Teilweise leitet sich das Erfordernis der Bestimmtheit aus dem Grundsatz der Zweckbindung ab. Prinzipiell muss aus der Einwilligung hervorgehen, welche Daten zu welchem Zweck verarbeitet werden dürfen. Das Ausmaß der Bestimmtheit sollte sich an der Eingriffsintensität der verarbeiteten Daten ausrichten.

(4) Kopplungsverbot

Das Kopplungsverbot ist ein Element des Freiwilligkeitsprinzips. Eine Kopplung im datenschutzrechtlichen Sinne ist gegeben, wenn ein Vertragsabschluss oder die Erbringung einer Leistung davon abhängig gemacht wird, dass die betroffene Person in eine weitergehende Verarbeitung der personenbezogenen Daten einwilligt, welche jedoch prinzipiell nicht zur Abwicklung des Geschäfts erforderlich ist.[23]
Grundlegend darf kein emotionaler oder wirtschaftlicher Druck auf die betroffene Person ausgeübt werden, um diese zu einer Einwilligung zu bewegen. Zudem darf eine Verweigerung einer Einwilligung für den Betroffenen nicht zu „Nachteilen" führen.

(5) Nachweisbarkeit

Beruht eine Verarbeitung von personenbezogenen Daten auf dem Tatbestand einer Einwilligung, so muss die verantwortliche Person nachweisen können, dass die betroffene Person ihre Einwilligung für eine Datenverarbeitung erteilt hat. Es ist somit zu empfehlen, Einwilligungen beim Betroffenen in schriftlicher Form einzuholen. [24]

(6) Widerruflichkeit

Die betroffene Person kann eine einst erteilte Einwilligung jederzeit widerrufen. Der Widerruf gilt „ex nunc", d.h. ab dem Zeitpunkt des

[22] Kühling/Buchner, DS-GVO BDSG, Art. 4 Nr. 11, Rn. 8;

[23] Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, Art. 7, Rn. 94;

[24] Rubel in Wagner EKD-Datenschutzgesetz, § 11, Rn. 10;

Widerrufs. [25] Der Widerruf einer Einwilligung führt nicht zwangsläufig zu einer sofortigen Löschpflicht des Verantwortlichen. Möglicherweise kann sich der Verantwortliche nach dem Widerruf auf spezialgesetzliche Grundlagen berufen, die eine weitere Aufbewahrung ermöglichen und notwendig machen. [26]

db) Einwilligungserklärung im Beschäftigtenverhältnis

Mit dem § 49 DSG-EKD hat die Evangelische Kirche in Deutschland eine eigene Vorschrift für die Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis erlassen. Gem. § 49 Abs. 1 DSG-EKD ***dürfen Beschäftigtendaten verarbeitet werden, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Beschäftigtenverhältnisses oder zur Durchführung organisatorischer und personeller und sozialer Maßnahmen, insbesondere auch für die Zwecke der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.***
Für eine Erfassung von personenbezogenen Daten über die eben aufgeführten Zwecke hinaus ist eine anderweitige Rechtsgrundlage bspw. in Form einer Einwilligung erforderlich. Aufgrund eines Über- und Unterordnungsverhältnisses und einer möglicherweise bestehenden daraus resultierenden Abhängigkeit des Beschäftigten erhöht § 49 Abs. 3 DSG-EKD die Erfordernisse an eine rechtsgültige Einwilligung. Die Beurteilung der Wirksamkeit wird diesbezüglich am Erfordernis der Freiwilligkeit sowie an den Umständen gemessen, unter welchen die Einwilligung des Beschäftigten eingeholt wurde.
Folgendes ist somit beim Einholen einer Einwilligung im Beschäftigungsverhältnis zu beachten:

- Beachtung des Aspekts der Freiwilligkeit;
- Die Umstände, unter welchen die Einwilligung eingeholt wurde;
- Schriftformerfordernis;
- Informiertheit des Beschäftigten über den Zweck der Datenerhebung;
- Hinweis des Beschäftigten auf bestehende Widerrufsrechte.

dc) Dienstvereinbarung gem. MVG-EKD

§ 49 Abs. 1 zweite Variante sieht als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten den Abschluss einer Dienstvereinbarung vor. Die zwischen der Dienststellenleitung und der Mitarbeitervertretung abzuschließende Dienstvereinbarung trägt zu einem sachgerechten Ausgleich der Interessen von Dienststellenleitung und Beschäftigten bei. [27] Dienstvereinbarungen sind schriftlich niederzulegen, von beiden Parteien zu unterzeichnen und in geeigneter Weise bekannt zu geben. Grundsätzlich darf die Mitarbeitervertretung für alle Angelegenheiten eine Dienstvereinbarung schließen, bei

[25] Rubel in Wagner (Hrsg.) EKD-Datenschutzgesetz, § 11, Rn. 18;

[26] Rubel in Wagner (Hrsg.) EKD-Datenschutzgesetz, § 11, Rn. 23;

[27] Joussen in Wagner (Hrsg.) EKD-Datenschutzgesetz § 49, Rn. 25 ff.

denen sie ein gesetzliches Mitbestimmungsrecht hat. Die gesetzlichen Mitbestimmungsrechte sind in §§ 39, 40 MVG-EKD normiert. Dazu zählen die allgemeinen personellen Angelegenheiten gem. § 39 MVG-EKD sowie eine Mitbestimmung zu organisatorischen und sozialen Angelegenheiten gem. § 40 MVG-EKD.

> Grundlegend gelten Dienstvereinbarungen für alle Arbeitnehmer:innen, sofern der Geltungsbereich nicht explizit auf einzelne Arbeitnehmergruppen beschränkt ist.

Für die Einführung einer Kita-App ist ein Mitbestimmungsrecht gem. § 40 lit. k MVG-EKD gegeben. Danach besteht ein Mitbestimmungsrecht bei Einführung und Anwendung von Maßnahmen oder technischen Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Mitarbeiter:innen zu überwachen. Je nach Umfang der App können weitere mitbestimmmungsrelevante Punkte betroffen sein, z.B. wenn über die App ein Dienstplan erstellt wird oder die Arbeitszeiterfassung über die App erfolgen soll.

Um die Rechte der Mitarbeiter:innen zu schützen, ist die Vereinbarung einer möglichst detaillierten Dienstvereinbarung grundsätzlich notwendig. Folgende Punkte sollte eine Dienstvereinbarung enthalten:

Inhalt einer Dienstvereinbarung

- Überschrift der Dienstvereinbarung
  Bei der Überschrift einer Dienstvereinbarung sollte auf eine positive Formulierung geachtet werden, um nicht bereits an diesem Punkt Ängste zu schüren.
- Präambel
  Die Präambel ist die Einleitung eines Vertrages. Diese sollte die Motivation für den Abschluss der Dienstvereinbarung erfassen.
- Geltungsbereich
  Unterschieden wird zwischen einem betrieblichen, persönlichen und zeitlichen Geltungsbereich.
  - Betrieblicher Geltungsbereich
    Stellt einen räumlichen Aspekt dar
  - Persönlicher Geltungsbereich
    Hier wird auf eine Gruppe von natürlichen oder juristischen Personen abgestellt
  - Zeitlicher Geltungsbereich
    Bestimmt den Beginn und das Ende somit die Laufzeit der Dienstvereinbarung
- Begriffsbestimmungen
  Dieser Absatz kann genutzt werden, um unklare Begrifflichkeiten zu definieren.

- Regelungen zur Bildung einer Clearing- o. Schlichtungsstelle
  Je nach Brisanz des Dienstvereinbarungsinhalts kann es zu Streitigkeiten zwischen den Parteien kommen, die durch eine Clearing- o. Schlichtungsstelle beigelegt werden könnte.
- Regelung über die Möglichkeit einer Änderung bzw. Anpassung der Dienstvereinbarung.
- Ausformulierung der konkreten Rechte bzw. Pflichten der Mitarbeiter:innen, Vereinbarungen und Verabredungen.
- Datenschutz
- Mögliche Rechte der MAV
- Regelung zur Bekanntmachung der Dienstvereinbarung
- Schlussbestimmungen
  - Zeitpunkt des Inkrafttretens
  - Kündigungsfrist
  - Zeitraum einer erneuten Verhandlungsaufnahme beider Parteien nach der Kündigung der Dienstvereinbarung
  - Salvatorische Klausel
  - Unterschrift der Beteiligten (Dienststellenleitung, Vorsitzende/-r der Mitarbeitervertretung, bei Bedarf Schwerbehindertenvertretung)

Bei Streitigkeiten zu Mitbestimmungstatbeständen aus § 40 MVG-EKD ist die Einigungsstelle nach § 36a MVG-EKD zuständig.

