# Fragestellungen der Querschnittsprüfung „Datenschutz in Kindertageseinrichtungen“

Im Folgenden werden die im Rahmen der Querschnittsprüfung gestellten Fragen aus den unterschiedlichen Bereichen des technischen und organisatorischen Datenschutzes dargestellt. Teilweise wurde den Einrichtungen eine Auswahl an mehreren möglichen Antworten angeboten. Auszugsweise sind diese unter einigen Frage mit aufgeführt.

Generell war gefordert, nur aktuelle Informationen anzugeben und bei verwendeten Techniken oder Maßnahmen nur solche zu benennen, die zum Zeitpunkt der Befragung in Betrieb bzw. Verwendung waren. Geplante oder sich im Aufbau oder Umsetzung befindliche Maßnahmen durften nicht genannt werden.

## Bereich „Allgemeine Infos“

| | |
|---|---|
| 1 | Wie lautet die genaue Bezeichnung der Einrichtung? Bitte - wenn nötig - ergänzen oder korrigieren! |
| 2 | Geben Sie bitte - falls vorhanden - die Homepage der Einrichtung an. |
| 3 | Zu welchem (Erz-)Bistum gehört die Einrichtung? |
| 4 | Wer steht als Ansprechpartner für Rückfragen zur Verfügung? |
| 5 | Welche Organisation ist Träger der Kindertageseinrichtung? Bitte - wenn nötig - ergänzen oder korrigieren! |
| 6 | Wie viele Mitarbeiter hat die Einrichtung? Bitte geben Sie die Zahl aller mitarbeitenden Personen inklusive Ehrenamtlicher, BufDi, FSJ, Praktikanten usw., an. |
| 7 | Wie viele Kinder werden in der Einrichtung betreut? |
| 8 | Werden Kinder im Rahmen von Inklusionsmaßnahmen betreut? |
| 9 | Wo liegt die Einrichtung? |

## Bereich „Betrieblicher DSB“

| | |
|---|---|
| 1 | Wurde für Ihre Einrichtung ein betrieblicher Datenschutzbeauftragter benannt?<br>*Wenn Antwort verneint wurde:*<br>➢ Warum wurde kein betrieblicher Datenschutzbeauftragter benannt? |
| 2 | Bitte geben Sie die dienstlichen Kontaktdaten des betrieblichen Datenschutzbeauftragten an. |
| 3 | Wurde der betriebliche Datenschutzbeauftragte der zuständigen Datenschutzaufsicht gemeldet? |

| | |
|---|---|
| 4 | Art des betrieblichen Datenschutzbeauftragten. *(intern oder extern)*<br>*Wenn bei Art des bDSB „extern" angegeben wurde:*<br>➢ Wie hoch ist das für Ihre Einrichtung vorgesehene monatliche Kontingent bei dem externen betrieblichen Datenschutzbeauftragten?<br>*Wenn bei Art des bDSB „intern" angegeben wurde:*<br>➢ Wie hoch ist der durch den Verantwortlichen festgelegte Anteil der Stelle des betrieblichen Datenschutzbeauftragten zur Wahrnehmung seiner Aufgaben (gemessen an einer Vollzeitstelle)? |
| 5 | Welche Aufgaben übernimmt Ihr betrieblicher Datenschutzbeauftragter? |

## Bereich „Datensicherung"

| | |
|---|---|
| 1 | Wie viele Endgeräte haben Sie in Betrieb? Um die Erfüllung datenschutzrechtlicher Anforderungen in Bezug auf Endgeräte wie Desktop-PCs, Laptops, Smartphones usw. nachweisen zu können (z.B. Zugangskontrolle und Patchmanagement), ist es zunächst erforderlich, diese aufzulisten. |
| 2 | Welche Speichermedien nutzen Sie im Alltagsbetrieb für die Speicherung personenbezogener Daten? Die Art der Speichermedien kann Einfluss auf die zu treffenden Maßnahmen zum Schutz dieser Medien (z.B. Aufbewahrung) haben. |
| 3 | Führen Sie regelmäßig Datensicherungen durch?<br>*Wenn Antwort verneint wurde:*<br>➢ Warum führen Sie keine Datensicherung durch?<br>*Wenn Antwort bejaht wurde:*<br>➢ Wie oft führen Sie Datensicherungen durch? |
| 4 | Auf welchen Speichermedien werden Ihre Datensicherungen gespeichert? Die Art der Speichermedien kann Einfluss auf die zu treffenden Maßnahmen zum Schutz dieser Medien (z.B. Lagerung) haben. |

