Abschlussbericht über die erste Schwerpunktprüfung des BfD EKD in Kindertageseinrichtungen

Einleitung

Im Sommer 2021 startete der BfD EKD in Erfüllung seiner gesetzlichen Aufgaben in seine erste Schwerpunktprüfung. Gemäß § 43 Abs. 1 DSG-EKD haben die Aufsichtsbehörden insbesondere die einheitliche **Anwendung und Durchsetzung des kirchlichen Datenschutzrechtes** in ihrem Zuständigkeitsbereich **zu überwachen und sicherzustellen**. Dazu gehören auch Prüfungen von kirchlichen und diakonischen Stellen. Auch die **Rechtsprechung des Europäischen Gerichtshofs (EuGH)** macht deutlich, dass die Aufsichtsbehörden ihre Aufgaben erst dann umfassend erfüllen, wenn nicht nur anlassbezogene, sondern auch anlasslose Prüfungen erfolgen. Zunächst stellte sich die Frage, wie **anlasslose Prüfungen** effektiv und unter der Berücksichtigung der personellen Ressourcen durchgeführt werden können. Es entstand die Idee, dass der BfD EKD zur Erfüllung seiner Aufgaben im aufsichtlichen Bereich zukünftig **Schwerpunktprüfungen** durchführt. Der BfD EKD versteht unter einer Schwerpunktprüfung eine anlasslose Prüfung **in einem (verfasst-)kirchlichen oder diakonischen Tätigkeitsfeld** mit dem Ziel der kontinuierlichen Verbesserung des Datenschutzes in den geprüften Einrichtungen. Im Ganzen ist es somit das Ziel der Schwerpunktprüfungen, den Datenschutz in den zu prüfenden Einrichtungen zu verbessern sowie die gesetzlichen Aufgaben im Rahmen der Vorgaben des EuGH zu erfüllen.

Für die erste Schwerpunktprüfung wurde der **Bereich der Kindertageseinrichtungen** ausgewählt. Es sollte eine relevante Anzahl von Kindertageseinrichtungen aus der Vielzahl von Einrichtungen, die unter das EKD-Datenschutzgesetz fallen, in einer überschaubaren Zeitspanne geprüft werden. Ausgewählt wurden daher EKD-weit **100 evangelische Kindertageseinrichtungen**. Die Schwerpunktprüfung wurde mit einem Online-Fragebogen durchgeführt und ggf. ergänzt durch die Vorlage von Dokumenten und die Durchführung von Vor-Ort-Terminen.

Ablauf der Schwerpunktprüfung

Zur Sicherstellung eines standardisierten Verfahrens und um eine belastbare Datenqualität zu erreichen wurde ein **Online-Fragebogen** verwendet.

Der Fragebogen wurde von einer internen Arbeitsgruppe erstellt und in zwei Einrichtungen **pilotiert,** um erste Erfahrungen zu sammeln. Während der Pilotierungen wurde bereits ein **Bewertungsmaßstab** entwickelt, der der späteren Auswertung der Antworten zugrunde lag, um eine einheitliche Qualität der Prüfungen zu gewährleisten.

Die Open Source Software „**Limesurvey**“ wurde ausgewählt, um den Online-Fragebogen zu realisieren. Die Umsetzung erfolgte mit einem Dienstleister in einem deutschen Rechenzentrum.

Nachdem die Anzahl der zu prüfenden Kindertageseinrichtungen pro Landeskirche entsprechend dem EKD-Verteilschlüssel festgelegt wurde, sind die zu prüfenden Kindertageseinrichtungen **innerhalb der Landeskirche zufällig ausgewählt** und postalisch informiert worden. Alle Kindertageseinrichtungen bekamen ihren **individuellen Zugangsschlüssel** zum Fragebogen mit einer Frist von

mehreren Wochen, um den Fragebogen zu beantworten. Zeitgleich wurden die Landeskirchen darüber informiert, welche Kindertageseinrichtungen in ihrem Bereich geprüft werden sollen. Auch der Fragebogen wurde zur Kenntnis gegeben.