2. Daten und Prozesse

a) Welche personenbezogenen Daten werden innerhalb der App verarbeitet?

Kita-Apps bieten die Möglichkeit, quantitativ viele Daten zu erfassen, unabhängig von der Tatsache, ob sie tatsächlich zur Zweckerreichung verarbeitet werden müssen. Die reine Möglichkeit dessen animiert dazu, diese auch zu nutzen. Die verarbeiteten Daten sollten jedoch immer am Verarbeitungszweck gemessen werden. Wenn nicht das Vorhaben besteht, auch die Entwicklungsdokumentation mittels Kita-App anzufertigen, ist die Erfassung dieser Daten innerhalb der App auch nicht notwendig. Soll eine App ausschließlich zur Kommunikation (Team/Personensorgeberechtigte) genutzt werden, sollten keine Bildnisse bzw. Videoaufnahmen der Kinder hochgeladen und verarbeitet werden.
Bei einer Datenverarbeitung sollte immer auf den Grundsatz der Datenminimierung und Zweckbindung geachtet werden. Einige Kita-Apps lassen sich datenschutzfreundlich konfigurieren. Pflichtfeldangaben können durch den Nutzer häufig selbst festgelegt werden. Für die Kita-Apps, die sich grundsätzlich nicht datenschutzkonform voreinstellen lassen, sollte durch die Trägerverantwortlichen bzw. Verbandsverantwortlichen eine schriftliche Vorgabe erfolgen, welche personenbezogenen Daten zwingend innerhalb der App zu erfassen sind.

b) Von der Verarbeitung betroffene Personen

Wer ist von der Verarbeitung der personenbezogenen Daten innerhalb der App betroffen?
Von der Datenverarbeitung innerhalb der Kita-App sind folgende Personen betroffen:

- Mitarbeiter:innen
- Kinder der Kindertagesstätte
- Personensorgeberechtigte
- Notfall- und Abholkontakte

c) Empfänger der Daten

Gem. § 4 Nr. 11 DSG-EKD wird unter dem Begriff des „Empfängers" eine natürliche oder juristische Person, kirchliche oder sonstige Stelle verstanden, der personenbezogene Daten offenlegelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Der Empfängerkreis sollte so eng wie möglich gehalten werden.

Folgende Empfänger sind denkbar:

- Pädagogisches Fachpersonal der Kindertagesstätten
- Leitung der Kindertagesstätte
- Pädagogische Leitung des Verbandes/des Trägers
- Betriebswirtschaftliche Leitung des Verbandes/des Trägers
- Personensorgeberechtigte (personenbezogen für das eigene Kind)
- App-Firma (im Rahmen des bestehenden Auftragsverarbeitungsverhältnisses)
- Hosting-Firma (im Rahmen eines Unterauftragnehmerverhältnisses)
- ggf. die Finanzbuchhaltung

d) Lebenszyklus der Daten

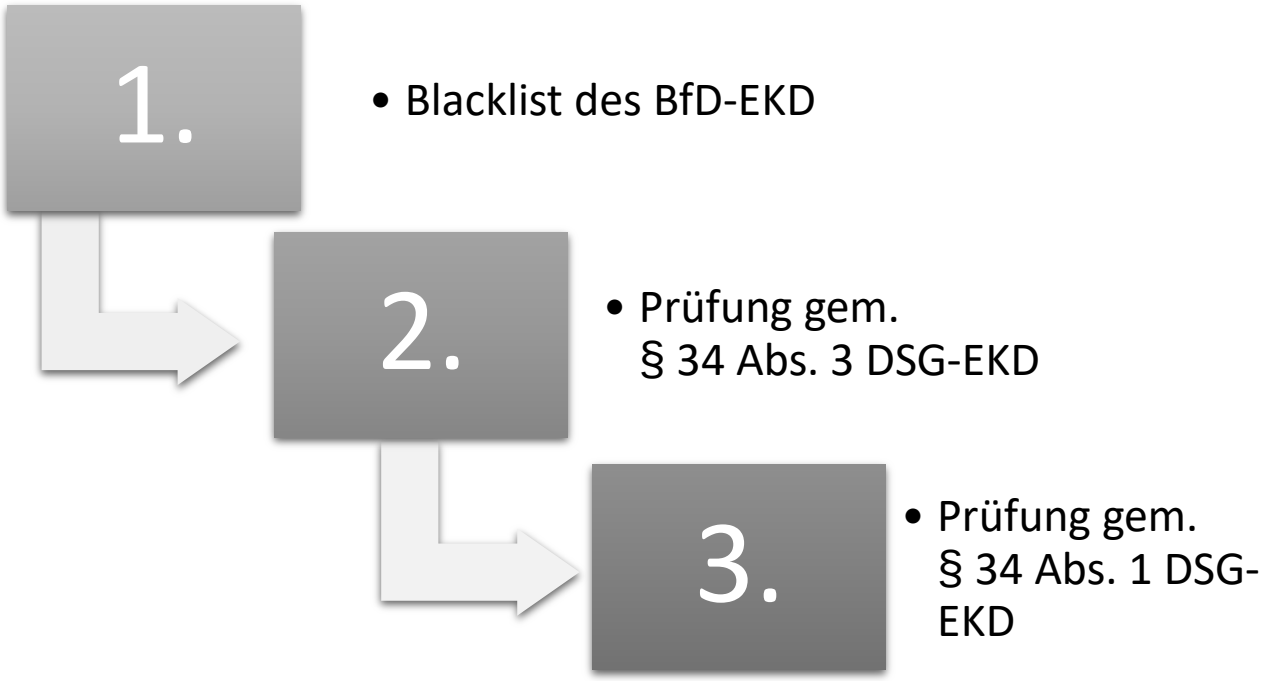
Der Datenlebenszyklus definiert die gesamte Zeitspanne, in dem Daten in einem System existieren.
In diesem Zusammenhang ist der Grundsatz der Speicherbegrenzung gem. § 5 Abs. 1 Nr. 5 DSG-EKD in Bezug zu nehmen. Zur Sicherstellung, dass die erfassten Daten nicht länger als zur Zweckerreichung notwendig gespeichert werden, soll die verantwortliche Stelle Fristen zur Löschung der Daten festlegen. Dabei sind zwingend die gesetzlich normierten Aufbewahrungsfristen (bspw. aus der AO bzw. dem HGB) zu beachten.

3. Notwendigkeit zur Erstellung einer Datenschutz-Folgenabschätzung (Schwellwertanalyse)

Die Durchführung einer Datenschutz-Folgenabschätzung ist immer dann notwendig, wenn die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge hat.

Ob die Anfertigung einer Datenschutz-Folgenabschätzung notwendig ist, kann nur durch eine systematische Überprüfung des § 34 DSG-EKD beantwortet werden. § 34 Abs. 1 DSG-EKD beschreibt die Grundbedingungen, Abs. 3 nennt konkrete Beispiele, in denen eine DSFA erforderlich ist, Abs. 5 verweist auf eine Positiv-Liste bzw. auf eine Negativ-Liste der Aufsichtsbehörde, nach der jeweils eine Datenschutz-Folgenabschätzung durchgeführt bzw. nicht durchgeführt werden muss.

Reihenfolge der Notwendigkeitsprüfung zur Erstellung einer DSFA



Schritt 1:

Befindet sich der Verarbeitungsvorgang auf der Blacklist des BfD-EKD, so ist stets die Anfertigung einer Datenschutz-Folgenabschätzung notwendig. Wenn nicht, ist mit Schritt 2 fortzufahren.

Schritt 2:

Eine Datenschutz-Folgenabschätzung ist stets in den genannten Fällen des § 34 Abs. 3 durchzuführen.

- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen auf Basis einer automatisierten Verarbeitung wie Profiling, aus der bestimmte Entscheidungen resultieren. Hier ist nicht das Bewertungsverfahren als solches zu betrachten, sondern die Datenverarbeitung, die auf der Grundlage einer Bewertung (bspw. eines Profilings) zu einer (teilweisen) automatischen Entscheidung führt.[28]
- Auch bei einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. § 14 DSG-EKD ist die Anfertigung einer Datenschutz-Folgenabschätzung notwendig. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten, ist für die Notwendigkeit der Erstellung einer DSFA der Umfang der Verarbeitung [29] maßgeblich.
  Die Art. 29-Arbeitsgruppe empfiehlt im Rahmen der Klärung, ob es sich um eine „umfangreiche Verarbeitung“ handelt, die folgenden Faktoren zu berücksichtigen.
  - Die Zahl der betroffenen Personen
  - Das Datenvolumen oder das Spektrum an in Bearbeitung befindlichen Daten
  - Die Dauer und Permanenz der Datenverarbeitungstätigkeit sowie
  - die geografische Ausdehnung der Verarbeitungstätigkeit. [30]

- Eine Datenschutz-Folgenabschätzung ist darüber hinaus auch anzufertigen, wenn es sich bei der Datenverarbeitung um eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche handelt. Umfangreich bezieht sich hierbei sowohl auf einen räumlichen Aspekt, aber auch auf die Anzahl der potenziell Betroffenen. Darüber hinaus muss bei der Überwachung zudem das Merkmal der „Systematik“ gegeben sein. Dafür muss mindestens eine der nachfolgend aufgeführten Eigenschaften vorliegen:
  - systematisch vorkommend,
  - vereinbart, organisiert oder methodisch,
  - im Rahmen eines allgemeinen Datenerfassungsplans erfolgend,
  - im Rahmen einer Strategie erfolgend.

Ist eines der oben aufgeführten Merkmale erfüllt, ist die Anfertigung einer Datenschutz-Folgenabschätzung notwendig, wenn nicht, ist mit Schritt 3 fortzufahren.

[28] Sydow/Marsch DS-GVO/BDSG/Schwendemann DS-GVO Art. 35, Rn. 12;
[29] Die Art. 29-Arbeitsgruppe war ein unabhängiges Beratungsgremium der EU-Kommission zu Fragen des Datenschutzes.
[30] Sydow/Marsch DS-GVO/BDSG/Schwendemann DS-GVO Art. 35, Rn. 13;

Schritt 3:

Sollte sich in den vorangegangenen Schritten die Durchführung einer Datenschutz-Folgenabschätzung noch nicht als notwendig erwiesen haben, ist gem. § 34 Abs. 1 DSG-EKD final zu prüfen, ob eine andere hochriskante Verarbeitungstätigkeit gegeben ist. Gem. § 34 Abs. 1 DSG-EKD soll lediglich ein voraussichtlich hohes Risiko vorliegen. Das ist sinnig, weil das Bestehen eines Risikos erst durch die Durchführung der DSFA bestimmt werden kann. Zur Beantwortung der Frage, ob die Verarbeitung der personenbezogenen Daten ein wahrscheinlich hohes Risiko für die betroffene Person mit sich bringt, hat die Art. 29-Datenschutzgruppe die nachfolgenden Kriterien zur Einordnung von Verarbeitungsvorgängen benannt:

- Bewertung und Einstufung
- Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
- Systematische Überwachung
- Vertrauliche Daten oder höchst persönliche Daten
- Datenverarbeitung in großem Umfang
- Abgleichen und Zusammenführen von Datensätzen
- Daten zu schutzbedürftigen Betroffenen
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
- Betroffene Person wird an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert.

Wird in der Einzelfallprüfung final festgestellt, dass von den oben aufgeführten Kriterien mehr als zwei zutreffend sind, so ist in der Folge auch von einem hohen Risiko auszugehen und somit das Erfordernis zur Anfertigung einer Datenschutz-Folgenabschätzung gegeben.

4. Prüfung der Verhältnismäßigkeit und Notwendigkeit

Innerhalb der Verhältnismäßigkeits- und Notwendigkeitsprüfung werden die bereits selektierten Verarbeitungsvorgänge, ausgehend von den von ihnen verfolgten Zwecken, daraufhin bewertet, ob die dadurch verursachten Eingriffe in die Rechte und Freiheiten der betroffenen Personen im Verhältnis zum verfolgten bzw. angestrebten Zweck stehen und ob sie zur Erreichung des angestrebten Zwecks überhaupt notwendig sind oder ob es ggf. ein Mittel gibt, welches weniger intensiv in die Rechte der betroffenen Personen eingreift. Die Prüfung der Verhältnismäßigkeit und Notwendigkeit wird in vier Prüfungsschritte eingeteilt:

a) Legitimer Zweck

Legitim ist ein Zweck, wenn er auf das Wohl der Gemeinschaft gerichtet und erlaubt ist. Der Zweck darf nicht im Widerspruch zu Recht und Gesetz stehen.

Legitime Zwecke für die Verwendung der Kita-App und die damit einhergehenden Verarbeitungsvorgänge sind beispielsweise:

- Die Verbesserung und Erleichterung der Arbeitsstrukturen;
- Die Verbesserung der Erreichbarkeit;
- Die Verbesserung der Kommunikation mit den Personensorgeberechtigten, aber auch innerhalb des Teams;
- Belebung der Attraktivität der Kindertagesstätte.

b) Geeignetheit

Die Verarbeitungsvorgänge müssen geeignet sein, um eine Zweckerreichung herbeizuführen. Geeignet erscheint ein Mittel dann, wenn es den angestrebten Zweck zumindest fördert.

c) Erforderlichkeit

Zudem muss der Verarbeitungsvorgang innerhalb der Kita-App zur Zweckerreichung auch erforderlich sein. Ein Verarbeitungsvorgang ist dann als erforderlich einzustufen, wenn kein milderes Mittel gleicher Eignung zur Verfügung steht. Das bedeutet im Konkreten, dass kein milderes Mittel zur Verfügung stehen darf, dass in gleicher Weise geeignet wäre, den legitimen Zweck zu erreichen, jedoch die betreffende Person weniger belastet. Unter den zur Verfügung stehenden Mitteln ist stets das zu wählen, welches am geringsten in die Rechte der betroffenen Person eingreift.

d) Angemessenheit

Eine Verarbeitung ist dann als angemessen zu betrachten, wenn innerhalb der Interessenabwägung im Rahmen einer Zweck-Mittel-Relation die Abwägung zu Gunsten der verantwortlichen Stelle ausfällt. Innerhalb der Interessenabwägung sind die Interessen der verantwortlichen Stelle gegen die Interessen der betroffenen Personen abzuwägen und in Relation zu stellen.

5. Einhaltung der Prinzipien der Datenverarbeitung

Lt. Datenschutzgesetz der Evangelischen Kirche in Deutschland sind personenbezogene Daten nach den Grundsätzen gem. § 5 DSG-EKD zu verarbeiten. Die Rechenschaftspflicht hierfür liegt bei der verantwortlichen Stelle. Im Rahmen der DSFA ist aufzuführen, durch welche Maßnahmen die Grundsätze gem. § 5 DSG-EKD eingehalten und umgesetzt werden können.

a) Der Grundsatz der Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

aa) Grundsatz der Rechtmäßigkeit

Eine Verarbeitung ist rechtmäßig, wenn die Einwilligung des Betroffenen oder ein gesetzlicher Erlaubnistatbestand gem. §§ 6 Nrn. 1, 3-8 DSG-EKD vorliegt.

Eine Verarbeitung personenbezogener Daten innerhalb der Kita-App ist ausschließlich mit Einwilligung der betroffenen Personen rechtmäßig. Die Nutzung einer Kita-App durch die Personensorgeberechtigten, Angehörige, etc. ist freiwillig. Sie darf nicht verpflichtend für die Aufnahme in eine Kindertagesstätte sein. Daher ist die Kommunikation im Vorfeld einer Einführung bedeutsam für eine erfolgreiche Umsetzung. Insoweit sollte auch dargelegt werden, welche alternativen Informations- und Kommunikationswege für Personensorgeberechtigte, Angehörige, etc. vorgehalten werden, die eine Kita-App nicht nutzen können oder wollen.

ab) Grundsatz der Verarbeitung nach Treu und Glauben

Eine Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffene Person in der Lage ist, von der Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Verarbeitung informiert wird.

ac) Grundsatz der Transparenz

Um den Grundsatz der Transparenz zu gewährleisten, ist die betroffene Person im Rahmen der Informationspflichten schriftlich über die Verarbeitung zu informieren.

