Richtlinie zur Risikoanalyse und Risikobehandlung im Rahmen des Kirchlichen Datenschutzmodells (KDM)

1 Grundsätzliches:

Für jede Verarbeitungstätigkeit (Verfahren) ist eine Übersicht über mögliche Risiken und deren Bewertung (Risikoanalyse) zu erstellen und es sind geeignete Maßnahmen zur Risikobehandlung zu treffen.

Gemäß der Grundrechtecharta der EU ist der Schutz personenbezogener Daten ein Grundrecht, und folglich birgt jede Verarbeitung personenbezogener Daten für sich bereits die Gefahr eines Grundrechtseingriffs, der nur erlaubt ist, wenn es dafür eine rechtliche Grundlage gibt. Das KDM ist auf dieses Faktum gestützt. Die Verarbeitungstätigkeit muss daher zum einen rechtlich legitimiert, zum anderen so gestaltet sein, dass der Grundrechtseingriff möglichst minimal ausfällt. Risiken für die Rechte und Freiheiten natürlicher Personen können ihren Ursprung dabei in der Ausgestaltung der Verarbeitungstätigkeit selbst oder aber in Gefährdungen aus dem Bereich der IT-Sicherheit sowie dem organisatorischen Umfeld haben.

2 Begriffe und deren Bedeutung:

Gewährleistungsziel:	zentrales Element des KDM, abgeleitet aus den Grundsätzen und Schutzzielen und weiteren rechtlichen Anforderungen in den kirchlichen Datenschutzgesetzen.
Bedrohung:	Ereignisse, welche das Einhalten der Gewährleistungsziele gefährden können. Genutzt werden kann z.B. der Gefährdungskatalog der ISO 29134 mit 11 Bedrohungen oder eine Auswahl der elementaren Gefährdungen aus dem IT-Grundschutz.
Schadensereignis:	Eintritt eines Ereignisses, das zu einer Verletzung der Gewährleistungsziele führt.
Schadenshöhe:	Höhe des Schadens für den Betroffenen durch ein Schadensereignis, bezogen auf die Verletzung eines Gewährleistungszieles.
Schutzbedarf:	Der Schutzbedarf einer natürlichen Person bei der Verarbeitung personenbezogener Daten in Bezug auf ihre Rechte und Freiheiten ergibt sich aus dem potentiellen Schaden, der von der Verarbeitungstätigkeit und deren Eingriffsintensität ausgeht. Es wird zwischen normalem und hohem Schutzbedarf unterschieden.
Eintritts-wahrscheinlichkeit:	Einstufung für die Häufigkeit des Eintretens einer Bedrohung, die zur Verletzung eines Gewährleistungsziels führt.

Risiko	Möglichkeit des Eintritts eines Ereignisses, das einen Schaden für die Freiheiten und Rechte betroffener Personen (und damit die Verletzung eines Gewährleistungsziels) darstellt oder zu einem solchen für eine oder mehrere natürliche Personen führen kann. Das Risiko hat zwei Dimensionen: Schadenshöhe und Eintrittswahrscheinlichkeit

3 Vorgehensmodell:

3.1 Vorbereitung der Risikoanalyse

Benennung / Identifikation des zu bewertenden Verfahrens sowie Zweckbestimmung

Beispiel: *Bildungsdokumentation in der Kindertageseinrichtung*
Zweck: Erfüllung der gesetzlichen Vorschrift zur Dokumentation der persönlichen Entwicklung des Kindes über die gesamte Betreuungsdauer.

Diese und weitere Angaben können in der Regel aus dem Verzeichnis von Verarbeitungstätigkeiten übernommen werden. Gegenstand der Risikoanalyse ist das zu bewertende Verfahren einschließlich aller inbegriffenen technischen und organisatorischen Maßnahmen. Andere, ggf. auch geplante, aber noch nicht in das Verfahren integrierte, technische und organisatorische Maßnahmen werden bei der Risikoanalyse vorerst nicht berücksichtigt.

Zunächst erfolgt die Identifikation der Betroffenen / Betroffenengruppen, deren personenbezogene Daten im Verfahren verarbeitet werden.