Nach Ende der Frist und einer **Antwortquote von 80%** wurden die Einrichtungen, die den Fragebogen noch nicht ausgefüllt hatten, an die Abgabe erinnert. Einige wenige Kindertageseinrichtungen gaben auch in dieser Nachfrist den Fragebogen nicht ab, so dass der Träger angeschrieben und um Mithilfe gebeten wurde. In Einzelfällen kam es zu einer Vor-Ort-Prüfung durch die jeweils zuständige Außenstelle, da der Fragebogen nicht oder nicht vollständig ausgefüllt wurde. Pandemiebedingt wurden die Vor-Ort-Prüfungen per Videokonferenz durchgeführt.

Am Hauptsitz wurden zunächst alle Fragebögen mit Hilfe eines **Ampelsystems** summarisch geprüft. Über die Hälfte der Einrichtungen wurde im Ampelsystem bei der ersten Prüfung als „grün“ kategorisiert, da auf den ersten Blick keine offensichtlichen Datenschutzmängel erkennbar waren. Bei den „gelben“ und „roten“ Fragebögen wurde vorgeschlagen, Dokumente zur tieferen Prüfung des Datenschutzniveaus in den Einrichtungen anzufordern. Auch Rückfragen zu den Antworten aus den Fragebögen waren für die abschließende Prüfung teilweise erforderlich.

Zu diesem Zeitpunkt wurde der **Zwischenbericht** zur ersten Schwerpunktprüfung des BfD EKD auf der Internetseite veröffentlicht.

Die Anforderung der Dokumente und die abschließende Prüfung erfolgten in den jeweils zuständigen Außenstellen und endeten mit entsprechenden **Abschlussschreiben** an die geprüften Kindertageseinrichtungen. Diese Schreiben zeigten die Ergebnisse sowie die erkennbar gewordenen Mängel auf und gaben den Einrichtungen konkret umzusetzende Anforderungen und Empfehlungen an die Hand.

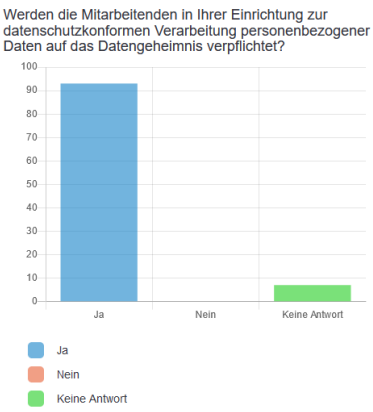
Mit der Erstellung und Veröffentlichung dieses **Abschlussberichts** endet die erste Schwerpunktprüfung des BfD EKD.

Ergebnisse der Schwerpunktprüfung

Der **Fragebogen** umfasst **30 Fragen**. Neben allgemeinen Angaben wurden Fragen zum rechtlichen und organisatorischen Umfeld sowie zum technischen Umfeld gestellt. Dabei waren überwiegend mehrere Antwortmöglichkeiten vorgegeben. Einige wenige Fragen enthielten Freitextfelder. Die meisten Fragen stammen aus dem technischen Bereich.

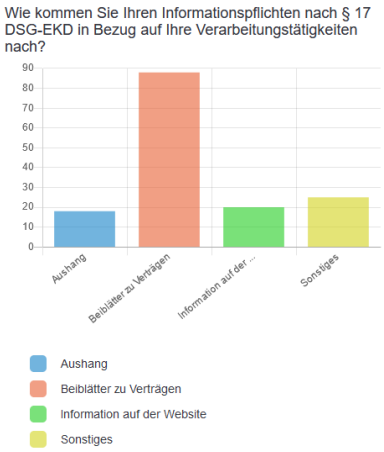
Fragen aus dem rechtlichen und organisatorischen Umfeld

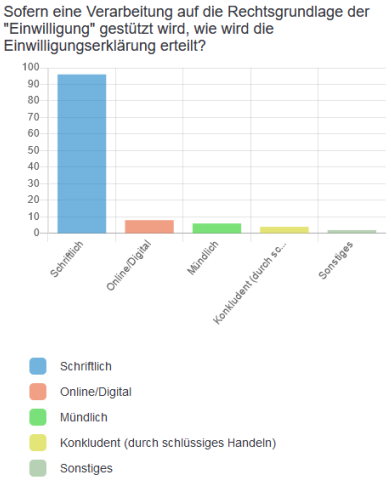
Die Auswertung der Fragen aus diesem Bereich ergab, dass in den meisten Kindertageseinrichtungen bereits ein **Bewusstsein** für die datenschutzrechtlichen Anforderungen durchaus **vorhanden** ist.