Die Umsetzung des Transparenzgrundsatzes ist durch die Zurverfügungstellung einer Datenschutzinformation möglich. Folgenden Inhalt sollten die Informationen enthalten:

- Name und Kontaktdaten der verantwortlichen Stelle sowie die Kontaktdaten der/des örtlich Beauftragten für den Datenschutz
- Zweck und Rechtsgrundlage der Verarbeitung. Dabei ist zwingend auf Vollständigkeit und Detailgenauigkeit zu achten
- Empfänger und Kategorien von Empfängern der personenbezogenen Daten
- Verarbeitung o. die Absicht des Verantwortlichen, die Daten in einem Drittland zu verarbeiten
- Angaben zur Speicherdauer
- Aufklärung des Betroffenen über die Rechte aus §§ 16 ff. DSG-EKD

Die Datenschutzinformation sollte den Personensorgeberechtigten vor Verarbeitung der personenbezogenen Daten innerhalb der Kita-App zur Verfügung gestellt werden. Dies kann in Kombination mit dem Einholen der erforderlichen Einwilligungen erfolgen.

b) Grundsatz der Zweckbindung

Personenbezogene Daten sind ausschließlich für die vorher festgelegten, eindeutigen und legitimen Zwecke zu erheben. Für jede Verarbeitung über den Zweck hinaus bedarf es einer neuen Rechtsgrundlage, vgl. § 7 DSG-EKD.

Die Grundsätze der Datenverarbeitung sollten ein fester und wiederkehrender Bestandteil des datenschutzrechtlichen Schulungs- und Sensibilisierungskonzepts der Mitarbeiter:innen sein. Wenn möglich und zur Zweckerfüllung ausreichend, sollten innerhalb der Kita-Apps ausschließlich die Pflichtfelder ausgefüllt werden. Grundsätzlich ist kritisch zu hinterfragen, ob die Erfassung der Daten zur Zweckerreichung notwendig ist.

c) Grundsatz der Datenminimierung

Personenbezogene Daten dürfen ausschließlich auf ein angemessenes sowie notwendiges Maß beschränkt, erfasst und verarbeitet werden.

Ist die Kita-App ursprünglich ausschließlich zur internen und externen Kommunikation angeschafft worden, soll jedoch zukünftig auch zur Erstellung eines Portfolios genutzt werden, so ist dafür vorab die Einwilligung der betroffenen Personensorgeberechtigten einzuholen, weil die anfänglich eingeholte Einwilligungserklärung im Zweifel nicht ausreichend ist.

d) Grundsatz der Richtigkeit

Es sind ausschließlich aktuelle und sachlich richtige Daten zu verarbeiten.

Wenn nicht die Möglichkeit der Datenübertragung aus bestehenden Systemen gegeben ist, sollten die personenbezogenen Daten durch die Personensorgeberechtigten selbst in die Kita-App eingepflegt werden. Somit können im Zweifel Übertragungs- bzw. Eingabefehler vermieden und der Arbeitsaufwand für das pädagogische Fachpersonal verschlankt werden.

e) Grundsatz der Speicherbegrenzung

Nach dem Grundsatz der Speicherbegrenzung dürfen personenbezogene Daten in der Kita-App nur so lange gespeichert werden, wie es zur Zweckerreichung erforderlich ist. Grundsätzlich gilt: Wenn der Zweck nicht (mehr) besteht und die Verarbeitung der personenbezogenen Daten nicht mehr erforderlich ist, müssen sie gelöscht werden.

Die Erforderlichkeit kann sich dabei insbesondere aus festgelegten Aufbewahrungsfristen ergeben, die einer Löschung entgegenstehen. Ein Löschpflicht kann sich auch aus einem berechtigten Löschbegehren betroffener Personen ergeben, beispielwiese wenn eine Einwilligung widerrufen wird.

Prüfschema

ea) Ist der Zweck der Daten entfallen?
Es kommt auf den ursprünglichen Zweck an: Eine Vorratshaltung für andere denkbare Zwecke ist nicht zulässig. Verlässt ein Kind die Kita, ist die Vorhaltung der Entwicklungsdokumentation und der darin enthaltenen personenbezogenen Daten daher nicht mehr erforderlich.

eb) Liegt eine gesetzliche Aufbewahrungspflicht vor?
Es ist zu prüfen, ob in einem Gesetz oder einer Rechtsvorschrift eine Mindestaufbewahrungsdauer vorgeschrieben ist. Derartige Fristen ergeben sich insbesondere im Bereich der Buchhaltung, für Geschäfts- oder Vertragsunterlagen aus der Kassationsordnung.

ec) Ist aus anderen Gründen eine Vorhaltung der Daten erforderlich?
Wenn keine gesetzliche Aufbewahrungsfrist besteht, kann dennoch eine weitere Aufbewahrung geboten sein, z.B. zu Dokumentations- und Beweiszwecken, wenn ein Gerichtsverfahren noch nicht abgeschlossen ist oder Schadensersatzpflichten nicht auszuschließen sind.

ed) Liegt eine Einwilligung der Betroffenen vor?
Eine wirksam erteilte Einwilligung kann eine Weiterverarbeitung auch über den ursprünglichen Zweck und die Dauer der Verarbeitung hinaus zulassen.

Nach Verlassen des Kindes aus der Kindertagesstätte sind sämtliche personenbezogenen Daten in ihrer Verarbeitung einzuschränken. Sind sämtliche im Prüfschema genannten Punkte zu verneinen, sind die personenbezogenen Daten zu löschen. Es ist darauf zu achten, dass die Daten nach der Löschung in der Clusterumgebung ausschließlich in anonymisierter Form vorgehalten werden

f) Grundsatz der Integrität und Vertraulichkeit

Personenbezogene Daten, die verarbeitet wurden, müssen durch geeignete technische und organisatorische Maßnahmen vor unbefugter und unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust oder unbeabsichtigter Beschädigung geschützt werden.

Erforderliche Maßnahme zur Einführung einer Kita-App sind dem Abschnitt D) „Erforderliche Unterlagen bzw. Maßnahmen für die Einführung einer Kita-App“ zu entnehmen.

6. Risikobeurteilung

Eine Datenschutz-Folgenabschätzung ist gem. § 34 Abs. 1 DSG-EKD nur für die geplante Verarbeitung, nicht für das IT-System vorgesehen.

Risikoidentifikation	**Beschreibung des Risikos**
	Kurze Benennung der Verarbeitung, der beteiligten Personen sowie die Nennung der Datenkategorien.
	Benennung der Risikoquellen Was hat zu dem Schadenseintritt geführt? Ist die Risikoquelle menschlicher oder technischer Art? ▪ Interne menschliche Quelle ▪ Externe menschliche Quelle ▪ Interne / externe technische Quelle **Beispiele für Risikoquellen:** ▪ Interne:r Mitarbeiter:in ▪ Externe:r Mitarbeiter:in ▪ Betroffene:r ▪ Sonstige:r Dritter ▪ Softwarefehler ▪ Hardwaredefekt (physikalisch) ▪ Umwelteinflüsse (Naturgewalt) ▪ Cyberkriminelle (Hacker/Schadsoftware)

- Staatliche Institutionen (Nachrichtendienste, Strafverfolgung)
- Geschäftsführung

Risikoursache

Was führt zum Schadenseintritt?

Zum Schadenseintritt kann sowohl die Nichteinhaltung der Grundsätze rechtmäßiger Datenverarbeitung gem. § 5 DSG-EKD führen, die Nichtwahrnehmung der Betroffenenrechte als auch anderweitige Verstöße gegen das Datenschutzgesetz der Evangelischen Kirche in Deutschland.

Beispiele für Ursachen:

- Unbefugte und unrechtmäßige Verarbeitung der personenbezogenen Daten
- Verarbeitung entgegen Treu und Glauben
- Intransparente Verarbeitung
- Unbefugte Offenlegung
- Unbeabsichtigter Verlust, Zerstörung oder Schädigung
- Verweigerung der Betroffenenrechte
- Verwendung der Daten zu inkompatiblen Zwecken
- Verarbeitung nicht vorhergesehener Daten
- Verarbeitung nicht richtiger Daten
- Fehlerhafte Verarbeitung
- Verarbeitung über die Speicherfrist hinaus
- Der Verarbeitungsvorgang selbst, wenn der Schaden in der Durchführung der entsprechenden Verarbeitung liegt
- Verarbeitung entgegen dem Zweckbindungsgrundsatz

Möglicher Schadenseintritt für die betroffene Person

Welcher Schadenseintritt (physisch, materiell, immateriell) ist möglich?