Beispiel: *Kinder, Erzieher*

Dann werden die personenbezogenen Daten / Kategorien personenbezogener Daten, welche im Verfahren bearbeitet werden, identifiziert,

Beispiel: *Kinder: Stammdaten / Medizinische Daten / Entwicklungsdaten / Beobachtungen / Ereignisse*

Erzieher: Benutzerdaten

Anschließend folgt die Identifikation der an der Verarbeitung beteiligten weiteren Komponenten (Systeme und Dienste sowie Prozesse)

Beispiel: *Laptop*
Erfassungssoftware (Textverarbeitung oder Fachanwendung)
Lokales Netzwerk
Speicher (NAS bzw. Server)
Langzeitregistratur
Löschverfahren

3.2 Schutzbedarfsbestimmung

Unter Berücksichtigung der verarbeiteten personenbezogenen Daten, der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung wird der Schutzbedarf ermittelt; der Schutzbedarf entspricht der maximalen Schadenshöhe, die den jeweiligen Betroffenen widerfahren kann (siehe Beispiel unten), falls ein oder mehrere Gewährleistungsziele verletzt werden. Die Gewährleistungsziele sind

- Datenminimierung
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Nichtverkettung
- Transparenz
- Intervenierbarkeit

Der Schutzbedarf wird von ggf. bereits getroffenen technischen und organisatorischen Maßnahmen nicht beeinflusst und wird auf einer vierstufigen Skala wie folgt festgelegt (Empfehlung):

Schadenshöhe	**Definition**	**Beispiele**
Gering	Es handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung **keine besonders schwerwiegende Beeinträchtigung** des Betroffenen erwarten lässt.[1]	Namens- und Adressangaben ohne Sperrvermerke sowie Berufs-, Branchen- oder Geschäftsbezeichnungen.
Normal	Es handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen **beeinträchtige**n kann.[2]	Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten.
Hoch	Es handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen **erheblich beeinträchtigen** kann. Darunter fallen personenbezogene Daten besonderer Kategorien, personenbezogene Daten, die dem Berufsgeheimnis unterliegen, deren Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl	genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln. Personenbezogene Daten Schutzbedürftiger (z.B. Kinder),

[1] Siehe auch Datenschutzklasse I in § 11 Abs.1 KDG-DVO
[2] Siehe auch Datenschutzklasse II in § 12 Abs. 1 KDG-DVO

	oder -betrug, einem finanziellen Verlust, einer Rufschädigung, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann sowie personenbezogene Daten, die für Zwecke des Profiling verwendet werden können, insbesondere zur Analyse oder Prognose von Aspekten bezgl. Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, den Aufenthaltsort oder Ortswechsel, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.[3]	eindeutig identifizierende, hoch verknüpfbare Daten (z.B. KV-Nummer, Steuer-ID)
Sehr hoch	Es handelt sich um personenbezogene Daten, bei deren missbräuchlicher Verarbeitung **eine Gefahr für Leib und Leben** oder die **persönliche Freiheit** des Betroffenen gegeben ist.	Besondere Gesundheitsdaten, Aufenthaltsorte gefährdeter Personen

Geringe oder normale Schadenshöhe führen zu einem normalen Schutzbedarf. Hohe oder sehr hohe Schadenshöhe führen zu einem hohen Schutzbedarf.

Ein wichtiges Merkmal von Verarbeitungstätigkeiten sind die verarbeiteten Kategorien personenbezogener Daten. Anhand der verarbeiteten Kategorien personenbezogener Daten kann oft bereits ohne weitere Untersuchung der passende Schutzbedarf zugeordnet werden, wie der obigen Tabelle zu entnehmen ist.

Beispiel: *Verarbeitungen personenbezogener Daten von Kindern haben immer mindestens einen „hohen" Schutzbedarf.*

Die Verarbeitung der Benutzerdaten von Erziehern hat i.d.R. einen normalen Schutzbedarf.

Vererbung des Schutzbedarfs auf die Komponenten

Der auf diese Art ermittelte Schutzbedarf hat ebenfalls Einfluss auf die an der Verarbeitung beteiligten Systeme und Dienste sowie Prozesse. Grundsätzlich überträgt sich der Schutzbedarf auf die Komponenten, mit denen eine Verarbeitung erfolgt. In Ausnahmefällen kann es z.B. bei zentralen Komponenten wie Servern zu einer anderen Einstufung kommen, wenn die Komponente auch für andere Verfahren eingesetzt oder aber redundant vorhanden ist.

