Vorbereitungen für den geplanten Einsatz von App-Software und Online-Diensten im KITA-Bereich

Beachten Sie den Hinweis in der Fußnote[1].

Die folgenden Übersichten lassen erkennen, dass sich ein Team aus Mitarbeitern des Kita-Trägers sowie der Fachleute für Datenschutz und IT frühzeitig und systematisch im Rahmen eines Projektes mit den genannten Anforderungen und sich daraus ergebenden Aufgaben befassen muss. Empfehlenswert ist die Nutzung gemeinsamer Ressourcen durch Kooperation von Trägern und Einrichtungen, die das gleiche Ziel verfolgen.

Allgemeine Checkliste zur internen Verantwortung im KITA-Bereich

- ☐ Liste und ggf. Beschreibung der konkreten Anforderungen
  - Warum und wofür soll eine App-Software oder ein Online-Dienst eingesetzt werden?
    - alle oder nur bestimmte Funktionen?
  - Sind die Zwecke klar benannt?
    - Dienst- und Personalplanung
    - Kommunikation mit Eltern
    - Datenaustausch intern/extern
    - Vertragsabwicklung mit Eltern
    - Abrechnung von Elternbeiträgen
    - Dokumentation der kindlichen Entwicklung
    - …….
  - Sind die Zwecke durch den Auftrag der kirchlichen Stelle bzw. eine rechtliche Grundlage gedeckt?
  - Braucht es für bestimmte Fälle wirksame Einwilligungen der von der Datenverarbeitung Betroffenen, wenn keine andere Rechtsgrundlage greift? Ist die Verwaltung solcher Einwilligungen einschließlich möglicher Widersprüche sichergestellt?
  - Sind die gewünschten Funktionen der App-Software bzw. des Dienstes erforderlich, damit die Einrichtung ihre Aufgaben (besser) erfüllen kann?
  - Können die Datenschutzrechte der Betroffenen (§§ 16-25 DSG-EKD) auch mit dem Einsatz der App-Software sichergestellt werden?
- ☐ Liste, welche personenbezogenen Daten verarbeitet und gespeichert werden sollen?
  - Allgemeine Stammdaten und Kontaktdaten

[1] Für alle kirchlichen bzw. diakonischen Einrichtungen gelten die gesetzlichen Regelungen zum Datenschutz gemäß dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) und gemäß weiterer vorrangiger Rechtsvorschriften, welche die jeweilige kirchliche Stelle anzuwenden hat (z. B. § 35 SGB I und § 67 ff. SGB X). Die Datenschutz-Grundverordnung (DS-GVO) und das Bundesdatenschutzgesetz (BDSG) gelten nicht im kirchlichen bzw. diakonischen Bereich.

- Spezielle Informationen – Sorgeberechtigte; Abholberechtigte; Geschwister, die schon in der Kita waren
- Vertrauliche Informationen – hier speziell „besondere Kategorien personenbezogener Daten“ gemäß § 4 Ziff. 2 DSG-EKD, die da beispielsweise sind: Handicaps (Behinderungen); notwendige Medikationen; bekannte Verhaltensstörungen, ….
- Daten der Sorgeberechtigten
- Daten von Bevollmächtigten
- Informationen über Personen, die keinesfalls abholberechtigt sind
- Portfolio – Fotos, Berichte, gemalte Bilder von Kindern, …….

☐ Protokoll der Mitarbeitervertretung

- Sind die Rechte der Beschäftigten tangiert (§ 49 DSG-EKD)?

☐ Ergebnisbericht der Risiko-Vorabeinschätzung

- Besteht durch die Datenverarbeitung mit der App-Software voraussichtlich ein hohes Risiko für die Rechte der Betroffenen
- Ist eine Datenschutzfolgenabschätzung (DSFA) gemäß § 34 DSG-EKD nötig?
  - Die Frage ist zu bejahen, wenn mit der App-Software irgendwelche Daten von Minderjährigen oder besondere Kategorien von Daten wie Gesundheitsdaten (z. B. Krankmeldungen) verarbeitet werden
- Weitere Anhaltspunkte für die Notwendigkeit einer DSFA sind:
  - Systematische und umfassende Bewertung persönlicher Aspekte (z. B. mit einer Bildungs- und Entwicklungsdokumentation des Kindes) oder
  - Bestehen eines voraussichtlich hohen Risikos für die Rechte und Freiheiten natürlicher Personen oder umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten

☐ Ergebnisbericht der Risiko-/Sicherheitsanalyse

- Die Risiko-/Sicherheitsanalyse des Herstellers / Anbieters deckt nur den Bereich der App-Software bzw. des Online-Dienstes in allgemeiner Form ab
- Die Risiko-/Sicherheitsanalyse des KITA-Trägers berücksichtigt die Nutzung der App-Software bzw. des Online-Dienstes aus der Perspektive der datenschutzrechtlich verantwortlichen kirchlichen Stelle
- Risikoanalysen müssen den Ansatz- nach § 27 Abs. 1 DSG-EKD berücksichtigen. Eine Anleitung dazu bietet die Richtlinie zur Risikoanalyse des Kirchlichen Datenschutzmodells[2]
- Erforderliche technische Schutzmaßnahmen gelten als Anforderungen an die App-Software bzw. den Online-Dienst und sind wichtig für den Anbieter- und Produktvergleich

☐ Ergebnisbericht der Datenschutz-Folgenabschätzung

- Anforderungen siehe § 34 Abs. 4 DSG-EKD
- Das Kirchliche Datenschutzmodell unterstützt eine DSFA

[2] https://www.kirchliches-datenschutzmodell.de/wp-content/uploads/Richtlinie_Risikoanalyse-und-Risikobehandlung_KDM.pdf

  - Ggf. Einbeziehung des Datenschutzbeauftragten für Kirche und Diakonie (Aufsichtsbehörde) zum Zwecke der Beratung, wenn die DSFA ergibt, dass ein rechtskonformer Einsatz in der geplanten Form nicht möglich ist

- ☐ Aktualisiertes Verzeichnis der Verarbeitungstätigkeiten (VVT)
- ☐ Anforderungskatalog /-beschreibung für die App-Software
  - Funktionen
  - Dokumentation
  - Service Level Agreements
  - Sicherheit
  - Datenschutz
- ☐ Beschluss / Entscheidung
  - Vergleich verschiedener Anbieter
    - Technische Aspekte, wie z. B.:
      - Wie sollen Daten gespeichert werden? (lokal, in Netzwerk, in Cloud)
      - Wie arbeitet das Programm selbst? (lokal oder als WEB-Anwendung)
      - Wie erfolgen Datensicherungen und wer ist dafür verantwortlich?
      - Wer ist im laufenden Betrieb für die Administration des Programmes verantwortlich?
    - Gibt es eine unverbindliche Testinstallation/DEMO-Version?
      - Einbeziehung des betrieblichen Datenschutzbeauftragten in den Test
      - Ergebnisoffene Durchführung des Testes durch mehrere Mitarbeiter
      - Gibt es eine gute Dokumentation?
      - Wie ist das Handling? Welche Probleme wurden identifiziert?
      - Verifizierung der Ergebnisse
      - Nutzung der Möglichkeiten der Beratung
  - Fazit: Für welche Produkte kann bestätigt werden, dass sie die Anforderungen erfüllen und wie hoch ist der damit verbundene geschätzte Aufwand, einmalig und im laufenden Betrieb?

Vorliegen prüffähiger Unterlagen des App-Software Herstellers/Anbieters

Der Hersteller/Anbieter hat alle Informationen fortlaufend aktualisiert bereitzustellen, die es der kirchlichen Stelle erlauben, die Konformität der App-Software und Online-Dienste zu überprüfen. Solche Unterlagen sind regelmäßig die Folgenden:

- ☐ Kurzinformation
  - Überblick zur App-Software und den Online-Diensten
- ☐ Nutzerhandbuch
  - Zwingend erforderliche detaillierte Beschreibung zur Software- und Dienstnutzung als Schulungs- und Arbeitsgrundlage für die Nutzer
- ☐ Übersicht der Technisch-Organisatorischen Maßnahmen (TOM)
  - Insbesondere im Fall einer gehosteten Online-Dienstbereitstellung sind alle TOM für einen sicheren und datenschutzkonformen Betrieb zu benennen und zu erläutern (Verfügbarkeit, Belastbarkeit der Systeme, Vertraulichkeit, Intervenierbarkeit...)

- Zu den TOM gehören auch Funktionen, welche den Kunden (die kirchliche Stelle) dabei unterstützen, die Rechte von Betroffenen sicherzustellen (Recht auf Auskunft, auf Einschränkung der Verarbeitung, auf Löschung, auf Datenübertragung usw.)

☐ Datenschutzerklärung
- Datenschutzerklärung des Herstellers/Anbieters speziell für die Apps und Dienste

☐ Datenschutz-Folgenabschätzung
- Der App-Software und Dienstanbieter muss eine DSFA für die auf seinen Systemen durchgeführten Verarbeitungen durchführen und regelmäßig überprüfen. Das hohe Risiko ist bei Verarbeitung von Daten Minderjähriger und ggf. von Gesundheitsdaten, z.B. bei Verwaltung von Krankmeldungen grundsätzlich anzunehmen.

