

## Handreichung zum Kirchlichen Datenschutzmodell (KDM)

(Stand: 21. April 2021)

### Das Wichtigste in einem Satz

Der Zweck des KDM ist es, dabei zu helfen, die richtigen technisch-organisatorischen Maßnahmen zur Gestaltung und Absicherung von Verarbeitungstätigkeiten auszuwählen, um das ermittelte Risiko für die Rechte und Freiheiten der von dieser Verarbeitung betroffenen Personen zu minimieren.

### Adressaten dieser Handreichung

Neben den örtlichen/betrieblichen Datenschutzbeauftragten zur Unterstützung ihrer beratenden Rolle sollten zuerst die Prozessverantwortlichen einer Verarbeitung das Kirchliche Datenschutzmodell kennen und ihr erworbenes Wissen für die Auswahl und Umsetzung geeigneter Maßnahmen nutzen.

### Erste Hinweise

Lesen Sie bitte zuerst diese Handreichung. Danach werden Sie das Hauptdokument leichter lesen können. Der Datenschutz als notwendiger Schutz von Menschen im Hinblick auf ihr Grundrecht auf Privatheit und informationelle Selbstbestimmung ist dabei dem KDM sinngemäß.

## KDM Überblick

### Struktur des KDM

Das KDM gliedert sich, vereinfacht dargestellt, nach Theorie (Teile A – D1) und Praxis (Teil D2 und Folgende). Es verfolgt den Ansatz einer fortlaufenden Prozesskette von Planen > Umsetzen > Kontrollieren > Verbessern bzw. in Englisch: Plan, Do, Check und Act (PDCA- oder auch dem sogenannten Deming-Kreis, siehe <https://de.wikipedia.org/wiki/Demingkreis>).

<b>KDM Theorie</b>	<b>KDM Praxis</b>
Das nötige Hintergrundwissen zum Verstehen	Das KDM innerhalb von P D C A
Teil A – Beschreibung des KDM	<b>P</b> D C A – Verstehen der Verarbeitung (Teil D2)
Teil B – Die gesetzlichen Anforderungen	<b>P</b> D C A – Risikoanalyse /-behandlung (Teil D3)
Teil C – Die Gewährleistungsziele	<b>P</b> D C A – Maßnahmenbestimmung (Teil D4 und Richtlinie für Risikoanalyse)
Zentral sind die Gewährleistungsziele im KDM.	Dem KDM folgen dann...
Teil C2 zeigt, wie die datenschutzrechtlichen Anforderungen in den Gewährleistungszielen verankert sind.	P <b>D</b> C A – Maßnahmenumsetzung
Teil D1 nennt „typische“ Maßnahmen zu jedem Gewährleistungsziel zur Absicherung einer VT	P D <b>C</b> A – Umsetzungs-/Wirksamkeitskontrolle
	P D C <b>A</b> – Überprüfung, Neustart des Zyklus

Eine ähnliche Verbindung von Theorie und Praxis findet sich in den Referenzmaßnahmen (Siehe dazu den Abschnitt *Referenzmaßnahmenkatalog – die SDM-Bausteine für das KDM*).

### KDM und SDM

Das KDM ist in enger Abstimmung mit den Autoren des Standard-Datenschutzmodells (SDM) unter Berücksichtigung kirchlicher Aspekte entstanden. So ist das KDM-Projekt ein Beispiel der Zusammenarbeit kirchlicher und staatlicher Aufsichtsbehörden, um die einheitliche Anwendung datenschutzrechtlicher Anforderungen zu fördern ([Link zu Informationen zum SDM](#)).

### Referenzmaßnahmenkatalog - SDM-Bausteine für das KDM

Über die „typischen“ Maßnahmen in Teil D1 hinaus verweist das KDM auf weitere Maßnahmen, die das SDM als Bausteine bereitstellt und die für das KDM genutzt werden können und sollen. ([Link zu den Bausteinen](#)). Diese Bausteine stellen ein umfangreiches Methodenwissen zur Verfügung, wie technische und organisatorische Maßnahmen im Detail modelliert bzw. ausgestaltet werden können.