## Bereich „Virenscanner"

| | |
|---|---|
| 1 | Setzen Sie Virenscanner ein? |
| 2 | Wie oft wird der Virenscanner aktualisiert? |
| 3 | Welche(n) Virenscanner setzen Sie ein? |

## Bereich „Datenspeicher"

| | |
|---|---|
| 1 | Wie viele externe/mobile Datenspeicher nutzen Sie? |
| 2 | Wo und wie werden die Endgeräte und die externen Datenspeicher aufbewahrt, wenn diese nicht benutzt oder beaufsichtigt werden (insb. außerhalb der Dienstzeiten)? |
| 3 | Nutzen Sie einen Server (intern oder extern) als zentrales System (z.B. zur Datenspeicherung oder für Anwendungen)? Werden z.B. Daten zentral auf einem Server gespeichert oder sind diese auf die eingesetzten Geräte „verteilt"?<br>*Wenn Antwort bejaht wurde:*<br>➢ Durch wen wird der Server betrieben?<br>➢ Durch wen wird der Server gewartet? |

## Bereich „Zugangsschutz“

| | |
|---|---|
| 1 | Wie ist der Zugang zu den Betriebssystemen geschützt? *(Mehrfachauswahl)*<br>○ Individueller Account mit individuellem Passwort<br>○ Gruppenaccount mit Gruppenpasswort<br>○ Kein Passwort<br>○ Sonstiges |
| 2 | Gibt es eine systemseitige Automatik für die Änderung der Passwörter für den Zugang zum Betriebssystem? |
| 3 | Wie oft wird das Passwort geändert? |

## Bereich „Verzeichnis von Verarbeitungstätigkeiten“

| | |
|---|---|
| 1 | Ist für Ihre Einrichtung ein Verzeichnis von Verarbeitungstätigkeiten vorhanden? |
| 2 | Wie stellen Sie die Aktualität des Verzeichnisses sicher? |
| 3 | Wer führt das Verzeichnis von Verarbeitungstätigkeiten |
| 4 | Sofern eine Verarbeitung auf die Rechtsgrundlage der "Einwilligung" gestützt wird, wie wird die Einwilligungserklärung erteilt? |
| 5 | Wie werden eingeholte Einwilligungen dokumentiert? |

## Bereich „Informationspflicht“

| | |
|---|---|
| 1 | Wie kommen Sie Ihren Informationspflichten in Bezug auf Ihre Verarbeitungstätigkeiten nach? |
| 2 | Sind die Mitarbeiter zur datenschutzkonformen Verarbeitung personenbezogener Daten in Ihrem Arbeitsbereich sensibilisiert, geschult und verpflichtet worden?<br>*Wenn Frage bejaht wurde:*<br>➢ Zu welchem Zeitpunkt führen Sie die Verpflichtung durch? |
| 3 | Wie oft werden die Mitarbeiter auf die Verarbeitung von personenbezogenen Daten hin sensibilisiert/geschult? |

## Bereich „Datenschutzverletzungen“

| | |
|---|---|
| 1 | Wenn bei uns Datenschutzverletzungen festgestellt werden, (unter Datenschutzverletzungen im Sinne dieser Frage sind sämtliche "Datenpannen, z.B. Versand von Unterlagen an den falschen Empfänger, Veröffentlichung vertrauenswürdiger Informationen, Veröffentlichung von Fotos ohne Einwilligung, Schadsoftwarebefall mit nachfolgendem Verlust personenbezogener Daten, etc. zu verstehen, unabhängig von einer Meldepflicht an die Datenschutzaufsicht: *(Mehrfachauswahl)*<br>○ Führen wir ein internes Verfahren zur Erfassung und Bewertung durch.<br>○ Nehmen wir eine interne Dokumentation vor.<br>○ Melden wir den Vorfall an den Träger.<br>○ Melden wir den Vorfall an den betrieblichen Datenschutzbeauftragten.<br>○ Melden wir den Vorfall bei der Datenschutzaufsicht.<br>○ Findet keine Dokumentation statt. |

## Bereich „Private Endgeräte“

| | |
|---|---|
| 1 | Benutzen Mitarbeiter private Endgeräte zu dienstlichen Zwecken? |
| 2 | Welche Regelungen haben Sie zur Nutzung von privaten Endgeräten zu dienstlichen Zwecken getroffen? Regelungen könnten z.B. in Form von Dienstanweisungen oder Dienstvereinbarungen bestehen. Bitte fassen Sie den Inhalt eventueller Bestimmungen/Vereinbarungen stichwortartig zusammen. |

