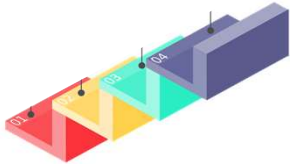
Das KDM

Ein neues Werkzeug für den kirchlichen Datenschutz

Inhalt

KDM
Kirchliches Datenschutzmodell

1. Überblick: Aufbau und Struktur des KDM
2. Die Gewährleistungsziele
3. Risikoanalyse und die Bestimmung von Maßnahmen zur Risikobehandlung
4. Datenschutzmanagement

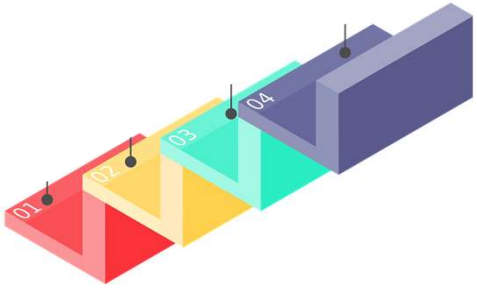


Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Inhalt

KDM
Kirchliches Datenschutzmodell

1. **Überblick: Aufbau und Struktur des KDM**
2. Die Gewährleistungsziele
3. Risikoanalyse und die Bestimmung von Maßnahmen zur Risikobehandlung
4. Datenschutzmanagement



Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Die Entwicklung zum kirchlichen Datenschutzmodell (KDM)

KDM
Kirchliches Datenschutzmodell

Das Kirchliche-Datenschutzmodell (KDM) basiert auf dem Standard-Datenschutzmodell (SDM) von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

- // Die erste Version des SDM stammt aus April 2018
- // Im November 2019 ist die Version 2.0 von der DSK verabschiedet worden
- // Die aktuelle Version 2.0b des SDM ist im April 2020 beschlossen worden

Eine Methode zur Datenschutzberatung und -prüfung auf Basis einheitlicher Gewährleistungsziele

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Die Entwicklung zum kirchlichen Datenschutzmodell (KDM)

KDM
Kirchliches Datenschutzmodell

Die Grundwerte des staatlichen SDM sollen auf die Vorgaben des kirchlichen Datenschutzes anwendbar gemacht werden.

- // Bildung einer ökumenischen Arbeitsgruppe im April 2018
- // Paritätisch besetzt mit Vertretern der Aufsichten katholischen und evangelischen Kirche
- // Erarbeitung eines Hauptdokumentes mit Bezug auf das KDG und DSG-EKD als Rechtsgrundlagen (Das SDM bezieht sich ausschließlich auf die DSGVO)
- // Förderung der Lesbarkeit des Hauptdokumentes
- // Die Überarbeitung erfolgt in Absprache mit der Unterarbeitsgruppe SDM aus dem Arbeitskreis Technik der Datenschutzkonferenz

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Aufbau und Struktur des KDM

KDM
Kirchliches Datenschutzmodell

Das KDM gliedert sich neben der Einleitung in fünf Bereiche

- // Teil A: Beschreibung des KDM
- // Teil B: Anforderung der kirchlichen Datenschutzgesetze
- // Teil C: Gewährleistungsziele des KDM
- // Teil D: Praktische Umsetzung
- // Teil E: Organisatorische Rahmenbedingungen

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil A)

KDM
Kirchliches Datenschutzmodell

Zweck des KDM

- Bereitstellung eines Werkzeuges, mit dem die Auswahl und Bewertung von TOMs unterstützt wird, die sicherstellen, dass die Verarbeitung der pb-Daten nach Vorgaben der kirchlichen Datenschutzgesetze erfolgt

- Das KDM systematisiert die TOMs auf Basis von Gewährleistungszielen und unterstützt somit die Auswahl geeigneter Maßnahmen

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil A)

KDM
Kirchliches Datenschutzmodell

Struktur des KDM

- // Systematisieren der Anforderungen in Gewährleistungsziele
- // Leitet aus den Gewährleistungszielen generische Maßnahmen ab
- // Modelliert die Verarbeitungstätigkeiten (*oder auch Prozesse der kirchlichen Stelle*)
- // Identifiziert die Risiken des Verfahrens bei der Verarbeitung von pb-Daten
- // Bietet ein Vorgehensmodell für die Modellierung, Umsetzung, Kontrolle und Prüfung von Verarbeitungstätigkeiten

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil B)

KDM
Kirchliches Datenschutzmodell

Anforderungen der kirchlichen Datenschutzgesetze

- // Umsetzung der zentralen datenschutzrechtlichen Anforderungen aus KDG und DSG-EKD (Diese Anforderungen finden sich später in Kapitel C in einer Referenztabelle wieder)
- // Es wird gesondert auf die Verarbeitung von pb-Daten auf Grundlage von Einwilligungen eingegangen
- // Ebenso wird die aufsichtsbehördliche Anordnung gesondert hervorgehoben und erläutert

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil C)

KDM
Kirchliches Datenschutzmodell

Die sieben Gewährleistungsziele

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

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil C)

KDM
Kirchliches Datenschutzmodell

Systematisierung der Gewährleistungsziele

Nr.	Anforderungen	Fundstelle im Gesetz	Gewährleistungsziel
B1.1	Transparenz für Betroffene	§ 5 Abs. 1 Nr. 1, § 16 Abs. 1 und 3 bis § 19, § 33 DSG-EKD / § 7 Abs.1 lit a, § 14, Abs. 1 und 3 bis § 17, § 34 KDG	Transparenz
B1.2	Zweckbindung	§ 5 Abs. 1 Nr. 2 DSG-EKD / § 7 Abs. 1 lit. b und § 54 KDG	Nichtverkettung

// Zuordnung der Gewährleistungsziele zu den gesetzlichen Anforderungen

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil D)

KDM
Kirchliches Datenschutzmodell

Generische Maßnahmen

- In diesem Abschnitt werden konkret TOMs ausgeführt, die in der Praxis vieler Datenschutzaufsichtsbehörden seit vielen Jahren erprobt sind
- Die Zuordnung dieser Maßnahmen zu den Gewährleistungszielen des KDM soll zeigen, dass sich die Datenschutzanforderungen sinnvoll strukturieren lassen und in der Folge systematisch umsetzen lassen
- Bei geringem oder normalem Risiko muss mindestens eine Maßnahme pro Gewährleistungsziel umgesetzt werden

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil D)

KDM
Kirchliches Datenschutzmodell

Die Ebenen einer Verarbeitung oder Verarbeitungstätigkeit

Um eine personenbezogene Verarbeitung zu erfassen, hat es sich bewährt, bei der Prüfung von Verarbeitungstätigkeiten zumindest drei verschiedene Ebenen zu betrachten.