[3] Siehe auch Datenschutzklasse III in § 13 Abs. 1 KDG-DVO

3.3 Ermitteln (relevanter) Gefährdungen/Bedrohungen für die Komponenten des Verfahrens

Im Sinne des KDM stellt jede Verarbeitung personenbezogener Daten selbst schon ein Ereignis dar, durch das die Rechte und Freiheiten natürlicher Personen beeinträchtigt werden können. Bedrohungen für eben diese Rechte und Freiheiten können daher zum einen in der Gestaltung der Verarbeitungstätigkeit selbst, d.h. der Ausgestaltung der zugehörigen Systeme und Dienste und der (Teil-)Prozesse liegen. Beispiele dafür wären nicht nach dem Need-to-Know-Prinzip vergebene Berechtigungen für den Datenzugriff oder wenn die Intervenierbarkeit seitens der Betroffenen nicht gegeben ist.

Zum anderen können die Bedrohungen für die Rechte und Freiheiten auch aus dem Bereich der IT-Sicherheit und dem organisatorischen Umfeld der Verarbeitung stammen und insbesondere auf Grund von unzureichender Absicherung mittelbar auf die Verarbeitungstätigkeit und die darin verarbeiteten Daten wirken. Als Beispiel sei hier der Befall mit einer Schadsoftware zu nennen, durch die die Vertraulichkeit von personenbezogenen Daten kompromittiert werden kann.

Anhand von Gefährdungs-/Bedrohungskatalogen (z.B. ISO 29143 oder IT-Grundschutzkompendium) werden Szenarien ermittelt, in denen in den Komponenten der Verarbeitungstätigkeit, d.h. den Daten, Systemen und Diensten oder Prozessen, die Gewährleistungsziele verletzt werden können.

Beispiel: *Unbeabsichtigtes Verändern von Beobachtungsdaten durch Fehlbedienung der Fachanwendung*

Unbefugter Zugriff auf (und Offenlegung von) Stammdaten der Kinder durch Diebstahl des Laptops

3.4 Bewerten der Eintrittswahrscheinlichkeit

Für jede ermittelte Bedrohung wird die Eintrittswahrscheinlichkeit auf einer vierstufigen Skala wie folgt festgelegt (Empfehlung):

Eintrittswahrscheinlichkeit	**Definition**
Äußerst selten:	• Eintritt des Schadens ist denkmöglich, er widerspricht aber jeder Erfahrung/ist eine rein theoretische Möglichkeit
Selten:	• Eintritt des Schadens ist möglich, die konkreten Umstände sprechen aber gegen eine solche Entwicklung und es ist nicht zu erwarten, dass sich daran etwas ändert. • Eintritt des Schadens ist möglich, er hängt von einem Verhalten Dritter ab, die konkreten Umstände sprechen dafür, dass der Dritte dem Eintritt des Schadens entgegenwirkt, und es ist nicht zu erwarten, dass sich daran etwas ändert.
Gelegentlich:	• Eintritt des Schadens ist möglich, er hängt von Unwägbarkeiten ab, die sich nicht quantifizieren lassen. • Eintritt des Schadens ist möglich, er hängt von einem Verhalten Dritter ab, das sich nicht vorhersagen lässt.
Häufig:	• Eintritt des Schadens ist erwartbar. • Eintritt des Schadens ist möglich; es ist zu erwarten, dass Umstände eintreten, die den Schaden herbeiführen.

	• Eintritt des Schadens ist möglich, er hängt vom Verhalten Dritter ab, das sich bereits abzeichnet/das naheliegt/für das eine wirksame Anreizsituation besteht

Beispiel: *Unbeabsichtigtes Verändern von Beobachtungsdaten durch Fehlbedienung der Fachanwendung:* ***Selten***