- Diskriminierung
- Identitätsdiebstahl- oder betrug
- Lebensgefährdung
- Finanzieller Schaden
- Rufschädigung
- Existenzgefährdung
- Unbefugte Aufhebung von Pseudonymisierung
- Verlust des Arbeitsplatzes
- Geheimnisoffenbarung
- Bloßstellung
- Gesellschaftliche Nachteile
- Wirtschaftliche Nachteile
- Sonstige Folgen

Risikoanalyse und Bewertung (status quo)	Eintrittswahrschein-lichkeit	Schadensausmaß	Risikobewertung
	▪ Vernachlässigbar (1) ▪ Eingeschränkt (2) ▪ Wesentlich (3) ▪ Maximal (4)	▪ Vernachlässigbar (1) ▪ Eingeschränkt (2) ▪ Wesentlich (3) ▪ Maximal (4)	▪ Vernachlässigbar (1) ▪ Eingeschränkt (2) ▪ Wesentlich (3) ▪ Maximal (4)

Im Zuge der Risikobeurteilung sind die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu eruieren. [31]

Tabelle 1 und 2 zeigen die hinter den rangskalierten Merkmalsausprägungen stehenden Annahmen zur angemessenen Einstufung des identifizierten Risikoszenarios. [32]

Wert	Beschreibung
Vernachlässigbar	Für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Bedrohung eintreten zu lassen.
Eingeschränkt	Für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Bedrohung eintreten zu lassen.
Wesentlich	Für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Bedrohung eintreten zu lassen.
Maximal	Für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Bedrohung eintreten zu lassen.

Tabelle 1: Risikoausprägung für Eintrittswahrscheinlichkeit [33]

Wert	Beschreibung
Vernachlässigbar	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
Eingeschränkt	Betroffenen erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
Wesentlich	Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.
Maximal	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

Tabelle 2: Risikoausprägungen für Schadensausmaß [34]

Nach Analyse und Zuordnung werden die jeweiligen Skalenwerte in der Risikomatrix verortet.

[31] Vgl. ErwGr. 75 und 76 DSGVO;

[32] Vgl. Bitkom, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 ff.;

[33] Vgl. Bitkom, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 30 f.;

[34] Vgl. Bitkom, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 f.;

		Eintrittswahrscheinlichkeit			
		Vernachlässigbar	**Eingeschränkt**	**Wesentlich**	**Maximal**
Schadensausmaß	**Maximal**	Normal (4)	Normal (8)	Hoch (12)	Hoch (16)
	Wesentlich	Normal (3)	Normal (6)	Normal (9)	Hoch (12)
	Eingeschränkt	Gering (2)	Normal (4)	Normal (6)	Normal (8)
	Vernachlässigbar	Gering (1)	Gering (2)	Normal (3)	Normal (4)

7. Maßnahmenplan

Ein Maßnahmenplan konkretisiert die Maßnahmen, mit denen sich die identifizierten Risiken eindämmen bzw. minimieren lassen.

8. Erstellung eines DSFA-Berichts

Abschließend ist durch die verantwortliche Stelle ein DSFA-Bericht zu erstellen. Dieser Bericht ist für Prüffälle durch Dritte, wie z.B. die Datenschutzaufsichtsbehörde vorzuhalten. Soweit ein Datenschutzmanagement besteht, sollte dieser dort eingestellt werden.

D ERFORDERLICHE MASSNAHMEN ZUR EINFÜHRUNG DER KITA-APP

I PERSONENSORGEBERECHTIGTE

1. Elternabend vor Einführung der Kita-App

Seien Sie transparent und nehmen Sie die Eltern bei der Einführung der Kita-App mit. Je transparenter Sie sind, desto höher gestaltet sich die Akzeptanz und Befürwortung für das Projekt. Nutzen Sie die Veranstaltung eines Elternabends zum direkten Austausch mit den Personensorgeberechtigten. Im Nachgang sollte zudem eine ausführliche schriftliche Information für die Personensorgeberechtigten zur Verfügung gestellt werden.

2. Einwilligungserklärungen

Verarbeiten Sie keine personenbezogenen Daten innerhalb einer Kita-App ***ohne gültige Rechtsgrundlage***. Vor Einführung und somit vor Verarbeitung von personenbezogenen Daten ist von den Personensorgeberechtigten und Notfall- bzw. Abholkontakten eine Einwilligung einzuholen. Folgende Einwilligungen sind notwendig:

- Einwilligung zur App-Nutzung
  Für die App-Nutzung, d.h. für die Registrierung der Nutzer innerhalb der App ist eine Einwilligung der betroffenen Personen notwendig.

- Einwilligung für die Verarbeitung von personenbezogenen Daten von Personensorgeberechtigten, Kita-Kindern, Notfall-Kontakten und Abholberechtigten
  Innerhalb der Kita-App werden quantitativ, aber auch qualitativ eine Menge personenbezogener Daten verschiedener Kategorien verarbeitet. Dafür ist vorab die Einwilligungserklärung der betroffenen Personen einzuholen.

- Einwilligung für die Verarbeitung von Gesundheitsdaten (Impfstatus, lebensbedrohliche Erkrankungen)
  Gesundheitsdaten gehören zu den besonderen Kategorien personenbezogener Daten gem. § 4 Nr. 2 DSG-EKD. Gem. § 13 Abs. 1 DSG-EKD besteht für diese Art von Daten ein ***Verarbeitungsverbot mit Ausnahmevorbehalt***. Die Ausnahmen sind in § 13 Abs. 2 DSG-EKD normiert. Unter anderem gehören zu den Ausnahmen das Einholen einer Einwilligung der betroffenen Personen.

- Verarbeitung von Bildnissen (Fotos) und Videoaufnahmen
  Bei Bildnissen (Fotos) und Videoaufnahmen von identifizierbaren Personen handelt es sich stets um personenbezogene Daten gem. § 4 Nr. 1 DSG-EKD. Bei digitalen Bildnissen ist zudem häufig auch Zeit und Ort der Aufnahmen gespeichert.

- In Bezug auf Bilder und Videoaufnahmen wird nicht nur das Datenschutzgesetz der Evangelischen Kirche in Deutschland tangiert, sondern häufig auch das KunstUrhG (Kunsturhebergesetz). Für die Verarbeitung solcher personenbezogenen Daten ist stets eine Einwilligung der betroffenen Person, bei Kindern und Jugendlichen die Einwilligung der Personensorgeberechtigten notwendig. Ob zusätzlich eine Einwilligung des Jugendlichen notwendig ist, hängt von der Einsichtsfähigkeit des Jugendlichen ab. Im Kindergartenalter ist von einer Einsichtsfähigkeit nicht auszugehen, sodass die Einwilligung der Personensorgeberechtigten ausschlaggebend ist.
  Auch nach § 22 KunstUrhG dürfen Bilder nur mit Einwilligung des Abgebildeten verarbeitet oder öffentlich zur Schau gestellt werden. Ausnahmen dieses Grundsatzes ergeben sich aus § 23 KunstUrhG:

- Bildnisse aus dem Bereich der Zeitgeschichte
  Maßgeblich, ob es sich um ein Bildnis aus dem Bereich der Zeitgeschichte handelt, ist der Begriff des Zeitgeschehens. Dies ist grundsätzlich nicht wörtlich zu verstehen, sondern am Informationsinteresse der Öffentlichkeit zu bestimmen. Nach dem Grundsatz der Verhältnismäßigkeit sind bei der Frage des zeitgeschichtlichen Ereignisses auch die Interessen der Betroffenen zu berücksichtigen.[35]

[35] Dreier/Schulze UrhG § 23 KUG; Rn. 11

- Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen.
- Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben. Dies umfasst Ansammlungen von Menschen, die den kollektiven Willen haben, etwas gemeinsam zu tun. Zusätzlich muss der Wille vorhanden sein, von Dritten wahrgenommen zu werden.[36]
- Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verarbeitung oder Schaustellung einem höheren Interesse der Kunst dient.