- // **Ebene 1:** Personenbezogene Verarbeitung im datenschutzrechtlichen Sinne
- // **Ebene 2:** Praktische Umsetzung der Verarbeitung und des Zwecks
- // **Ebene 3:** IT-Infrastruktur

Auf allen Ebenen wird besonderer Wert auf die Zweckbindung der Verarbeitung gelegt

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil D)

KDM
Kirchliches Datenschutzmodell

Komponenten einer Verarbeitung oder Verarbeitungstätigkeit

Aus den Vorgaben der kirchlichen Datenschutzgesetze ergeben sich unmittelbar die Komponenten Daten, Systeme und Dienste. Bei der konkreten Modellierung von Verarbeitungstätigkeiten mit Personenbezug ist es jedoch notwendig, die folgenden Komponenten zu beachten:

- die personenbezogenen **Daten**
- die beteiligten technischen **Systeme und Dienste**
- die technischen, organisatorischen und personellen **Prozesse** der Verarbeitung von Daten

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil D)

KDM
Kirchliches Datenschutzmodell

Risiken und Schutzbedarf

Ein Risiko im Sinne der kirchlichen Datenschutzgesetze ist das Bestehen der Möglichkeit eines Eintritts eines Ereignisses, das einen Schaden für die Rechte und Freiheiten natürlicher Personen darstellt. Es hat zwei Dimensionen:

- die Schwere des Schadens für die Rechte und Freiheiten der betroffenen Person
- die Wahrscheinlichkeit, dass das Ereignis und der Schaden eintreten

Hier gibt es den gravierendsten Unterschied zu der Sichtweise der IT-Sicherheit, die den Schaden auf die Organisation und nicht auf die natürliche Person bezieht

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil D)

KDM
Kirchliches Datenschutzmodell

Datenschutzmanagement mit dem KDM

Das Datenschutzmanagement ist ein Methode, um systematisch alle Anforderungen des kirchlichen Datenschutzrechts in einer kirchlichen Stelle umzusetzen. Das KDM strukturiert es in vier Phasen:

- **Rechtliche Grundlage** (direkter Bezug auf die §§ des KDM / DSG-EKD)
- **Vorbereitung** (Klarheit über sachliche Verhältnisse / Prüfung der Zulässigkeit / weitere materiell rechtliche Beurteilungen der Rechtmäßigkeit der Verarbeitung)
- **Spezifizieren und Prüfen** (Bezug zu den Gewährleistungszielen in Abhängigkeit von dem festgestellten Risiko)
- **Datenschutzmanagement-Prozess** (in Anlehnung an den bewährten PDCA-Zyklus)

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM konkret (Teil E)

KDM
Kirchliches Datenschutzmodell

Ist das KDM verpflichtend für kirchliche Stellen?

Das KDM kann sowohl von **kirchlichen Aufsichtsbehörden** im Rahmen ihrer gesetzlichen Beratungs-, Prüf- und Sanktionstätigkeiten als auch von den **Verantwortlichen und Auftragsverarbeitern** bei der Planung und beim Betrieb der Verarbeitung personenbezogener Daten sowie den Datenschutzbeauftragten im Rahmen ihrer Beratungs- und Prüftätigkeiten angewendet werden.

Eine Verpflichtung besteht somit nicht!

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Und was ist mit den Bausteinen?

KDM
Kirchliches Datenschutzmodell

Die von der UAG-SDM erarbeiteten und vom AK-Technik freigegebenen Bausteine behandeln spezielle Themen mit Datenschutzbezug und werden dem KDM nach redaktioneller Betrachtung durch die öPG KDM als Anlagen beigefügt.

1. Bezug zu den Anforderungen der DS-GVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO-Anforderungen (vgl. SDM-V2b-Methodik-Handbuch, Teil B):

Anforderungen der DS-GVO	Gewährleistungsziele
Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO)	Nichtverkettung
Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)	Datenminimierung
Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO)	Integrität
Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO)	Datenminimierung
Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO)	Vertraulichkeit
Löschbarkeit von Daten (Art. 17 Abs. 1 DS-GVO)	Intervenierbarkeit

Bezug zu Referenztabelle

Durch den direkten Bezug der Bausteine zu den Gewährleistungszielen des KDM fügen sie sich nahtlos ein und dienen insbesondere bei einem festgestellten hohen Risiko für die Verarbeitungstätigkeit als Maßnahmenkatalog.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Baustein: Dokumentieren

KDM
Kirchliches Datenschutzmodell

Version: V1.0a

Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Versionshistorie	gültig seit	gültig bis
SDM-V2.0_Dokumentieren_V1.0	30. Juni 2020	1. September 2020
SDM-V2.0_Dokumentieren_V1.0a	2. September 2020	

1. Bezug zu den Anforderungen der DS-GVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO-Anforderungen (vgl. SDM-V2b-Methodik-Handbuch, Teil B):

Anforderungen der DS-GVO	Gewährleistungsziele
Transparenz für Betroffene (Art. 5 Abs. 1 lit. a DS-GVO)	Transparenz

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Baustein Dokumentieren/Inhaltliche Anforderungen

KDM
Kirchliches Datenschutzmodell

Ebene Daten

Nr.	Maßnahme	PDCA	Gültigkeit
M42.D01	Prüfung auf hinreichende Darstellung des Datenmodells in M42.P20	P, C	V1.0

Ebene Systeme

M42.S01	Dokumentation der Systeme und Dienste, ggf. Querverweise in M42.P20 (P, C)	P, C	V1.0

Ebene Prozesse

M42.P01	Strukturierung der Gesamtdokumentation	P	V1.0

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Inhalt

KDM
Kirchliches Datenschutzmodell

1. Überblick: Aufbau und Struktur des KDM
2. **Die Gewährleistungsziele**
3. Risikoanalyse und die Bestimmung von Maßnahmen zur Risikobehandlung
4. Datenschutzmanagement

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Funktion der Gewährleistungsziele