## Bereich „Löschen von Daten“

| | |
|---|---|
| 1 | Haben Sie für alle Datenarten festgelegt, wie lange diese aufbewahrt werden müssen (gesetzliche oder betriebliche Gründe)? |
| 2 | Haben Sie Regeln und Verfahren, wie Sie mit zu löschenden Daten umgehen? Daten sind zu löschen, wenn ihre Verarbeitung durch den Fristablauf der Zweckbestimmung nicht mehr rechtmäßig ist. |
| 3 | Existiert ein Löschkonzept, das auch das Löschen aus dem Langzeitregister (internes Archiv) und von Datensicherungen regelt? |
| 4 | Wie stellen Sie sicher, dass auf ausgemusterten Endgeräten keine personenbezogenen Daten mehr gespeichert sind? |

## Bereich „Datensicherheit“

| | |
|---|---|
| 1 | Sind alle Festplatten (interne und externe) Ihrer Einrichtung verschlüsselt?<br>*Wenn Frage verneint wurde:*<br>➢ Warum sind die digitalen Datenträger mit personenbezogenen Daten nicht verschlüsselt?<br>*Wenn Frage bejaht wurde:*<br>➢ Mit welcher Software führen Sie die Festplattenverschlüsselung durch? |

| | |
|---|---|
| 2 | Sind alle weiteren digitalen Datenträger (z.B. USB-Sticks, SD-Karten) mit personenbezogenen Daten verschlüsselt?<br>*Wenn Frage vereint wurde:*<br>➢ Warum sind die digitalen Datenträger mit personenbezogenen Daten nicht verschlüsselt? |
| 3 | Kopieren Sie personenbezogene Daten auf externe Datenspeicher (Festplatten, USB Sticks, SD-Karten)? |

## Bereich „Technische und Organisatorische Maßnahmen“

| | |
|---|---|
| 1 | Welche Vorkehrungen sind zur Zutrittskontrolle zum Gebäude getroffen? Hierunter versteht man Maßnahmen, die den Zutritt zu den Räumlichkeiten der Datenverarbeitung beschränken und kontrollieren. *(Mehrfachauswahl)*<br>○ Einbruchmeldeanlage.<br>○ Regelung zur Information über einen Einbruchalarm ("Alarmkette").<br>○ Zentrales Schließsystem.<br>○ Sicherheitsschlösser.<br>○ Chipkarten/Transpondersysteme.<br>○ Zentrale Schlüsselausgabe und -verwaltung.<br>○ Gesicherte Aufbewahrung überzähliger Schlüssel.<br>○ Dokumentation der Schlüsselausgabe (z.B. Schlüsselbuch oder Empfangsquittungen).<br>○ Unterschiedliche Zutrittsbereiche (Gruppenräume, Büro der Leitung, Verwaltung etc.).<br>○ Vergabe nur der nötigen Zutrittsberechtigungen.<br>○ Regelmäßige Überprüfung der vergebenen Zutrittsberechtigungen (z.B. turnusmäßig zu Beginn des Kita-Jahres).<br>○ Gelegentliche Überprüfung der vergebenen Zutrittsberechtigungen (z.B. bei Neueinstellung/Ausscheiden von Mitarbeitenden).<br>○ Besucherregelung für sensible Bereiche (z.B. Büro der Einrichtungsleitung).<br>○ Türen mit Knauf auf der Außenseite (nur von innen oder mit Schlüssel zu öffnen).<br>○ Keine dieser Maßnahmen.<br>○ Sonstige Maßnahmen. |