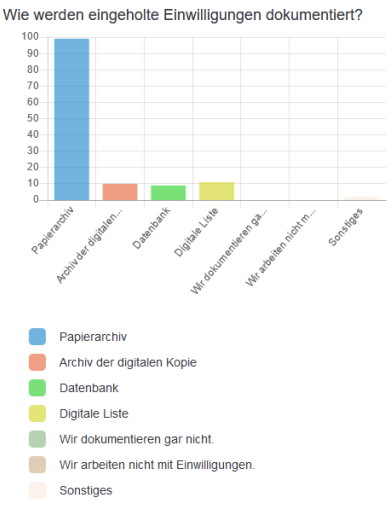
Die rechtliche Verpflichtung, **eine oder einen örtlich Beauftragte(n) für den Datenschutz** gem. § 36 Abs. 1 DSG-EKD zu bestellen, wird weitestgehend erfüllt. Die Verpflichtung auf das **Datengeheimnis** gem. § 26 DSG-EKD geschieht sogar nahezu flächendeckend. Ebenso erfreulich ist die Erkenntnis, dass in mehr als der Hälfte der Einrichtungen die **Informationspflichten** gem. § 17 DSG-EKD aktiv, also nicht erst auf Verlangen, erfüllt werden. Überwiegend geschieht dies durch Beiblätter zu den Verträgen. Auch auf den Internetseiten werden diese Informationen teilweise zur Verfügung gestellt.

Gefragt wurde auch nach der (regelmäßigen) **Sensibilisierung** der Mitarbeitenden. Hier stellte sich heraus, dass zwar bei der Einarbeitung einer oder eines neuen Mitarbeitenden recht häufig eine Sensibilisierung stattfindet, eine regelmäßige Auffrischung aber meistens unterbleibt. Nur durch eine wiederkehrende Sensibilisierung auf den Datenschutz wird jedoch erst ein Bewusstsein für dieses Thema gefestigt. Dieses Bewusstsein ist letztlich nötig für ein gutes Datenschutzniveau in einer Einrichtung. Oftmals entstehen Datenpannen durch menschliches Fehlverhalten. Ein gutes Bewusstsein für die datenschutzrechtlichen Probleme kann helfen, diese Fehler zu reduzieren. Wir raten daher, regelmäßige Schulungseinheiten in jeder Einrichtung zu etablieren.





Wie von uns empfohlen werden **Einwilligungen** in Datenverarbeitungen in der Regel schriftlich eingeholt. In den wenigen Fällen, in denen auf konkludente Einwilligungserklärungen gesetzt wird, wurde die dringende Empfehlung ausgesprochen, aus Gründen der Rechtssicherheit und des Nachweises der Rechenschaftspflichten aus § 5 Abs. 2 DSG-EKD künftig von diesem Vorgehen abzusehen und schriftliche Einwilligungserklärungen einzuholen. Bei der Erstellung einer Einwilligungserklärung sind immer die Voraussetzungen aus § 11 DSG-EKD einzuhalten. Die **Aufbewahrung** der Einwilligungserklärungen erfolgt in den allermeisten Fällen in **Papierform**. Schon an dieser Stelle wurde deutlich, dass in den meisten Kindertageseinrichtungen keine umfassende IT-Infrastruktur vorhanden ist. Eine Datenlöschung erfolgt richtigerweise zwar oft nach Zweckerfüllung. Ein eigenständiges und verschriftlichtes **Löschkonzept** existiert jedoch leider nur in wenigen Kindertageseinrichtungen. Das Löschkonzept sollte Teil des Datenschutzkonzepts sein.