KDM
Kirchliches Datenschutzmodell

- Das KDM systematisiert datenschutzrechtliche Anforderungen mit Hilfe von „Gewährleistungszielen“.
- Diese können bei einer rechtskonformen Verarbeitung nur erreicht werden, wenn die Verarbeitung durch technische und organisatorische Maßnahmen flankiert werden.
- Dadurch soll das Risiko von Abweichungen von den datenschutzrechtlichen Anforderungen hinreichend gemindert werden.
- Die Gewährleistungsziele bündeln und strukturieren die datenschutzrechtlichen Anforderungen und können durch verknüpfte und skalierbare Maßnahmen erreicht werden.
- Datenschutz interpretiert die Gewährleistungsziele jedoch nicht aus der Perspektive der Organisation, sondern aus der Perspektive der betroffenen Personen und umfasst die Erfüllung der Gesamtheit der datenschutzrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten.
- Das KDM betrachtet daher die Gewährleistungsziele in ihrer Gesamtheit und erfüllt somit auch die Funktion, die bekannten Schutzziele der Informationssicherheit und die datenschutzrechtlichen Anforderungen als Gewährleistungsziele zusammenzuführen.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Systematisierung der Gewährleistungsziele

KDM
Kirchliches Datenschutzmodell

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenminimierung

KDM
Kirchliches Datenschutzmodell

- Erfasst die grundlegende datenschutzrechtliche Anforderung
- Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken
- Personenbezogene Daten nur so lange und in dem Umfang zu speichern, wie es für den Zweck der Verarbeitung erforderlich ist.
- Betrifft auch das Design der Informationstechnik durch den Hersteller sowie ihre Konfiguration (*Privacy by Design /Privacy by Default*)
- Unterstützenden Prozesse zum Beispiel bei der Wartung der verwendeten Systeme, müssen ebenfalls Berücksichtigung finden.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Verfügbarkeit

KDM
Kirchliches Datenschutzmodell

- Verfügbarkeit bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten unverzüglich möglich ist.
- Verfügbarkeit umfasst zum einen die konkrete Auffindbar- und Verwendbarkeit von Daten z.B. in der für die Verarbeitungstätigkeit genutzten Anwendung.
- Zum anderen müssen zur Umsetzung der Verfügbarkeit Maßnahmen ergriffen werden, die sicherstellen, dass personenbezogene Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können. (*Wiederherstellbarkeit*)
- Die Verfügbarkeit muss auch gegeben sein, wenn die Systeme und Dienste, die diese verarbeiten, unter einer der Verarbeitung angemessenen zu erwartenden Last stehen und auch im Falle unerwartet hoher Last sicherstellen, dass der Schutz der personenbezogenen Daten nicht gefährdet ist. (*Resilienz / Belastbarkeit der Systeme*)
- Für den Fall der Störung der Verfügbarkeit personenbezogener Daten ist sicherzustellen, dass Maßnahmen zur Behebung und Abmilderung der Verletzung getroffen werden.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Integrität

KDM
Kirchliches Datenschutzmodell

- // Zu verarbeitende personenbezogene Daten müssen unversehrt, vollständig, richtig und aktuell bleiben.
- // Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein.
- // Somit können Abweichungen berücksichtigt und ggf. korrigiert werden.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Vertraulichkeit

KDM
Kirchliches Datenschutzmodell

- Bezeichnet die Anforderung, dass keine unbefugte Person sowohl innerhalb der eigenen Einrichtung als auch Dritte oder Beschäftigte technischer Dienstleister personenbezogene Daten zur Kenntnis nehmen oder nutzen können.
- Die Vertraulichkeit personenbezogener Daten ist auch dann sicherzustellen, wenn die unterliegenden Systeme und Dienste unerwartet hoher Last unterliegen.
- Für den Fall der Störung der Vertraulichkeit, ist sicherzustellen, dass Maßnahmen zur Behebung Verletzung des Schutzes personenbezogener Daten getroffen werden.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Nichtverkettung

KDM
Kirchliches Datenschutzmodell

- Bezeichnet die Anforderung, dass Datenbestände mit personenbezogenen Daten, die für einen jeweils spezifischen Zweck erhoben worden sind, nicht zusammengeführt, also verkettet, werden.
- Neben der Pseudonymisierung sind hierfür auch Maßnahmen geeignet, mit denen die Weiterverarbeitung organisations- bzw. systemseitig getrennt von der Ursprungsverarbeitung geschieht.
- Werden personenbezogene Daten miteinander verkettet, können neue Informationen generiert werden, die dann zu einem höheren Risiko für die von der Verarbeitung betroffenen natürlichen Person führen können.
- Die Nichtverkettung entspricht dem Grundsatz der Zweckbindung aus dem kirchlichen Datenschutzrecht.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Transparenz

KDM
Kirchliches Datenschutzmodell

- Die Transparenz findet bereits in den Grundsätzen des kirchlichen Datenschutzes besondere Bedeutung.
- Transparenz bezeichnet die Anforderung, dass sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten wann (Eingabekontrolle) und für welchen Zweck (Zweckbindung) bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden.
- Ferner muss klar definiert sein, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen (Weitergabekontrolle) und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.
- Sind die vorangegangenen Merkmale erfüllt, ist erst ein rechtskonformer Betrieb und eine informierte Einwilligung durch die betroffenen Personen möglich.
- Unter diesen Voraussetzungen können betroffene Personen und Kontrollinstanzen Mängel erkennen und ggf. entsprechende Änderungen an der Verarbeitung einfordern.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Intervenierbarkeit

KDM
Kirchliches Datenschutzmodell

// Bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf

- Benachrichtigung,
- Auskunft,
- Berichtigung,
- Löschung,
- Einschränkung,
- Datenübertragbarkeit,
- Widerspruch
- und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen

unverzüglich und wirksam gewährt werden.