☐ Datenschutzkonzept
- Der Hersteller / Anbieter belegt mit Vorlage seines Datenschutzkonzepts die datenschutzrechtlich geforderte Zuverlässigkeit als Anbieter und Dienstleister

☐ Funktionsumfang
- Die regelmäßig zu aktualisierende Übersicht zum Funktionsumfang soll Kunden ermöglichen, frühzeitig zu erkennen, wenn Funktionsänderungen oder -erweiterungen neue datenschutzrechtliche Fragen aufwerfen

☐ Lizenz-/Nutzungsvertrag
- dieser Vertrag gibt Antwort zu den Fragen der eingeräumten Nutzungsrechte und der tatsächlichen Aufteilung der datenschutzrechtlichen Verantwortung (Auftragsverarbeitung aufgrund Handelns nur auf Weisung des Auftraggebers oder gemeinsame Verantwortung der Vertragspartner)

☐ Vereinbarung zur Auftragsdatenverarbeitung
- Vertragsinhalte gemäß § 30 Abs. 3 DSG-EKD oder, im Fall von Herstellern/Anbietern, die nicht dem kirchlichen Recht unterliegen auch nach Art. 28 DS-GVO möglich
- Vertragliche Sicherstellung der Kontrollrechte des Auftraggebers
- In jedem Fall aber: Zusatzerklärung zur Unterwerfung des Herstellers/Anbieters unter die kirchliche Datenschutzaufsicht gem. § 30 Abs. 5 S. 3 DSG-EKD (Download möglich auf www.dsbkd.de).

Die Unterlagen müssen versioniert und Änderungen an den Dokumenten nachvollziehbar sein. Der Zugriff für Kunden auf ältere Dokumentversionen muss in einem Archiv sichergestellt werden, wenn diese keine Möglichkeit haben, die Dokumente selbst zu archivieren.

Grundsätzliche Erwägungen und Hinweise des Datenschutzbeauftragten für den Datenschutz in Kirche und Diakonie, Aufsichtsbehörde gemäß § 39 ff. DSG-EKD

Der Einsatz einer unabhängig geprüften App-Software für die Kita-Verwaltung oder Teilaufgaben davon, einschließlich der Kommunikation unter den Beschäftigten als auch der Kommunikation mit externen Personen wie den Personensorgeberechtigten, ist zulässig, solange der für den Datenschutz verantwortlichen Stelle keine Anhaltspunkte bekannt sind oder werden, die einen datenschutzkonformen Einsatz erschweren oder unmöglich machen. Regelmäßige, mindestens jährliche Überprüfungen in Korrespondenz mit dem Hersteller, die Dokumentation und entsprechende Nachweise dazu hat die verantwortliche Stelle zu führen.

Unbeschadet davon ist die Zulässigkeit daran gebunden, dass von der verantwortlichen kirchlichen Stelle alle Datenschutzregeln gemäß dem kirchlichen Datenschutzrecht (DSG-EKD) eingehalten werden und der Verarbeitung der Daten von Minderjährigen und besonderer Kategorien von personenbezogenen Daten, wie z.B. Gesundheitsdaten, besondere Aufmerksamkeit gewidmet wird. Dazu gehören neben Rechtsgrundlage, Zweckbestimmung und der notwendigen Ergänzung dieser speziellen Verarbeitung mit der App im Verzeichnis der Verarbeitungstätigkeiten u. a. eine Aufbewahrungsrichtlinie, mit der genau bestimmt wird, ob und wie lange Daten in der App gespeichert sind und bleiben und wie die Löschung am Ende der Aufbewahrungsfrist zweifelsfrei ggf. durch Protokoll nachgewiesen wird. Zu nutzen sind entsprechende durch den Hersteller bereitgestellte Hilfsmittel oder Serviceleistungen.

Im Verzeichnis der Verarbeitungstätigkeiten sollen zur Beschreibung der konkreten Verarbeitungen mit der App auch alle Maßnahmen mit aufgeführt werden (ggf. durch ein Zusatzblatt), die von der verantwortlichen Stelle zusätzlich zu den vom Hersteller getroffenen Schutzmaßnahmen umgesetzt werden, um auf technische oder organisatorische Art und Weise sicherzustellen, dass die Grundsätze und Gewährleistungsziele des Datenschutzes gewahrt bleiben (rechtmäßig | legitim | verhältnismäßig | transparent | minimal | richtig | sicher).

Zu solchen erforderlichen Zusatzmaßnahmen gehört eine schriftliche Nutzungsrichtlinie, die alle mit der App-Nutzung betrauten Beschäftigten verständlich, vollständig und verbindlich (Arbeitsanweisung) über die Nutzung der App informiert. Darüber hinaus muss mittels geeigneter administrativer Steuerung sichergestellt sein, dass zu jedem Zeitpunkt ausschließlich dazu befugte Beschäftigte der verantwortlichen Stelle entsprechend ihrer Rolle einen Zugriff auf die App und die darin gespeicherten Daten haben.

Chemnitz im August 2022

Der Datenschutzbeauftragte für Kirche und Diakonie, Kirchliche Aufsichtsbehörde für den Datenschutz gemäß EKD-Datenschutzgesetz (DSG-EKD)