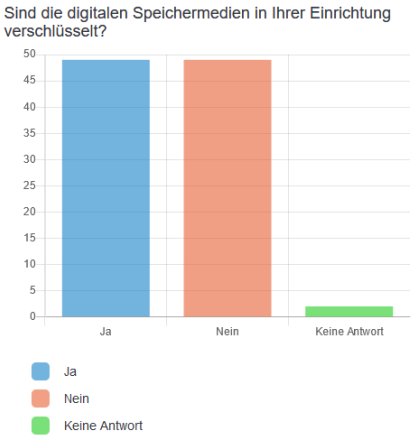
Eine weitere Frage drehte sich um den Umgang mit **Datenpannen**. Dabei fiel auf, dass in vielen Kindertageseinrichtungen die Prozesse für den Umgang mit Datenpannen nicht oder nur ungenügend etabliert sind bzw. umgesetzt werden. Nur in der Hälfte der Einrichtungen findet eine **interne Dokumentation** statt. Diese ist jedoch nach § 32 Abs. 5 DSG-EKD rechtlich verpflichtend und muss ggf. der Aufsichtsbehörde zur Überprüfung der Einhaltung der Bestimmungen aus § 32 DSG-EKD zur Verfügung gestellt werden. Auch ist diese interne Dokumentation eine Vorbereitung zur **Meldung** der Datenpanne **an die zuständige Aufsichtsbehörde**. Hier ergab die Auswertung der Fragebögen, dass eine Meldung der Datenpannen zwar in Teilen an die oder den örtlich Beauftragten für den Datenschutz oder an den Träger erfolgt, jedoch häufig keine direkte Meldung an die Aufsichtsbehörde erfolgt. Es empfiehlt sich zum einen **klare Prozesse** zum Umgang mit Datenpannen zu definieren und zum anderen dieses Thema im Rahmen einer Sensibilisierungsmaßnahme

aufzugreifen und regelmäßig zu wiederholen. Wichtig ist, dass Datenpannen als solche erkannt werden und dann die notwendigen Schritte eingeleitet werden. Dazu gehört auch die Überprüfung der Notwendigkeit einer **Benachrichtigung** an die betroffene Person gem. § 33 DSG-EKD.

Fragen aus dem technischen Umfeld

Im Blick auf die IT-Infrastruktur in den Kindertageseinrichtungen hat sich gezeigt, dass die meisten Einrichtungen eine sehr **einfache technische Struktur** aufweisen. Davon gibt es einige Ausnahmen, wenn die Kindertageseinrichtung die IT strukturiert und professionell z.B. über ihren Träger bezieht. Eine „typische Kindertageseinrichtung" hat meistens nur einen Laptop für die Leitung und darüber hinaus noch wenige Endgeräte für die Gruppen und die Mitarbeitenden.

In dem technischen Teil des Fragebogens wurde die grundlegende IT-Infrastruktur der Kindertageseinrichtungen abgefragt, wobei in einer Vielzahl der Einrichtungen ein „IT-Mangel" (schlechte Aufbewahrung, private Endgeräte ohne konkrete Regelung, Gruppenaccounts, keine Passwort-Richtlinie, kein Virenscanner, keine Verschlüsselung, veraltete Betriebssysteme) festgestellt wurde. Erfreulicherweise werden nur vereinzelt veraltete Betriebssysteme eingesetzt. Die Einrichtungen, die bisher keine **aktuellen Betriebssysteme** einsetzen, wurden entsprechend darauf hingewiesen die Systeme auf einen aktuellen Stand zu bringen.



Bei der **Aufbewahrung** von mobilen Endgeräten wurden in einigen der geprüften Einrichtungen Defizite festgestellt. Gerade wegen der Einbruchsgefahr und der Sensibilität der Daten ist die Verwahrung der (mobilen) Endgeräte außerhalb der Dienstzeiten in abgeschlossenen (Stahl)Schränken anzustreben. Im Blick auf die Einbrüche in Kindertageseinrichtungen muss auch jedes Endgerät standardmäßig **verschlüsselt** werden. Dies ist mit den „Bordmitteln" der gängigen Betriebssysteme in der Regel auch ohne weitere Kosten möglich. Die Hälfte der Einrichtungen hat angegeben ihre Endgeräte zu verschlüsseln. Die übrigen Einrichtungen haben einen entsprechenden Hinweis im Abschlussschreiben bekommen.

Die Nutzung von **privaten Endgeräten für dienstliche Zwecke** ist sehr kritisch zu sehen, da personenbezogene Daten der Kinder oder der Eltern auf privaten Endgeräten sehr schlecht kontrolliert werden können und auch das Risiko des Missbrauchs oder des Verlusts sehr hoch ist. Bei der Auswertung der Frage, ob private Endgeräte für dienstliche Zwecke verwendet werden, und der Prüfung der entsprechend geltenden Regelungen stellte sich heraus, dass aber nur in wenigen Einrichtungen private Endgeräte ohne entsprechende Regelungen verwendet werden. Der Einsatz beschränkt sich dann in der Regel nur auf Notfälle bei Ausflügen oder ähnlichen Situationen.