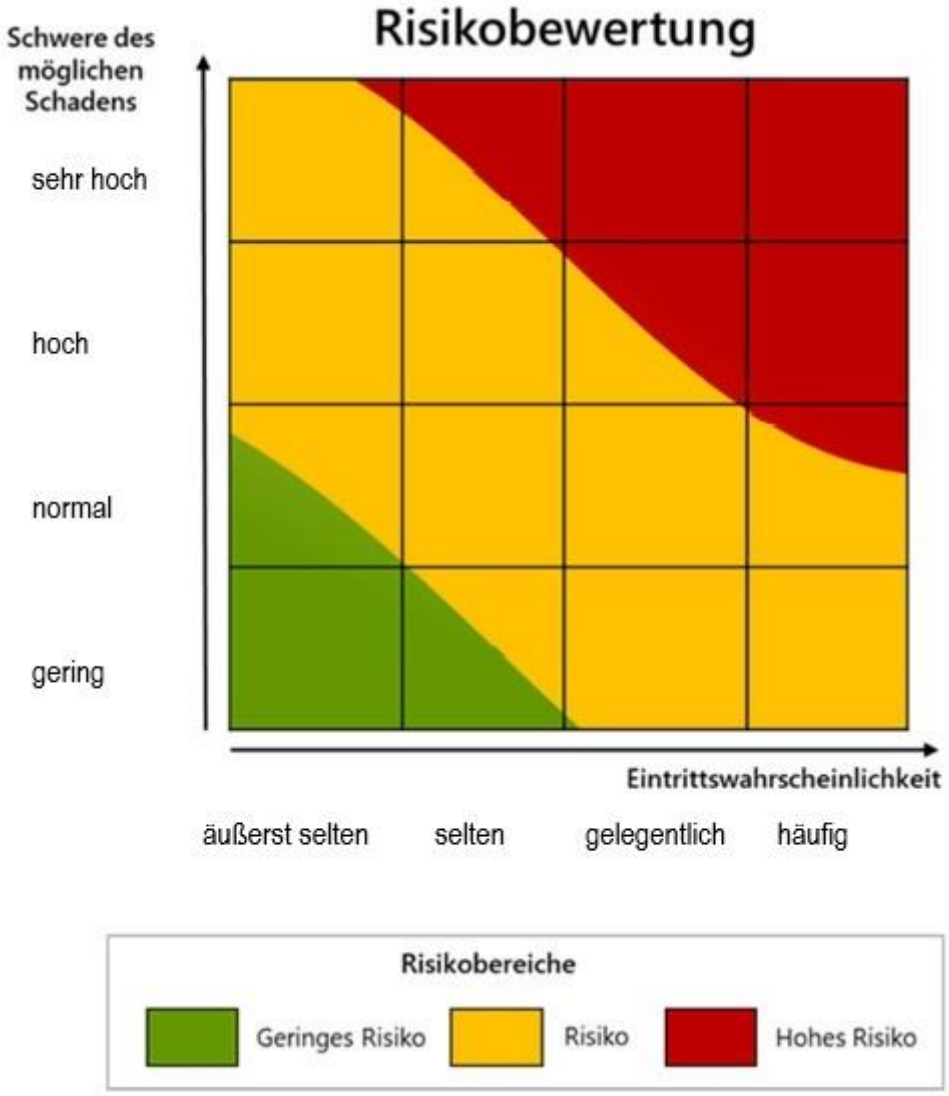
Unbefugter Zugriff auf (und Offenlegung von) Stammdaten der Kinder durch Diebstahl des Laptops: ***Häufig***

Bei der Einschätzung der Häufigkeiten ist zu beachten, dass für Ereignisse, die in der Gestaltung der Verarbeitungstätigkeit selbst liegen, demnach mit Gewissheit eintreten, grundsätzlich die höchste Eintrittswahrscheinlichkeit („Häufig“) anzunehmen ist. Die Einschätzung von Eintrittswahrscheinlichkeit für Bedrohungen, die ihren Ursprung jenseits des planungsgemäßen Ablaufs der Verarbeitungstätigkeit haben, kann auch geringer ausfallen.

Die Beschreibung der einzelnen Risiken ist damit komplett: Sie besteht aus der Konkretisierung einer Gefährdungssituation an einer an dem Verfahren beteiligten Komponente (Schadensereignis), dem Schutzbedarf der betroffenen personenbezogenen Daten) sowie der Eintrittswahrscheinlichkeit des Schadensereignisses.

3.5 Die Bewertungsmatrix

Die so ermittelten und hinsichtlich Schadenshöhe und Eintrittswahrscheinlichkeit eingestuften Risiken können zur Veranschaulichung und zur Ermittlung der Schwere des jeweiligen Risikos in einem zweidimensionalen Diagramm aufgetragen werden.