3. Datenschutzinformation gem. § 17 DSG-EKD

Zur Erfüllung des Verarbeitungsgrundsatzes der Transparenz ist es sinnvoll, den Informationenpflichten - entgegen des Gesetzeswortlauts „auf Verlangen“ - grundsätzlich bereits vor Verarbeitung nachzukommen. Diese Informationspflicht kann man- wie oben beschrieben - durch einen Elternabend vor Einführung einer Kita-App oder durch Aushändigung einer detaillierten Beschreibung der Verarbeitungsvorgänge erfüllen.

4. Nutzungsbedingungen der Kita-App

Vor erstmaliger Nutzung der App sind die Nutzungsbedingungen der App-Firma zu bestätigen. Nutzungsbedingungen sind einseitige vorvertragliche Vertragsbedingungen, mit denen der Anbieter die Nutzer der App über Ihre Rechte und Pflichten im Rahmen der App-Nutzung informiert.

II. MITARBEITRER:INNEN: / MITARBEITERVERTRETUNG (MAV)

1. Dienstvereinbarung

Weil die Einwilligung aufgrund der Anforderungen des § 49 DSG-EKD im Anstellungsverhältnis nicht ausreichend Sicherheit bringt, ist der Abschluss einer Dienstvereinbarung mit der MAV notwendig (siehe hierzu auch oben unter II 1. cc)).

2. Informationspflichten gem. § 17 DSG-EKD

Es ist sinnvoll, die Informationspflichten gem. § 17 DSG-EKD in die Dienstvereinbarung einfließen zu lassen, um für die Mitarbeiter:innen ein möglichst hohes Maß an Transparenz zu gewährleisten.

3. Mitbestimmungsrechte der MAV gem. § 40 MVG-EKD

Unabhängig vom Abschluss einer Dienstvereinbarung bestehen gesetzliche Beteiligungsrechte der MAV. Je nach Nutzungsmöglichkeit der App können mehrere Mitbestimmungstatbestände berührt sein. Neben § 40 lit. k (Einführung und Anwendung

[36] Dreier/Schulze UrhG § 23 KUG; Rn. 39

von Maßnahmen oder technischen Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Mitarbeitenden zu überwachen) kann auch § 40 lit. j (Maßnahmen zur Hebung der Arbeitsleistung und Erleichterung des Arbeitsablaufs) berührt sein. Bei Apps mit Arbeitszeiterfassung dürfte § 40 lit. d MVG-EKD in Frage kommen.

Neben den Beteiligungsrechten hat die MAV Informationsrechte. Das bedeutet, dass sie rechtzeitig und umfassend über die Einführung einer App zu informieren ist. Rechtzeitig ist eine Unterrichtung nur dann, wenn die MAV so frühzeitig eingebunden ist, dass sie sich angemessen in den Sachstand einarbeiten und noch argumentativ auf den Entscheidungsprozess der Dienststellenleitung Einfluss nehmen kann.

4. Einwilligung für Fotos

Gerade im Kindergarten-Alltag werden von Alltagssituationen zur anschließenden Verarbeitung innerhalb einer Entwicklungsdokumentation oder zur Portfolioerstellung Fotos angefertigt. Aus der Situation heraus, manchmal auch im Beisein von Mitarbeiter:innen. Mitarbeiter:innen sind in diesem Zusammenhang insoweit zu sensibilisieren, dass es für sie keine Verpflichtung gibt, bildlich abgelichtet zu werden. Im Zweifel sollte dafür vorab die Einwilligung der Mitarbeiter:innen eingeholt werden.

III. KITA-TRÄGER / KITA-VERBAND

1. IT-Sicherheitskonzept

Ein IT-Sicherheitskonzept ist eine Verschriftlichung von Maßnahmen zum Schutz der IT-Infrastruktur eines Unternehmens. Ein IT-Sicherheitskonzept, dient der Umsetzung des IT-Grundschutzes sowie der Gewährleistung der Informationssicherheit und soll die Verfügbarkeit, Integrität und Vertraulichkeit der IT-Systemen gewährleisten.

Komponenten eines IT-Sicherheitskonzeptes

- Selektierung der personenbezogenen Daten
- Zielsetzung: Welche Ziele sollen durch das IT-Sicherheitskonzept erreicht werden?
- Zuständigkeit: Wer ist für die Umsetzung des IT-Sicherheitskonzepts zuständig?
- Status quo: Wie ist der Status quo in Hinblick auf die IT-Sicherheit. Welche Maßnahmen wurden bereits umgesetzt?
- Maßnahmen: Welche Maßnahmen sind notwendig, um mögliche Gefahren zu minimieren und die IT-Sicherheit zu optimieren?
- Umsetzungszeitraum: In welchem Zeitraum sollen die Maßnahmen umgesetzt werden?
- Sensibilisierung der Mitarbeiter:innen: Auf welchem Wege werden Mitarbeiter:innen über das IT-Sicherheitskonzept informiert?
- Evaluierung der Maßnahmen: In regelmäßigen Abständen sollten die Maßnahmen auf ihre Wirksamkeit hin überprüft und ggf. angepasst werden.

2. Mobile Device Management System (MDM)

Ein Mobile Device Management (auch MDM genannt) umfasst die Inventarisierung und zentrale Verwaltung von Geräten (Tablets, Laptops, Smartphones) durch einen Administrator. Ein MDM verfolgt den Zweck, die Sicherheit und Funktionalität der Geräte zu gewährleisten und zu optimieren. Folgende Funktionen werden durch ein MDM abgedeckt:

- Geräteinventarisierung
- Inhaltsverwaltung
- Zentrale Steuerung von Software-Updates
- Identitätsmanagement
- App-Verwaltung
- Gerätekonfiguration
- Gewährleistung der Sicherheit

Gerade in Kindertagesstätten ist es von zentraler Bedeutung, die Geräte in ein MDM einzubinden, um diese im Falle eines Einbruchs oder Diebstahls übergeordnet zurücksetzen und bereinigen zu können.

Wird das Mobile Device Management System durch einen externen Dienstleister administriert, ist sowohl mit dem Dienstleister (welcher als Auftragsverarbeiter fungiert) als auch mit dem MDM-Service ein AV-Vertrag zu schließen.

3. Personalisierte Zugänge zur Kita-App

Durch personalisierte Zugänge zur Kita-App kann ein Identitäts- und Berechtigungsmanagement umgesetzt werden. Ein Identitätsmanagement stellt sicher, dass ausschließlich autorisierte Mitarbeiter:innen Zugriff auf Systeme und Ressourcen erhalten. Ein Berechtigungsmanagement soll gewährleisten, ob und in welchem Umfang Benutzer:innen auf Informationen und Dienste zugreifen, diese bearbeiten, verwalten und weiterleiten können. Darüber hinaus wird durch ein Identitäts- und Berechtigungsmanagement einigen Grundsätzen der Datenverarbeitung gem. § 5 DSG-EKD Genüge getan.

4. WLAN-Regelungen

WLAN steht für „Wireless Local Area Network“. Es wird in der Regel dafür genutzt, um ohne Kabel ins Internet zu gelangen. Dazu nimmt das Endgerät eine Funkverbindung zu einem Access-Point auf. Die Nutzung des WLAN kann jedoch auch Risiken mit sich bringen. Die WLAN-Nutzung in Kindertagesstätten sollte definiert und verschriftlicht werden. Ist die Nutzung lediglich von dienstlichen oder auch von privaten Geräten der Mitarbeiter:innen gestattet? Dürfen auch Gäste (beispielsweise Personensorgeberechtigte) das WLAN nutzen? Wird zu diesem Zweck ein Gäste-WLAN zur Verfügung gestellt?

Achten Sie im Zusammenhang mit dem WLAN auf folgende Maßnahmen:

- Wählen Sie ein langes und komplexes WLAN-Passwort. Dieses sollte aus mindestens 20 Zeichen bestehen;
- Ändern Sie den voreingestellten Netzwerknamen, sodass dieser keine hilfreichen Informationen für potenzielle Angreifer bietet;
- Achten Sie auf eine Aktualität der Firmware;
- Achten Sie auf eine aktive Firewall;
- Richten Sie wenn möglich ein Gast-Netzwerk ein.