Die Benutzung von **Gruppenaccounts** für die Mitarbeitenden ist ein wichtiges Thema. Aus Gründen der Transparenz, der Datentrennung und der Nachvollziehbarkeit sollten alle Mitarbeitenden individuelle Accounts besitzen. Ungefähr ein Drittel der Einrichtungen gaben an auch Gruppenaccounts zu benutzen. Diesen Einrichtungen wurde geraten zu individuellen Accounts zu wechseln. Allerdings muss erwähnt werden, dass es einige Hersteller von Tablets gar nicht ermöglichen individuelle Accounts zu erstellen. Sobald aber personenbezogene Daten mit einem Endgerät verarbeitet werden, sind individuelle Accounts zwingend. Weiterhin gibt es in knapp der Hälfte der Einrichtungen keine **Passwortrichtlinie**. Aufgrund der oft einfachen IT-Infrastruktur ist es nicht immer möglich dies technisch zu erzwingen. Jedoch sollten mindestens über eine organisatorische Maßnahme Vorgaben für die Mitarbeitenden gemacht werden.

Nur einzelne Einrichtungen haben angegeben, keinen **Virenschutz** einzusetzen. Aufgrund der Tatsache, dass bei den aktuellen Betriebssystemen von Microsoft, welche überwiegend eingesetzt werden, bereits nach der Installation der mitgelieferte Antivirus läuft, ist anzunehmen, dass die Quote eigentlich noch geringer ist.

Im Zuge der Bearbeitung der Fragebögen wurden auch die **Datenschutzerklärungen** auf den Internetseiten der Einrichtungen wahrgenommen. Die Kindertageseinrichtungen haben oft nur eine Unterseite auf der Internetseite ihres Trägers und nur gelegentlich auch eigene Auftritte. Dabei ist aufgefallen, dass die Datenschutzerklärungen oft unzureichend sind. Sie beziehen sich z.B. fälschlicherweise auf die Datenschutzgrundverordnung oder beschreiben Verarbeitungen, welche gar nicht durchgeführt werden oder haben andere Mängel. Hier besteht Handlungsbedarf.

Zusammenfassung

Die Prüfung hat gezeigt, dass es sowohl im rechtlichen und organisatorischen Bereich als auch im technischen Umfeld zum Teil noch Verbesserungsbedarf beim Datenschutz gibt. Die Prüfung hat aber ebenfalls aufgezeigt, dass es in den allermeisten Kindertageseinrichtungen **keine strukturellen Defizite** gibt und eine gewisse **Sensibilität für datenschutzrechtliche Fragen** vorhanden ist. Festzuhalten bleibt, dass ein gutes Datenschutzniveau nur über die kontinuierliche Weiterarbeit an den Themen etabliert werden kann. Es müssen Prozesse geschaffen, gelebt und weiterentwickelt werden. Bei den einrichtungsübergreifend relevanten Themen ist es mit Sicherheit von Vorteil Synergieeffekte zu nutzen und gemeinsame Vorgehensweisen oder Formulare einzuführen. Die **Muster und Handreichungen** des BfD EKD sollten genutzt werden.

Der Fragebogen enthielt den Hinweis, dass die Leitungen der Kindertageseinrichtungen bei der Beantwortung der Fragen aus dem Fragebogen die oder den zuständigen örtlich Beauftragte(n) für den Datenschutz und ggf. eine oder einen IT-Verantwortlichen beteiligen sollten. Diese Zusammenarbeit hätte nach unserem Eindruck gezielter und häufiger stattfinden können und in manchen Fällen möglicherweise zu besser auswertbaren Antworten geführt.

Abschließend möchten wir an dieser Stelle den geprüften Kindertageseinrichtungen für Ihre Kooperationsbereitschaft und die gute Zusammenarbeit danken. Ebenfalls möchten wir uns bei den Landeskirchen und den Diakonischen Landesverbänden bedanken, die das gesamte Verfahren begleitet und unterstützt haben.

Ausblick

Die nächste Schwerpunktprüfung wird im Bereich der **evangelischen Krankenhäuser** stattfinden. Genauere Informationen zum Ablauf und zum Zeithorizont der Prüfung werden zu gegebener Zeit den Diakonischen Landesverbänden mitgeteilt.

Hannover im September 2022