Grün: Akzeptabler Bereich

Rot: Nicht tolerierbarer Bereich

Gelb: Abwägungsbereich

Quelle: Kurzpapier Nr. 18 der DSK, Stand 26.04.2018
„Risiko für die Rechte und Freiheiten natürlicher Personen“

Anmerkung: Bei komplexen Verarbeitungstätigkeiten mit vielen Komponenten empfiehlt sich eine tabellarische Darstellung der Risiken. Zur Übersicht können die einzelnen Risiken in die Grafik eingetragen werden.

3.6 Auswertung / Interpretation

Für jedes ermittelte Risiko kann unter Berücksichtigung von Eintrittswahrscheinlichkeit und Schadenshöhe eine Bewertung vorgenommen werden.

Bei einem Ergebnis im **grünen** Feld (geringes Risiko) kann die Verarbeitung durchgeführt werden

Bei einem Ergebnis im **roten** Feld (hohes Risiko) darf die Verarbeitung in dieser Form, d.h. ohne Anwendung weiterer Maßnahmen nicht stattfinden. Hier muss der Verantwortliche zum Schritt 3.7. Risikobehandlung übergehen.

Bei einem Ergebnis im **gelben** Feld (mittleres Risiko) muss der Verantwortliche abwägen, ob die Verarbeitung in dieser Form stattfinden kann.

(Im Anhang E1 des KDM wird auf das hier zugrunde gelegte Verständnis der Begriffe „Risiko“ und „Schutzbedarf“ im Kontext von KDM und BSI-Grundschutz näher eingegangen)

3.7 Risikobehandlung

Für jedes zu behandelnde Risiko muss der Verantwortliche durch die Auswahl und Implementierung geeigneter Maßnahmen das Risiko so modifizieren, dass das Ergebnis im gelben oder grünen Bereich liegt. Sollte das nicht möglich sein, ist das Verfahren in dieser Ausprägung nicht gestattet; in diesem Fall kann jedoch eine Ausnahme nach vorheriger Konsultation durch die Aufsichtsbehörde genehmigt werden.

Eine Maßnahme kann sich entweder auf die Achse der Schadenshöhe oder auf die Achse der Eintrittswahrscheinlichkeit oder sogar auf beide Achsen auswirken. Sollten Maßnahmen formuliert werden, die etwa bestimmte Datenkategorien von der Verarbeitung ausschließen oder andere Formen der Datenminimierung implementieren, handelt es sich um eine grundlegende Änderung der Verarbeitungstätigkeit. Damit müssen die Risikoanalyse und -behandlung für die Verarbeitungstätigkeit wiederholt werden. Für die so geänderte Verarbeitung würde dann höchstwahrscheinlich ein geänderter Schutzbedarf festgestellt. Ansonsten ist lediglich die Einschätzung der Eintrittswahrscheinlichkeit zu wiederholen.

Wird für die in einer Verarbeitungstätigkeit verarbeiteten personenbezogenen Daten normaler Schutzbedarf festgestellt, sollten zunächst für jedes Gewährleistungsziel die jeweils anwendbaren generischen Maßnahmen sowie die Maßnahmen für normalen Schutzbedarf aus dem Referenzmaßnahmenkatalog (einschlägige Bausteine) des KDM berücksichtigt werden.[4]

Besteht für die in der betrachteten Verarbeitungstätigkeit verarbeiteten personenbezogen Daten hoher Schutzbedarf, so sollten ebenfalls die jeweils anwendbaren, in den generischen Maßnahmen aus Kapitel D1 sowie die Maßnahmen aus dem Referenzmaßnahmenkatalog (Bausteine) des KDM, insbesondere für hohen Schutzbedarf, berücksichtigt werden. Ggf. müssen diese durch individuelle Maßnahmen ergänzt werden.

In regelmäßigen Zyklen ist zu kontrollieren, ob die die gewählten Maßnahmen noch zielführend sind. Ggf. sind neue Maßnahmen auszuwählen. Zu beachten ist, dass das KDM sukzessive mit Bausteinen in der Anlage ergänzt wird.

[4] Ggf. bestehen zusätzliche Maßnahmenforderungen in der KDG-DVO.