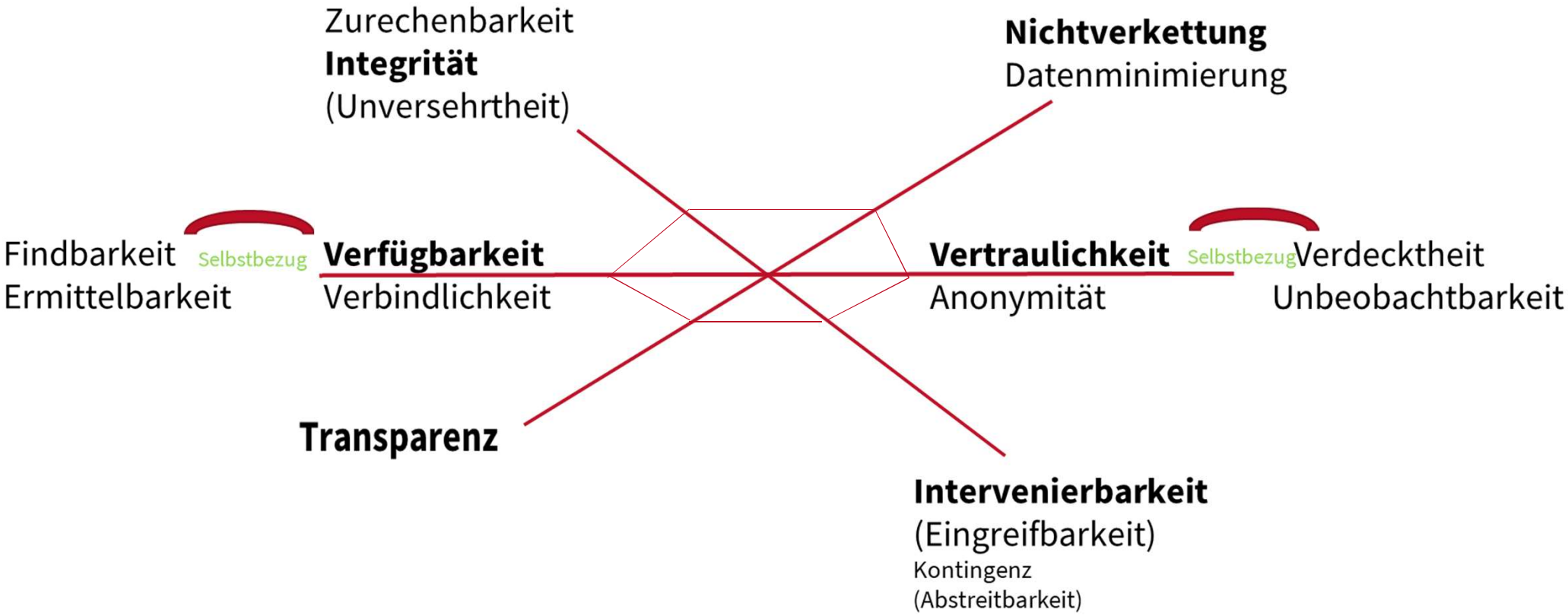
// Zur Umsetzung der Betroffenenrechte sowie der Behebung und Abmilderung von Datenschutzverletzungen müssen die für die Verarbeitungsprozesse Verantwortlichen jederzeit in der Lage sein, in die Datenverarbeitung vom Erheben bis zum Löschen der Daten einzugreifen.

// Verfügt der Verantwortliche über Informationen, die es ihm erlauben, Betroffene zu identifizieren, so sollte er dieses Wissen nicht gegen den Betroffenen verwenden.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Vollständige Systematik der Gewährleistungsziele

KDM
Kirchliches Datenschutzmodell



Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Referenzmaßnahmen zur Umsetzung

KDM
Kirchliches Datenschutzmodell

Sicherstellen von

- **Verfügbarkeit**: Redundante Datensätze, IT-Systeme, Prozesse, schnelle Reaktionszeiten
- **Integrität**: Hash-Wert-Vergleiche, Härten von IT-Systemen, Festlegen von Min./Mix.-Referenzen bei Prozessen, Steuerung der Regulation von Prozessen
- **Vertraulichkeit**: Verschlüsselung, Rollen- und Berechtigungskonzepte
- **Transparenz**: Prüffähigkeit durch Spezifikation, Protokollieren, Dokumentation, Tests und Freigaben
- **Nichtverkettbarkeit**: Pseudonymisierung, Anonymisierung, Trennung und Isolierung von Datenbeständen, IT-Systemen, Prozessabläufen, Rollen- und Berechtigungskonzept
- **Intervenierbarkeit**: SPOC für Änderungen, Korrekturen, Löschen, Aus-Schalter, standardisierte Changemanagementprozesse in Organisationen

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Grundsätzliches zu den Gewährleistungszielen

KDM
Kirchliches Datenschutzmodell

- Die Gewährleistungsziele können alle aus den Grundsätzen des kirchlichen Datenschutzes abgeleitet werden.
- Somit sind es unmittelbare Rechte zum Schutz des Persönlichkeitsrechtes direkt aus dem Gesetz heraus.
- Dies hat zur Folge, dass diese bei der Prüfung eines neuen Verfahrens unmittelbar Anwendung finden müssen.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Inhalt

KDM
Kirchliches Datenschutzmodell

1. Überblick: Aufbau und Struktur des KDM
2. Die Gewährleistungsziele
3. **Risikoanalyse und die Bestimmung von Maßnahmen zur Risikobehandlung**
4. Datenschutzmanagement

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Das KDM in der praktischen Anwendung: Risikoanalyse und Bestimmung von Maßnahmen

KDM
Kirchliches Datenschutzmodell

- Vorbereitung der Organisation als Ganzes
  - Einführung eines Datenschutz-Managementsystems (KDM Kapitel D4.4)
  - Definition von Spezifikations-, Entwicklungs- und Rollout-Prozessen nach Baustein 41

- Spezifisch für die Verarbeitung:
  - Schritt 1: Die Verarbeitung verstehen
  - Schritt 2: Risikoanalyse durchführen
  - Schritt 3: Maßnahmen bestimmen (umsetzen und kontrollieren)

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Beteiligte Quellen und Informationen

KDM
Kirchliches Datenschutzmodell

KDM
- Definitionen
- Gewährleistungsziele
- Gesetzliche Grundlagen
- Generische Maßnahmen

Richtlinie Risikomanagement
- Definitionen zu
- Schadenshöhen
- Schutzbedarf
- Eintrittswahrscheinlichkeit
- Risikohöhe
- Ablauf der Risikoanalyse

Bausteine
- Spezifische Maßnahmen in Themengruppen, abhängig von
  - Komponenten der Verarbeitungstätigkeit
  - Schutzbedarf

Verantwortlicher mit Datenschutzteam
- Ermittlung von Bedrohungsszenarien
- Einschätzung von möglichen Schadenshöhen
- Einschätzung der Eintrittswahrscheinlichkeiten
- Auswahl und Priorisierung von Schutzmaßnahmen

Verz. von Verarbeitungstätigkeiten
- Verarbeitete Datenarten
- Beteiligte Komponenten

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Schritt 1: Die Verarbeitung verstehen

KDM
Kirchliches Datenschutzmodell

Identifizieren der Komponenten der Verarbeitung:

- Daten, bzw. Datenarten (z.B. aus dem Verzeichnis von Verarbeitungstätigkeiten)
- Systeme und Dienste
  Hardware, Software, Infrastruktur
- Prozesse
  Technisch, Organisatorisch, Personell

Verarbeitungstätigkeit

Komponente 1: Daten
- Verarbeitete personenbezogene Daten

Besonders zu beachten: Eigenschaften von bestimmten Datenformaten (z. B. Metadaten und Eingabehistorien)