Bei der Bestimmung konkreter Maßnahmen hilft dann die Richtlinie zur Risikoanalyse und Risikobehandlung im Rahmen des Kirchlichen Datenschutzmodells (KDM).

Das KDM kann und soll Datenschutz-Folgenabschätzungen (DSFA) unterstützen. Aber auch für den Fall, dass im Ergebnis einer Schwellwertanalyse keine DSFA für eine geplante Verarbeitung erforderlich ist, soll das KDM helfen, Verarbeitungen sinnvoll und datenschutzgerecht zu gestalten.

# KDM Anwendung

## Anwendung des KDM in der Praxis

Ein gutes Verstehen der Verarbeitung ist die Voraussetzung, um die richtigen Maßnahmen zum Datenschutz bestimmen zu können.

Wichtiger Hinweis: Grundlegende Aspekte setzt das KDM bereits voraus.

Das KDM setzt voraus,

1. dass der Zweck, also wozu die Verarbeitung dienen soll, klar definiert ist,
2. dass die Erforderlichkeit genau dieser Verarbeitung gegeben ist und
3. dass es für genau diese (Art der) Verarbeitung eine rechtliche Grundlage gibt.

## Vorbereiten „Planen und Spezifizieren“

Die verantwortliche Stelle muss gemäß § 7 Abs. 2 KDG / § 5 Abs. 2 DSGVO die Einhaltung der Datenschutz-Grundsätze nachweisen können. Dies unterstützt nicht zuletzt das Thema „Herstellen von Transparenz“.

Das beginnt bei der Planung und bedeutet für die Datenschutzpraxis, dass bereits die Planungsschritte für eine Verarbeitung selbst nachvollziehbar und überprüfbar sein müssen. Gleich wie eine *Dokumentation* das Prüfen einer aktuell in Betrieb befindlichen Verarbeitungstätigkeit ermöglicht, soll eine *Protokollierung* die Prüffähigkeit für die Vergangenheit sicherstellen und eine datenschutzorientierte *Spezifikation* die Prüffähigkeit für die Zukunft herstellen.

## Schritt 1 Die Verarbeitung verstehen

Es braucht neben Fachkenntnissen auch praktische Erfahrungen, um eine Verarbeitung in allen ihren Facetten zu verstehen. Das Verständnis hilft hernach auch die Risiken zu erkennen, die mit der Verarbeitung verbunden sein können. In der Praxis betrachten wir deshalb die Ebenen und Komponenten der Verarbeitung wie das KDM sie erklärt.

## Schritt 2 Die Risikoanalyse einschließlich Schwellwertanalyse durchführen

Ist es wahrscheinlich, dass mit der Verarbeitung ein hohes Risiko für die Betroffenen besteht? Der Risikoansatz ist essenziell für den Datenschutz. Wenn ein hohes Risiko wahrscheinlich ist, wird die Risikoanalyse um eine Datenschutz-Folgenabschätzung ergänzt. Auch für „normales“ Risiko sind passende Maßnahmen zu bestimmen, die das Risiko auf ein akzeptables Maß verringern.

Die KDM Richtlinie „Risikoanalyse und -behandlung“ hilft, schrittweise zu einer Lösung zu kommen.

## Schritt 3 Die Maßnahmen bestimmen

- a) Gesunden Menschenverstand einsetzen (Passwörter verwenden, Schränke abschließen...)
- b) Wird für die in einer Tätigkeit verarbeiteten personenbezogenen Daten normaler Schutzbedarf festgestellt, sollten zunächst für jedes Gewährleistungsziel die jeweils anwendbaren generischen Maßnahmen (Kapitel D1) sowie die Maßnahmen für normalen Schutzbedarf aus dem Referenzmaßnahmenkatalog (einschlägige Bausteine) des KDM berücksichtigt werden. Wird hoher Schutzbedarf festgestellt, sollten Maßnahmen für hohen Schutzbedarf berücksichtigt werden. Gegebenenfalls müssen diese durch individuelle Maßnahmen ergänzt werden.