5. Firewall

Eine Firewall ist eine Netzwerksicherheitsvorrichtung, die den gesamten ein- und ausgehenden Datenverkehr des Netzwerks überwacht und einen Zugriff auf den Rechner von außen durch unbefugte Dritte verhindern soll. Grundsätzlich sollte keine Kita-App ohne den Einsatz einer Firewall betrieben werden.
Im Wesentlichen gibt es zwei verschiedene Varianten von Firewalls:
Die Personal-Firewall und die externe Firewall.
Die Personal-Firewall wird als Firewall-Software lokal auf dem Rechner installiert.
Die externe Firewall läuft auf einer externen Hardware. Sie kontrolliert und filtert den Datenverkehr zwischen zwei Netzwerken. Sie bietet im Gegensatz zur Personal-Firewall nicht nur für den jeweiligen Rechner Schutz, sondern kann auch einen Verbund mehrerer Rechner schützen. Die externe Firewall bietet im Gegensatz zur Personal-Firewall die stabilere Sicherheitslösung, weil diese durchaus schwieriger zu manipulieren ist. Das liegt primär daran, dass die möglichen Angriffe nicht direkt auf das interne Netz treffen.

6. Dienstliche E-Mail-Adressen

Grundsätzlich sollten alle pädagogischen Mitarbeiter:innen mit einer dienstlichen evlka.de-E-Mail-Adresse ausgestattet werden. Diese sind zum einen für die Registrierung innerhalb der Kita-App und zum anderen für die interne bzw. externe Kommunikation der Mitarbeiter:innen unerlässlich.

Als Zwischenlösung für den Registrierungsprozess besteht alternativ die Möglichkeit, die Funktions-E-Mail-Adresse der Kindertagesstätte anzugeben und direkt nach Registrierung das Passwort zu ändern. Diese Vorgehensweise stellt lediglich eine Behelfslösung dar und sollte aus datenschutzrechtlichen Gründen zwingend durch eine Implementierung dienstlicher E-Mail-Adressen ersetzt werden.

Zudem ist für die Nutzung von Seafile (Cloudspeicherdienst) eine personalisierte E-Mail-Adresse der Mitarbeiter:innen notwendig.

7. Cloudspeicherdienst „Seafile“

Grundsätzlich sollten lokal auf den Tablets keine personenbezogenen Daten gespeichert werden. Dazu zählen in Kindertagesstätten vornehmlich Fotos, Videos und

Entwicklungsdokumentationen. Wenn möglich, sind diese mit entsprechender Einwilligung der Personensorgeberechtigten in der Kita-App oder als Zwischenspeicherung bei einem datenschutzkonformen Cloudspeicherdienst hochzuladen.

Neben einer Dokumentenablage (auf zentralen landeskirchlichen Servern) bietet Seafile eine integrierte webbasierte Textverarbeitung und Tabellenkalkulation (OnlyOffice), sodass mehrere Mitarbeiter:innen kollaborativ an einem Dokument arbeiten können. Mittels Rechte- und Nutzerkonzept können Rechte an die jeweiligen Nutzer vergeben werden. Seafile bietet die Möglichkeit, Ordner zu verschlüsseln und Dateien temporär (mit zeitlicher Befristung) zu erstellen und freizugeben.

Es empfiehlt sich, personenbezogene Daten (Bildnisse, Entwicklungsdokumentationen) nicht länger als 30 Tage auf dem Endgerät (Tablets) vorzuhalten. Danach sind diese vom Endgerät zu löschen. Eine solche Vorgehensweise führt dazu, dass ausschließlich geringe Datenmengen auf den Endgeräten abgelegt sind.

8. Beschaffungsprozess Hardware bzw. Apps definieren

Definieren Sie den Beschaffungsprozess (von Hardware und Apps) und schaffen Sie dadurch klare Zuständigkeiten. Folgende Schritte des Beschaffungsprozesses gilt es zu definieren:

Beschaffungsprozess Hardware:

- Bedarfsfeststellung: Was wird benötigt?
- Angebotseinholung u. Angebotsvergleich: Wer ist für das Einholen des Angebots zuständig? An welcher Stelle werden die Angebote verglichen?
- Beschluss: Ist vor Abschluss eines Kaufvertrages der Beschluss des Trägers; geschäftsführender Ausschuss; Amtsleitung; betriebswirtschaftliche Leitung notwendig?
- Vertragsverhandlungen bzw. -abschluss: Wer führt die Vertragsverhandlungen mit dem Lieferanten?
- Rechnungsabwicklung
- Ausrollen der Hardware: Ist vor Ausrollen der Hardware eine Konfiguration notwendig, sollte dies von der IT übernommen werden?

Beschaffungsprozess Apps:

- Bedarfsfeststellung: Welche App wird benötigt?
- Entscheidung: Die Notwendigkeit zur Anschaffung der App sollte an übergeordneter Stelle (pädagogische Leitung des Verbands/Trägers) erfolgen.

- Datenschutzrechtliche Prüfung: Jede App sollte auf Datenschutzkonformität überprüft werden. Nach Freigabe durch den Datenschutz wird diese dann übergeordnet mittels MDM durch die IT oder durch den Administrator auf die Endgeräte aufgespielt.

9. Berechtigungskonzept für die Kita-App Nutzung

Ein Berechtigungskonzept stellt das Herzstück eines Datenschutzkonzeptes dar. Das Ziel einer solchen Verschriftlichung ist, dass ausschließlich befugte Personen einen Zugriff im notwendigen Ausmaß auf die zugewiesenen Daten haben.
Im Berechtigungskonzept werden Zugriffsregeln erstellt. Sie umfassen die Rechte für das:

- Lesen
- Schreiben
- Ändern
- Löschen

Diese Rechte können bereits auf Betriebssystemebene (Active Directory, MDM) oder aber auf Anwendungsebene (Anwendungen oder Apps) vergeben werden.
Mit der Umsetzung eines Berechtigungskonzepts kommen Sie den gesetzlichen Pflichten aus § 27 DSG-EKD nach.

- § 5 Abs. 1 Nr. 6 DSG-EKD

Der Grundsatz der Integrität und Vertraulichkeit verpflichtet bei Verarbeitung personenbezogener Daten zur Gewährleistung „angemessener Sicherheit“.[37] Werden Benutzerrechte nach dem „Need-to-know-Prinzip“ und dem „Need-to-do-Prinzip“ vergeben, trägt das zu einer „angemessenen Sicherheit“ bei.

- § 27 Abs. 1 Nr. 2 DSG-EKD

Es sind technische und organisatorische Maßnahmen zum Schutze der personenbezogenen Daten zu implementieren. Die Erstellung eines Berechtigungskonzepts bietet in diesem Zusammenhang Schutzmaßnahmen in Form einer Zugriffs- und Zugangskontrolle.

- § 5 Abs. 2 DSG-EKD

Zudem wird durch ein Benutzerkonzept dem Grundsatz der Rechenschafts- und Nachweispflicht Genüge getan.

[37] Ralph Wagner in Wagner EKD-Datenschutzgesetz, § 5, Rn. 47;

Inhalt eines Berechtigungskonzepts:

- Zusammentragen aller notwendigen Informationen
- Erstellung digitaler Identitäten
- Bestimmung der Zugriffsrechte
  - Keine Rechte
  - Leserechte
  - Schreibrechte
  - Änderungsrechte
  - Vollzugriff
- Bestimmung von Rollenkonzepten
  Anstatt der Bestimmung der Zugriffsrechte kann es mitunter sinnvoll sein, sogenannte Rollenkonzepte miteinzubeziehen. Das gilt vor allem dann, wenn mehrere Personen aufgrund gleicher Aufgaben dieselben Berechtigungen benötigen.
- Überprüfung und Auditierung
- Eine Auditierung bewertet, ob die eingeführten Prozesse die geforderten Standards erfüllen.
  Aufgrund der Dynamik des Datenschutzrechts ist auch das Konzept stetig zu überprüfen und ggf. anzupassen.

10. Regelungen zur Verarbeitung von Fotos- und Videos

Übergeordnet (auf Träger- o. Verbandsebene) sollten einheitliche Regelungen zur Verarbeitung von Fotos- und Videos definiert und verschriftlicht werden.

11. Verzeichnis von Verarbeitungstätigkeiten (VVT)

Gem. § 31 DSG-EKD führt jede verantwortliche Stelle ein Verzeichnis von Verarbeitungstätigkeiten, die Ihrer Zuständigkeit unterliegen. Ein VVT dient als Grundlage für eine Datenschutzdokumentation und setzt den Grundsatz der Rechenschaftspflicht gem. § 5 Abs. 2 DSG-EKD um.
Ausnahmen von der Pflicht zur Führung eines VVT ergeben sich aus § 31 Abs. 5 DSG-EKD.

Danach sind verantwortliche Stellen und Auftragsverarbeiter mit weniger als 250 Mitarbeiter:innen regelmäßig nicht verpflichtet, ein VVT zu führen. Dabei ist es nicht maßgeblich, ob alle Mitarbeiter:innen mit der Verarbeitung von personenbezogenen Daten betraut sind. Gemäß dem Wortlaut des § 31 DSG-EKD ist die Zahl der beschäftigten Personen gemeint.

Anderes gilt jedoch hinsichtlich der Verarbeitungstätigkeiten, die die Verarbeitung von besonderen Kategorien personenbezogener Daten gem. § 4 Nr. 2 DSG-EKD einschließen. In diesen Fällen sind angesichts des Risikos für die Rechte und Freiheiten der betroffenen Personen dennoch entsprechende Verzeichnisse zu erstellen. [38]

[38] Tino Naumann in Wagner EKD-Datenschutzgesetz, § 32, Rn. 36.

In Kindertagesstätten wird die Erstellung eines VVT regelmäßig notwendig sein, weil besondere Kategorien von personenbezogenen Daten in Form von Gesundheitsdaten aber auch die ethnische Herkunft erhoben werden.

Überprüfung der VVTs beim Auftragsverarbeiter
Vor Abschluss eines Auftragsverarbeitungsvertrags mit einem Kita-App-Unternehmen sollten die VVTs des Unternehmens angefordert und überprüft werden.

Folgende Angaben sollte das Verzeichnis von Verarbeitungstätigkeiten enthalten:

- Name und Kontaktdaten der verantwortlichen Stelle und der/des örtlichen Beauftragten für den Datenschutz
- Verarbeitungszwecke
- Beschreibung der Kategorien von betroffenen Personen sowie der personenbezogenen Daten
- ggf. Verwendung eines Profilings
- Kategorien von Empfängern von Datenübermittlungen
- Datenübermittlung in ein Drittland zzgl. der getroffenen Garantien
- Löschfristen
- Beschreibung der technischen und organisatorischen Maßnahmen (TOMs)

Für das Verzeichnis von Verarbeitungstätigkeiten für verantwortliche Stellen stellt der BfD-EKD im Internet ein entsprechendes Muster nebst Merkblatt zur Verfügung. (https://datenschutz.ekd.de/infothek-items/verzeichnis-der-verarbeitungstaetigkeiten)

12. Technische und organisatorische Maßnahmen (TOMs)

Technische und organisatorische Maßnahmen sind Maßnahmen, welche die Sicherheit der verarbeiteten personenbezogenen Daten gewährleisten sollen. Die Rechtsgrundlage für diese Verpflichtung befindet sich in § 27 Abs. 1 DSG-EKD. Danach hat die verantwortliche Stelle unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis darüber führen zu können.

Folgende Maßnahmen sind gem. § 27 Abs. 1 Nr. 1-4 DSG-EKD zu ergreifen:

- Pseudonymisierung, Anonymisierung und Verschlüsselung
- Eine dauerhafte Sicherstellung der Vertraulichkeit, Integrität und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung von personenbezogenen Daten
- Die Fähigkeit zur Wiederherstellung der personenbezogenen Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen

Eine Konkretisierung oder Aufführung möglicher Maßnahmen ist dem DSG-EKD nicht zu entnehmen. Die Anlage zu § 9 Satz 1 BDSG „alte Fassung“ bietet hingegen eine Definition der technischen und organisatorischen Maßnahmen unter Benennung einiger Bereiche.

Beispiele für technische Maßnahmen könnten sein:

- Zugriffskontrollen: Ein Rollen- und Benutzerkonzept regelt die Zugriffsrechte, sodass nur autorisierte Personen auf personenbezogene Daten zugreifen können.
- Firewall: Eine Firewall schränkt den Zugriff auf personenbezogene Daten von unbefugten Dritten ein.
- Virenschutz: Auch das Installieren und Aktualisieren eines Virenschutzes bietet einen Schutz der personenbezogenen Daten.
- Patches und Updates: Durch Patches und Updates wird das System bzw. die Software auf dem neusten Stand gehalten und Sicherheitslücken geschlossen.
- Datensicherung: Das Durchführen regelmäßiger Backups stellt sicher, dass Daten im Falle eines Datenverlustes rasch wiederhergestellt werden können.

Überprüfung der TOMs beim Auftragsverarbeiter

Vor Abschluss eines Auftragsverarbeitungsvertrages sind auch die technischen und organisatorischen Maßnahmen des Kita-App-Unternehmens zu überprüfen. Sollten diese nicht aussagekräftig und vollständig sein, ist von einem Vertragsabschluss abzuraten.

Beispiele für organisatorische Maßnahmen:

- Datengeheimnis: Eine Verpflichtung der Mitarbeiter:innen auf das Datengeheimnis.
- Sensibilisierung der Mitarbeiter:innen: Regelmäßige Schulungen sorgen für eine Sensibilisierung der Mitarbeiter:innen im Umgang mit personenbezogenen Daten.
- Beauftragung eines/einer Datenschutzbeauftragten: Die Implementierung eines Datenschutzkonzeptes führt zu einem datenschutzrechtlichen Bewusstsein und somit zu mehr Sicherheit der verarbeiteten personenbezogenen Daten.

Auch bei der Erfassung der TOMs gilt der Grundsatz der Nachweisbarkeit gem. § 5 Abs. 2 DSG-EKD. Der Verantwortliche muss die Grundsätze der Verarbeitung personenbezogener Daten gem. § 5 Abs. 1 DSG-EKD nachweisen können.

13. On- und Off-Boarding von Mitarbeiter:innen

Im Falle einer Einstellung aber auch Entlassung von Mitarbeiter:innen sind in Bezug auf die IT sowie Nutzung der Kita-App einheitliche Prozesse durch die Verantwortlichen zu definieren.
Diese Prozesse sollten in enger Abstimmung mit der Geschäftsführung der Kindertagesstätten, der IT sowie der Leitung der jeweiligen Kindertagesstätte definiert und einheitlich vorgegeben werden.

14. Datenschutzleitlinie

Eine Datenschutzleitline ist ein „Regelungskatalog“ zu internen Themen des Datenschutzes und dient der Anleitung sowie der Orientierung der Mitarbeiter:innen. Der Inhalt einer Datenschutzleitlinie wird einseitig durch die Geschäftsführung der Kindertagesstätten festgelegt, verschriftlicht und an die Mitarbeiter:innen ausgegeben. Eine Kenntnisnahme ist durch die Mitarbeiter:innen schriftlich zu bestätigen.

Inhalt einer Datenschutzleitlinie:

- Angabe zur verantwortlichen Stelle sowie ggf. die Kontaktdaten zum/zur Datenschutzbeauftragten
- Präambel
- Eine Präambel ist eine Einleitung, die vor die eigentliche Vereinbarung gestellt wird.

  Inhalte einer Präambel:
  - Die allgemeine Interessenlage der Vertragsparteien;
  - Beschreibung der Situation, warum erscheint eine Verschriftlichung notwendig?
  - Eine Fixierung der rechtlichen Ausgangslage, welche Normen sind anwendbar?
  - Zielsetzung.
- Geltungsbereich und Geltungsdauer
- Gegenstand der Regelung
- Ziel der Datenschutzleitlinie
- Ggf. Begriffsbestimmungen
- Ggf. Nutzungsbestimmungen zur dienstlichen Hard- und Software
- Ggf. Nutzungsbestimmungen dienstliche E-Mails-Accounts
- Ggf. Nutzungsbestimmungen Telefonanlage (bspw. Voice Over IP)
- Ggf. Nutzungsbestimmungen WLAN
- Ggf. Nutzungsbestimmungen der Kita-App
- Ggf. Nutzungsbestimmungen zur datenschutzkonformen Vernichtung
- Ggf. Regelungen zum Datenaustausch
- Einhaltung der Prinzipien der Datenverarbeitung
- Überprüfung und Überarbeitung
- Kenntnisvermerk
- Ort/Datum sowie Unterschrift Mitarbeiter:in