Komponente 2: Systeme und Dienste
- Hardware
- Microservices
- Software
- Infrastruktur

Besonders zu beachten: Schnittstellen

Komponente 3: Prozesse
- Technische Prozesse
- Organisatorische Prozesse
- Personelle Prozesse

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Schritt 2: Risikoanalyse durchführen

KDM
Kirchliches Datenschutzmodell

1. Bestimme für jedes Gewährleistungsziel und jede Datenart die mögliche Schadenshöhe (und damit den Schutzbedarf)

KDM
- Gewährleistungsziele

Verz. von Verarbeitungstätigkeiten
- Verarbeitete Datenarten

Richtlinie Risikomanagement
- Definitionen zu
- Schadenshöhen
- Schutzbedarf

Verantwortlicher mit Datenschutzteam
- Einschätzung von möglichen Schadenshöhen (und damit dem Schutzbedarf)

Gewährleistungsziel	Datenart	Mögl. Schadenshöhe	Schutzbedarf
Vertraulichkeit	Gesundheitsdaten Kind	Hoch →	Hoch
Integrität (Richtigkeit)	Gesundheitsdaten Kind	Sehr hoch →	Hoch

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Schritt 2: Risikoanalyse durchführen

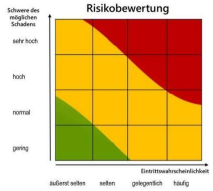
KDM
Kirchliches Datenschutzmodell

2. Bestimme für jedes Gewährleistungsziel, jede Datenart und jedes möglicherweise von Risiken betroffene Objekt mögliche Bedrohungsszenarien und deren Eintrittswahrscheinlichkeit

KDM
- Gewährleistungsziele

Verz. von Verarbeitungstätigkeiten
- Datenarten
- Beteiligte Komponenten

Richtlinie Risikomanagement
- Definitionen zu
  - Eintrittswahrscheinlichkeiten
  - Risikobewertung



Verantwortlicher mit Datenschutzteam
- Beschreibung von Bedrohungsszenarien
- Einschätzung von Eintrittswahrscheinlichkeiten

Ergebnis aus 1.

Neu!

Gewährleistungs-ziel	Datenart	Mögl. Schadenshöhe	Objekt	Bedrohungs-szenario	Eintrittswahr-scheinlichkeit	Risikobewertung
Vertraulichkeit	Gesundheitsdaten Kind	Hoch	Schnittstelle zu Behörde	Unverschlüsselte Übertragung kann in unberechtigte Hände gelangen	gelegentlich	„rot“
Integrität (Richtigkeit)	Gesundheitsdaten Kind	Sehr hoch	Verpflegungsplan	Unverträglichkeiten werden bei Essens-ausgabe nicht berücksichtigt	selten	„gelb-rot“

Schritt 3: Maßnahmen bestimmen

KDM
Kirchliches Datenschutzmodell

Bestimme für jedes mit „Rot“ oder „Dunkelgelb“ bewertete Risiko eine geeignete Maßnahme

KDM
- Generische Maßnahmen

Bausteine
- Spezifische Maßnahmen in Themengruppen, abhängig von
  - Komponenten/Ebenen des Verfahrens
  - Schutzbedarf

Verantwortlicher mit Datenschutzteam
- Ermittlung und Priorisierung von passenden Maßnahmen

Ergebnis aus 1. — *Ergebnis aus 2.* — *Neu!*

Gewährleistungs-ziel	Datenart	Schutzbedarf	Objekt	Bedrohungs-szenario	Risikobew.	Maßnahme	Quelle
Vertraulichkeit	Gesundheitsdaten Kind	Hoch	Schnittstelle zu Behörde	Unverschlüsselte Übertragung kann in unberechtigte Hände gelangen	„rot“	Daten verschlüsselt übertragen	KDM, Kap. D1.3
Integrität	Gesundheitsdaten Kind	Hoch	Verpflegungsplan	Unverträglichkeiten werden bei Essens-ausgabe nicht berücksichtigt	„gelb-rot“	Daten durch Betroffenen verifizieren lassen	KDM, Kap. D1.2 Baustein 62

Inhalt

KDM
Kirchliches Datenschutzmodell

1. Überblick: Aufbau und Struktur des KDM
2. Die Gewährleistungsziele
3. Risikoanalyse und die Bestimmung von Maßnahmen zur Risikobehandlung
4. **Datenschutzmanagement**

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

// Datenschutzmanagement mit dem KDM

Das Datenschutzmanagement ist eine Methode, um systematisch alle Anforderungen des kirchlichen Datenschutzrechts in einer kirchlichen Stelle umzusetzen. Das KDM strukturiert es in vier Phasen:

- **Rechtliche Grundlage** (direkter Bezug auf die §§ des KDM/DSG-EKD)
- **Vorbereitung** (Klarheit über sachliche Verhältnisse/Prüfung der Zulässigkeit/weitere materiell rechtliche Beurteilung der Rechtmäßigkeit der Verarbeitung)
- **Spezifizieren und Prüfen** (Bezug zu den Gewährleistungszielen in Abhängigkeit von dem gestellten Risiko)
- **Datenschutzmanagement-Prozess** (in Anlehnung an den bewährten PDCA-Zyklus)

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

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.

- Das Kirchliche Datenschutzmodell (KDM) ist aus den kirchlichen Gesetzen zum Datenschutz (DSG-EKD und KDG) abgeleitet, es lehnt sich dabei methodisch an den IT-Grundschutz an.
- In dem KDM sind generische Maßnahmen anhand der Referenzmaßnahmen gelistet.
- Anhand eines Datenschutzmanagementsystem können die Vorgaben aus dem KDM in den Einrichtungen umgesetzt werden.
- Zur Unterstützung des Datenschutzmanagementsystem können die Bausteine des KDM eingesetzt werden.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

Phase 1: Rechtliche Grundlagen des Datenschutzmanagements (Kap. D4.1)

Die kirchlichen Gesetze zum Datenschutz verpflichten den Verantwortlichen zur Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten und fordern darüber hinaus Nachweise und Dokumentationen, wie den Verpflichtungen nachgekommen wird.