| | |
|---|---|
| 2 | Welche Vorkehrungen sind zur Zugangskontrolle zu den Rechnern/Endgeräten (Anmeldung) bzw. zur Zugriffskontrolle auf die Anwendungsdaten (Berechtigungen) getroffen? Dies sind Maßnahmen, die auf der zweiten Stufe den Zugang zu Datenverarbeitungssystemen verhindern, nachdem die erste Stufe der Zutrittskontrolle überwunden wurde, sowie Maßnahmen, die Nutzern den Zugriff auf oder die Löschung von bestimmten Daten erlauben. *(Mehrfachauswahl)*<br>○ Login mit Nutzername + Passwort.<br>○ Login mit biometrischen Daten (z.B. Fingerabdruckscanner).<br>○ Definierter Ablauf für die Einrichtung/das Löschen von Nutzern und die Vergabe/den Entzug von Berechtigungen (z.B. "Laufzettel" bei Einstellung/Ausscheiden eines Mitarbeitenden).<br>○ Zentrale Nutzerverwaltung (Einrichtung und Löschung von Nutzern, Vergabe und Entzug von Rechten).<br>○ Rollenbasiertes Berechtigungskonzept.<br>○ Dokumentation vergebener Berechtigungen.<br>○ Gelegentliche Überprüfung der vergebenen Zugangs- und Zugriffsberechtigungen (z.B. bei Neueinstellung/Ausscheiden von Mitarbeitenden).<br>○ Regelmäßige Überprüfung der vergebenen Zugangs-/Zugriffsberechtigungen (z.B. turnusmäßig zum Beginn des Kita-Jahres).<br>○ Einhaltung des Prinzips der minimalen Rechtevergabe.<br>○ Sparsame Verwendung administrativer Rechte.<br>○ Nutzer können sich bei Abwesenheit gegenseitig vertreten.<br>○ Passwortrichtlinie (Passwortkomplexität, z.B. Verwendung von Klein- und Großbuchstaben, Ziffern und Sonderzeichen).<br>○ Passwortrichtlinie gilt auch für die Anmeldung an Anwendungen (z.B. KiTa Verwaltung).<br>○ Automatische Bildschirmsperre.<br>○ Es ist ein Mechanismus etabliert, der das Durchprobieren von Passwörtern unterbindet (Brute-Force-Schutz, z.B. Beschränkung der Anzahl erfolgloser Anmeldeversuche).<br>○ Sperre/Deaktivierung externer Schnittstellen.<br>○ Boot-Schutz (Sicherung gegen Booten des Rechners von CD oder USB-Stick).<br>○ Fernzugänge sind abgesichert.<br>○ Dienstleister müssen für einen Remote-Zugriff freigeschaltet werden und Tätigkeiten können verfolgt werden.<br>○ Regelungen zum Umgang mit (dienstlichen) mobilen Geräten (Mobile Device Policy).<br>○ Mobilgeräte (Smartphones, Tabletts) können bei Verlust aus der Ferne gelöscht werden (Mobile Device Management).<br>○ Separate Firewall.<br>○ Private USB-Sticks dürfen nicht genutzt werden.<br>○ Es gibt eine Testumgebung für neue Anwendungen und Funktionen.<br>○ Keine der genannten Maßnahmen.<br>○ Sonstige Maßnahmen. |
| 3 | Wie wird die Weitergabe von Daten kontrolliert? Gemeint sind Maßnahmen, die die Integrität und Vertraulichkeit personenbezogener Daten sowohl bei elektronischen Übermittlungsvorgängen als auch beim Transport der Datenträger sicherstellen. |
| 4 | Wird die Tätigkeit von Auftragsverarbeitern kontrolliert? |

| | |
|---|---|
| 5 | Wie kontrollieren Sie die Eingabe und das Löschen von personenbezogenen Daten? Dies sind Maßnahmen, die nachträgliche Feststellungen ermöglichen, ob und durch wen personenbezogene Daten in Verarbeitungssysteme eingegeben, verändert oder entfernt worden sind. *(Mehrfachauswahl)*<br>o Protokollierung von Eingaben personenbezogener Daten.<br>o Protokollierung des Löschens personenbezogener Daten.<br>o Vorhalten der Protokolle für mindestens sechs Monate.<br>o Klare Zuständigkeit für Löschungen.<br>o Keine der genannten Maßnahmen.<br>o Sonstige Maßnahmen. |
| 6 | Wie werden die permanente Verfügbarkeit bzw. die Wiederherstellung der Daten sichergestellt? Gemeint sind Maßnahmen zur Verhinderung eines ungewollten Datenverlustes sowie zur Wiederherstellung von Daten. *(Mehrfachauswahl)*<br>o Speicherung erfolgt auf zentralen Systemen.<br>o Backup- und Recovery-Konzept vorhanden.<br>o Backup- und Recovery-Konzept vorhanden und erprobt.<br>o Existenz eines Notfallplans.<br>o Patches und Sicherheitsupdates werden regelmäßig eingespielt.<br>o Externe Lagerung von Datensicherungen.<br>o Feuersichere Lagerung von Datensicherungen in der Einrichtung.<br>o Feuer- und Rauchmeldeanlage vorhanden.<br>o Keine der genannten Maßnahmen.<br>o Sonstige Maßnahmen. |