DSG-EKD	KDG
§ 5 Grundsätze	§ 7 Grundsätze
§ 11 Einwilligung	§ 8 Einwilligung (Schriftformerfordernis)
§ 27 Technische und organisatorische Maßnahmen, IT-Sicherheit	§ 26 Technische und organisatorische Maßnahmen
§ 28 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	§ 27 Technikgestaltung und Voreinstellungen

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

DSG-EKD	KDG
§ 31 Verzeichnis von Verarbeitungstätigkeiten	§ 31 Verzeichnis von Verarbeitungstätigkeiten
§ 34 Datenschutz-Folgenabschätzung	§ 35 Datenschutz-Folgenabschätzung und vorherige Konsultationen

Die Verantwortlichen sind gehalten ein Verzeichnis von Verarbeitungstätigkeiten vorzuhalten und für Verarbeitungstätigkeiten, die ein voraussichtliches hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, muss auch eine Datenschutz-Folgenabschätzung durchgeführt werden.

Darüber hinaus muss auch die Umsetzung und Wirksamkeit der Maßnahmen nachgewiesen, evaluiert, ggfs. verbessert und so aktuell gehalten werden.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

Die Rechenschaft- und Nachweispflichten ist eine dauerhafte Aufgabe und sollte als dauerhafter zyklischer Prozess in den Einrichtungen etabliert werden.

Ein bereits genutztes Managementsystem mit einem kontinuierlichen Verbesserungsprozess wie bei dem PDCA-Zyklus kann die Grundlage für einen Datenschutzmanagementprozess (DSM) bilden.

Der Datenschutzmanagementprozess dient der systematischen Planung, dem dauerhaften Betrieb, einer regelmäßigen Überprüfung und Verbesserung und hilft den gesetzlichen Vorgaben nachzukommen.

Der Prozess hilft auch den Aufsichtsbehörden bei der Beratung der Verantwortlichen und bei der datenschutzrechtlichen Prüfung der Verarbeitungstätigkeiten.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

Phase 2: Vorbereitungen (Kap. D4.2)

Vor dem Start eines Datenschutzmanagementprozess sind, wie auch vor der Anwendung des KDM, folgenden Voraussetzungen zu klären:

1. Klarheit über die sachlichen Verhältnisse, im Rahmen derer die zu betrachtende Datenverarbeitung stattfindet oder stattfinden soll,
2. Prüfung der Zulässigkeit der Verarbeitung,
3. Weitere materiellrechtliche Beurteilung der Rechtmäßigkeit der Verarbeitung.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

1. Feststellung der sachlichen Verhältnisse

Bei der Aufnahme und Feststellung der sachliche Verhältnisse in denen die Verarbeitung von personenbezogene Daten stattfinden soll, ist

- aufzunehmen, welche Stellen an der Verarbeitung beteiligt sind.
- Wer trägt für welche Teile der Verarbeitung die Verantwortung?
- Welche Geschäftsprozesse werden durch die Verarbeitung unterstützt?
- Welche Daten werden in welchen Schritten und unter Nutzung welcher Systeme und Netze verarbeitet?
- Welche Personen nehmen die Datenverarbeitung vor und durch welche Personen erfolgt eine Kontrolle?
- Welche Hilfsprozesse werden zur Unterstützung der Verarbeitungstätigkeiten betrieben?

Falls in den Einrichtungen bereits ein Managementsysteme genutzt wird, können die Angaben aus den Prozessbeschreibungen entnommen und evtl. um weitere Angaben ergänzt werden.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

2. Prüfung der Zulässigkeit der Verarbeitung

Hier ist die gesetzliche Grundlage der Verarbeitungstätigkeit zu eruieren. Dazu können bei der Verarbeitung personenbezogener Daten insbesondere aus den datenschutzrechtlichen Gesetzen abgeleitete Fragen herangezogen werden:

- Bilden Einwilligungen der Betroffenen die Rechtsgrundlage für die Verarbeitungstätigkeit?
- Ist die Verarbeitung für die Erfüllung eines Vertrages erforderlich, dessen Vertragspartei die betroffene Person ist oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen?
- Ist die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der bzw. die Verantwortliche unterliegt?

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

- Ist die Verarbeitung erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen?
- Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im kirchlichen Interesse liegt?
- Ist die Verarbeitung zur Wahrung der berechtigten Interessen der bzw. des Verantwortlichen oder eines Dritten erforderlich? Überwiegen dabei die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, insbesondere dann, wenn die betroffene Person noch minderjährig ist?

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

3. Marteriellrechtliche Beurteilung der Rechtmäßigkeit der Verarbeitung

An dieser Stelle erfolgt die Beurteilung inwieweit eine geplante oder gegebenenfalls von einer Aufsichtsbehörde zu prüfende Verarbeitungstätigkeit grundsätzlich zulässig ist.

Des weiteren können so bereits Antworten generiert werden, die auf die Anwendung des KDM vorbereiten:

- Welches kirchliche oder ggfs. auch weltliche Datenschutzrecht ist auf die Verarbeitung anzuwenden?
- Welche legitimen Zwecke können mit der Verarbeitung verfolgt werden und welche Zweckänderungen sind um Zuge der Verarbeitung zulässig?
- Welche Daten sind für die Erfüllung der zulässigen Zwecke erheblich und erforderlich?
- Welche Rechtsgrundlagen bestehen zur Übermittlung von Daten an Personen innerhalb und außerhalb der

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

beteiligten Stellen sowie von diesen an Dritte?

- Sind die erforderlichen Vereinbarungen getroffen, wenn mehrere Verantwortliche in die Verarbeitungstätigkeit involviert sind und gemeinsam verantwortlich sind?
- Sind Auftragsverarbeiter in die Verarbeitung involviert und sind die Rechtsverhältnisse zwischen ihnen geregelt?
- Welchen, auf den Einzelfall bezogenen, besonderen Anforderungen müssen die technischen und organisatorischen Maßnahmen genügen?

Eine strukturierte Zusammenfassung der Ergebnisse ist unabhängig von den weiteren Schritten unentbehrlich. Diese Feststellungen gehen in die Stufe 1 „Planen/Spezifizieren“ des Datenschutzmanagement-Zyklus (DSM) ein.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

Phase 3: Spezifizieren und Prüfen (Kap. D4.3)

Die grundlegende Voraussetzung für ein Spezifizieren und daran anschließendes Prüfen ist die Festlegung, wie die gesetzlich geforderten Gewährleistungsziele für die zu betrachtende Datenverarbeitung operationalisiert werden können.

Nach der Eruierung des festgestellten Risikos (Abschnitt D3 KDM) und unter Berücksichtigung der konkreten rechtlichen Anforderungen sind nun die aus den jeweiligen Gewährleistungszielen resultierenden Eigenschaften der Verarbeitungstätigkeiten qualitativ näher zu bestimmen:

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

Gewährleistungsziel		
Verfügbarkeit	Innerhalb von welchen Prozessen ist für wen die Verfügbarkeit von welchen Daten zu gewährleisten? Innerhalb welcher Zeit müssen die Daten für wen verfügbar und ggfs. wiederherstellbar sein?	Der Einfluss der ordnungsgemäßen Verwendung der Daten auf die Interessen der Betroffenen ist der Maßstab für die Konkretisierung des Gewährleistungsziels.
Integrität	Welche Daten sind auf eine identifizierte oder identifizierbare Person bezogen und müssen daher unversehrt und aktuell gehalten werden?	Wie wird sichergestellt, dass die Prozesse, Systeme und Dienste dem gesetztem Zweck entsprechend korrekt geplant, betrieben und kontrolliert werden? Der Maßstab der Beurteilung sind die Interessen des Betroffenen.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

Gewährleistungsziel		
Vertraulichkeit	Wem ist die Kenntnisnahme welcher Daten zu verwehren? Welche Prozesse, Systeme und Dienste sind für unbefugte Zugriffe mit gewisser Wahrscheinlichkeit anfällig?	Das Ausmaß des befugten Zugriffs ist zunächst technikunabhängig aus den jeweiligen Prozessen abzuleiten. Damit ist der Rahmen zu bestimmen, innerhalb dessen sich die Maßnahmen zum Schutz der Vertraulichkeit zu bewegen haben.
Transparenz	Wie und in welcher Form ist die Verarbeitung der Daten transparent zu gestalten?	Die Anforderungen aus den Informations- und Auskunftspflichten, die Benachrichtigungspflichten, den Dokumentationspflichten und den Rechenschaftspflichten sind festzuhalten.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

Gewährleistungsziel		
Intervenierbarkeit	In welcher Ausprägung sind Betroffenenrechte zu gewähren?	Es ist festzulegen, wie Betroffene ihre Rechte wahrnehmen können, wie Anfragen gestellt und gesetzeskonform bearbeitet werden können, wie in die Verarbeitung von personenbezogenen Daten eingegriffen werden kann und in welcher Art Daten übertragen werden können.
Nichtverkettung	Welche Zweckänderungen sind möglich? Welche Zwecke von Hilfsprozessen leiten sich aus dem Hauptprozess ab?	Hier sind Maßnahmen zu benennen, die die Verarbeitung oder Nutzung von Daten außer für den festgelegten Zweck ausschließen.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

Gewährleistungsziel		
Datenminimierung	Wie wird das Ziel der Datenminimierung umgesetzt?	Grundsätzliche Vorgabe die Verarbeitung pb Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken. Das Gebot erstreckt sich auch auf die Speicherfrist der Daten und ihre Zugänglichkeit.
Belastbarkeit	Sind Systeme und Prozesse auf Ereignisse, welche Störungen der regulären Abläufe verursachen, hinreichend vorbereitet?	Welche Schadensereignisse, Störungen oder Angriffe können negative Auswirkungen für die Betroffenen haben? Stehen hierfür Gegenmaßnahmen zur Verfügung und können diese effektiv angewendet werden?

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

- Nach der Überprüfung der Gewährleistungsziele für die Verarbeitung von personenbezogenen Daten können nun die technischen und organisatorischen Maßnahmen bestimmt werden. Dazu können auch die Ergebnisse aus den Datenschutz-Folgenabschätzungen heran gezogen werden, soweit diese durchgeführt wurden. Darüber hinaus ist das im Rahmen der Risikobeurteilung festgestellte Risiko für die Rechte und Freiheiten der Verarbeitung von personenbezogenen Daten für die weitere Planung und Umsetzung maßgeblich.
- Die weitere Betrachtung ist dreiteilig:
  - Quantitative Bestimmung der Gewährleistungsziele
  - Ergebnis der Risikoprüfung bzw. Datenschutz-Folgenabschätzung bilden die Grundlage für die Abwägung zwischen der Wahrung der Interessen der Betroffenen und dem hierfür erforderlichen Aufwand der Verantwortlichen.
  - Das Ergebnis der Datenschutz-Folgenabschätzung fließt in die Bewertung der Restrisiken ein, die nach Umsetzung der Maßnahmen

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

// Phase 4: Datenschutzmanagementprozess (DSM) (Kap. D4.4)

Der Datenschutzmanagementprozess ist an den PDCA-Zyklus angelehnt und gliedert sich in vier Stufen:

1. Plan: Planen und Spezifizieren/DSFA/Dokumentieren
2. Do: Implementieren/Protokollieren
3. Check: Kontrollieren/Prüfen/Beurteilen
4. Act: Verbessern

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

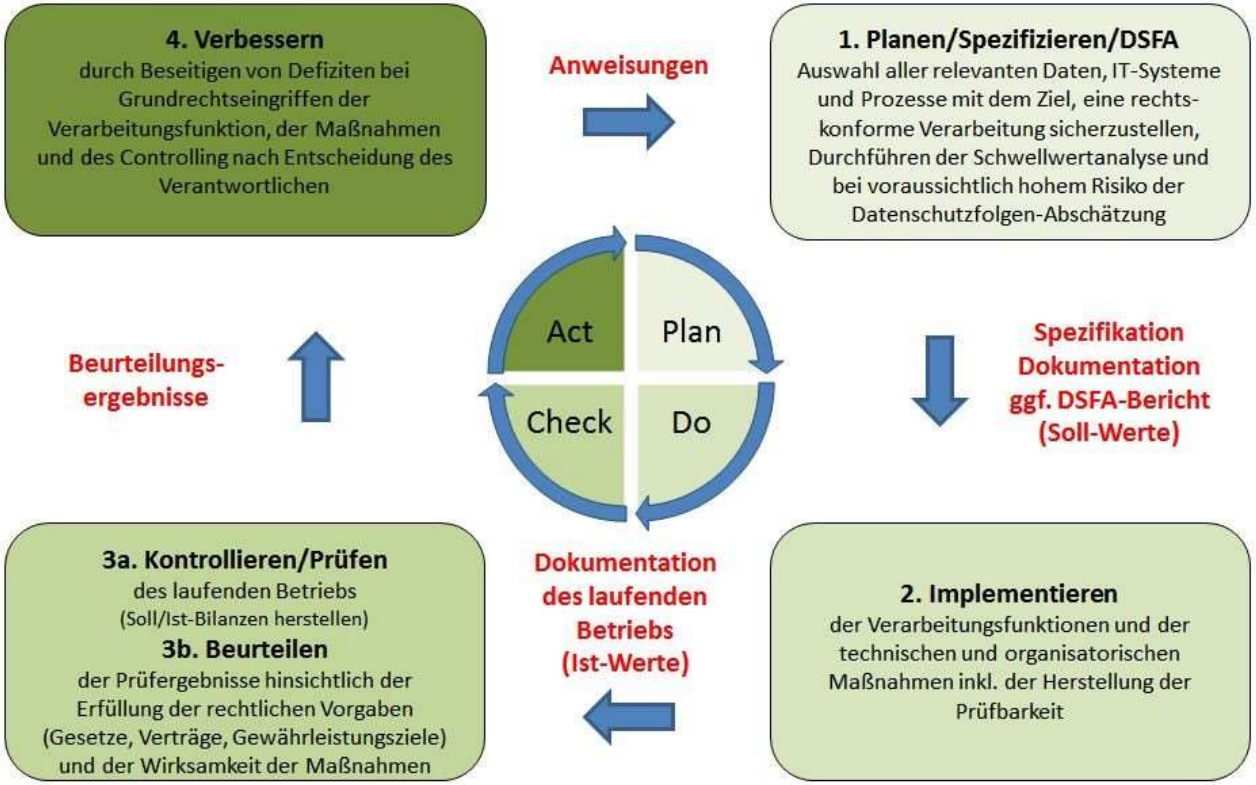
KDM
Kirchliches Datenschutzmodell

- In ***Stufe 1*** des DSM-Zyklus werden die durch die Schwellwertanalyse (Kap. D3.1) und durch die Datenschutz-Folgenabschätzung ermittelten Maßnahmen mit den in dem Referenzmaßnahmenkatalog vorgeschlagenen Maßnahmen verglichen.
- Die daraus resultierenden Maßnahmen werden in der ***Stufe 2*** des DSM für den laufenden Betrieb umgesetzt.
- In der dritten Stufe werden die aus der Planungsphase resultierenden Soll-Werte mit den aus dem laufenden Betrieb resultierenden funktionalen Ist-Werten verglichen (***Stufe 3a***). Daran anschließend erfolgt eine Beurteilung der Erfüllung der rechtlichen Vorgaben und der ggfs. verbleibenden Restrisiken für die Rechte und Freiheiten der Betroffenen (***Stufe 3b***)
- Ein zu geringes Schutzniveau bzw. ein als zu hoch eingestuftes Restrisiko muss durch geeignete Verbesserungsmaßnahmen auf ein akzeptables Maß gemindert werden (***Stufe 4***).

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell



Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

1. Plan: Spezifizieren/DSFA/Dokumentieren (Kap D4.1)

In der ersten Stufe der Planung einer Verarbeitungstätigkeit mit personenbezogenen Daten werden angemessene Maßnahmen bestimmt, durch die Risiken des Grundrechtseingriffs gemildert werden können, der Schutz der Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden können. Um die Wirksamkeit der Maßnahmen nachweisen zu können, müssen funktionale Anforderungen (Soll-Werte) festgelegt und dokumentiert werden.

Die Soll-Werte leiten sich aus den gesetzlichen Anforderungen ab. Im Anschluss daran wird festgelegt, welche Aktivitäten der eingesetzten Programme und Systeme und welche Ereignisse von Prozessen zu protokolieren sind.

Die Durchführung einer Schwellwertanalyse und die daraus ggfs. resultierende Datenschutz-Folgenabschätzung ist der wesentliche Bestandteil der ersten Stufe.

Für die Phase „Plan: Spezifizieren/DSFA/Dokumentieren“ kann der Baustein 41 „Planen und Spezifizieren“ genutzt werden.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

2. Do: Implementieren /Protokollieren (Kap. D4.2)

Die Implementierung der in der ersten Stufe eruierten und empfohlenen technischen und organisatorischen Maßnahmen erfolgt nun in der zweiten Stufe.

Wenn in der ersten Stufe eine Datenschutz-Folgenabschätzung durchgeführt wurde, müssen die Ergebnisse in diesem Abschnitt berücksichtigt und umgesetzt werden.

Bei der Implementierung von Systemen und Programmen ist auf die Systemdokumentation zu achten, die die Funktionen der Fachapplikationen und der Schutzvorkehrungen von IT-Systemen und Diensten auf den unterschiedlichen Ebenen (Client, Server) darstellt.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

3. Check: Kontrollieren/Prüfen/Beurteilen (Kap D4.3)

Die Stufe 3 ist in zwei Teile unterteilt. In dem ersten Teil sind die in der Planungsphase bestimmten funktionalen Soll-Werte (Dokumentation aus Stufe 2) mit den festgestellten Ist-Werten zu vergleichen. Zudem werden die relevanten Referenzmaßnahmen mit den tatsächlich umgesetzten technischen und organisatorischen Maßnahmen verglichen.

Abweichungen von den Soll-Werten sind danach zu beurteilen, inwieweit sie die Umsetzung der Grundsätze aus § 5 DSG-EKD/§ 7 KDG bzw. das Erreichen der Gewährleistungsziele gefährden.

In einem zweiten Teil (Stufe 3b) werden die Feststellungen der Soll-Ist-Differenz beurteilt. Die Differenzen werden wieder ins Rechtliche übersetzt und mit den datenschutzrechtlichen Anforderungen (Soll) verglichen.

Im Rahmen der Beurteilung werden aus den festgestellten Abweichungen ggfs. „Normative Mängel". Je gravierender der Mangel ist, desto wirksamer muss er durch entsprechende Änderungsanweisungen in der vierten Stufe abgestellt werden.

Das Ergebnis des zweiten Teil der dritten Stufe besteht in Beurteilungen, die geeignet sind, um rechtliche und funktionale Verbesserungen herbeizuführen.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutzmanagement und KDM

KDM
Kirchliches Datenschutzmodell

4. Act: Verbessern und Entscheiden (Kap D4.4)

Die in der Stufe 3b festgestellten Mängel müssen so formuliert sein, dass daraus konkrete funktionale Maßnahmen getroffen werden können. Diese Beurteilungen und Feststellungen sind im vierten Abschnitt zu sichten, beraten und zu priorisieren. Die daraus beschlossenen Entscheidungen sind in Anweisungen zu Änderungen von Maßnahmen oder zu neuen Maßnahmen zu formulieren. Diese sind in einem neuen Zyklus zu planen, zu implementieren und zu prüfen.

Wenn Maßnahmen getroffen wurden, die alle Mängel beseitigen, kann davon ausgegangen werden, dass alle Defizite beseitigt wurden und die Verarbeitungstätigkeit rechtskonform ist.

Katholisches Datenschutzzentrum
Evangelisch-Lutherische Landeskirche Sachsens
EKD Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD