Das
Kirchliche Datenschutzmodell

Erstellt durch die ökumenische Projektgruppe KDM und verabschiedet auf der ökumenischen Konferenz der Datenschutzaufsichtsbehörden der Katholischen Kirche in Deutschland und der Datenschutzaufsichtsbehörden der Evangelischen Kirche in Deutschland (EKD) und ihrer Gliedkirchen vom 21. April 2021

Version 1.0

Stand vom 20. Oktober 2021

basierend auf

Das
Standard-Datenschutzmodell
Eine Methode zur Datenschutzberatung
und –prüfung auf der Basis einheitlicher Gewährleistungsziele

Version 2.0 (Version 2.0b teilweise berücksichtigt)

Verabschiedet auf der 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 5. bis 7. November 2019 in Trier

Inhalt

Einleitung

Die Europäische Datenschutz-Grundverordnung (2016/679/EU-DSGVO) ist am 24. Mai 2016 in Kraft getreten und gilt nach einer zweijährigen Übergangsfrist unmittelbar seit dem 25. Mai 2018 in der gesamten Europäischen Union. Die DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Sie schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

In Art. 91 Abs. 1 DSGVO wird erstmalig auf europäischer Ebene normiert, dass die Kirchen eigenes Datenschutzrecht anwenden dürfen, wenn dieses Recht mit der DSGVO in Einklang steht. Sowohl für die evangelische Kirche als auch die katholische Kirche in Deutschland bestehen auf dieser Grundlage eigene Datenschutzgesetze. Seit dem 24. Mai 2018 gelten in der evangelischen Kirche das EKD-Datenschutzgesetz (DSG-EKD) und in der katholischen Kirche das Gesetz über den Kirchlichen Datenschutz (KDG).

In den kirchlichen Datenschutzgesetzen werden wie in der DSGVO wesentliche Grundsätze für die Verarbeitung personenbezogener Daten formuliert: Die Verarbeitung muss rechtmäßig, nachvollziehbar, zweckgebunden, auf das notwendige Maß beschränkt, auf der Basis richtiger Daten, vor Verlust, Zerstörung und Schädigung geschützt und die Integrität und Vertraulichkeit wahrend stattfinden[1]. Die Einhaltung der Grundsätze muss nachweisbar sein („Rechenschaftspflicht“). Darüber hinaus fordern die kirchlichen Regelungen mit dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu einer sehr frühzeitigen Befassung mit datenschutzrechtlichen Vorgaben bereits bei der Planung von Verarbeitungen auf. Die kirchlichen Regelungen verlangen ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Das Kirchliche Datenschutzmodell (KDM) – basierend auf dem Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder - bietet geeignete Mechanismen, um die Anforderungen der Datenschutzgesetze in technische und organisatorische Maßnahmen zu überführen. Zu diesem Zweck erfasst das KDM zunächst die rechtlichen Anforderungen und bildet sie anschließend als Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit ab. Mit dieser Herangehensweise unterstützt es die Übertragung abstrakter rechtlicher Anforderungen in konkrete technische und organisatorische Maßnahmen. Diese Maßnahmen werden im Referenzmaßnahmenkatalog[2] des KDM detailliert beschrieben.

[1] Ergänzt um „Treu und Glauben“ gemäß DSG-EKD § 5 Abs.1 und DSGVO Art. 5

[2] Der Referenzmaßnahmenkatalog beinhaltet die generischen Maßnahmen nach Kapitel D1. sowie die freigegebenen Bausteine des SDM nach Begutachtung durch die ökumenische Projektgruppe KDM.

Mit diesem Referenzmaßnahmenkatalog kann bei jeder einzelnen Verarbeitung geprüft werden, ob das rechtlich geforderte „Soll“ von Maßnahmen mit dem vor Ort vorhandenen „Ist“ von Maßnahmen übereinstimmt. Das KDM und der Referenzmaßnahmenkatalog bieten zudem eine Grundlage für die Planung und Durchführung einer Datenschutz-Folgenabschätzung. Spezifische Regelungen, wie z.B. aus existierenden Durchführungs-verordnungen, sind zu berücksichtigen.

Mit dem KDM wird eine Methode bereitgestellt, mit der die Risiken für die Rechte und Freiheiten natürlicher Personen mit Hilfe von geeigneten technischen und organisatorischen Maßnahmen beseitigt oder reduziert werden können.

Die evangelischen und katholischen Datenschutzaufsichtsbehörden hoffen mit dem KDM ein abgestimmtes, transparentes und nachvollziehbares System der datenschutzrechtlichen Beurteilung zu bieten.

Teil A: Beschreibung des KDM

A1 Zweck des KDM

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 zur Nutzung des KDM ist nicht vorgesehen. Die Verwendung des KDM wird dennoch von den kirchlichen Aufsichtsbehörden empfohlen.

Mit dem KDM wird ein mögliches Werkzeug bereitgestellt, mit dem die Auswahl und Bewertung technischer und organisatorischer Maßnahmen unterstützt wird, sodass die Verarbeitung personenbezogener Daten nach den Vorgaben der kirchlichen Datenschutzgesetze erfolgt. Diese Maßnahmen müssen angemessen und geeignet sein, die Risiken für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen soweit einzudämmen, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Für jede Verarbeitung ist also zu prüfen, ob die personenbezogenen Daten durch eine angemessene Auswahl technischer und organisatorischer Maßnahmen so verarbeitet werden, dass die Rechte der Betroffenen gewahrt bleiben und die Sicherheit der Verarbeitung gewährleistet wird. Das KDM systematisiert diese Maßnahmen auf der Basis von Gewährleistungszielen und unterstützt somit die Auswahl geeigneter Maßnahmen.

Das KDM dient einer konformen Gestaltung von Verarbeitungstätigkeiten im Sinne des Datenschutzes. Voraussetzung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sind eine Rechtsgrundlage (Zulässigkeit der Verarbeitung) und die Gewährleistung der Sicherheit der Datenverarbeitung. Es gelten die Verarbeitungsgrundsätze und die Bedingungen für die Rechtmäßigkeit der Verarbeitung der kirchlichen Datenschutzgesetze[3]. Das KDM kann erst nach Feststellung einer Rechtsgrundlage angewendet werden.

Anschließend ist zu prüfen, ob die Datenverarbeitung auf das notwendige Maß beschränkt (Datenminimierung) und geeignete Maßnahmen zur Eindämmung des Risikos für die Rechte und Freiheiten der betroffenen Personen umgesetzt wurden[4]. Diese Prüfung setzt voraus, dass dieses Risiko der Verarbeitung klar bestimmt ist. Denn die Auswahl geeigneter Maßnahmen ist abhängig von den Risiken.

Insofern ist das KDM Teil eines sich wiederholenden und fortlaufend verbessernden Prozesses bestehend aus der rechtlichen Bewertung, der Gestaltung der Verarbeitungsvorgänge sowie der risikobasierten Auswahl und Umsetzung von begleitenden technischen und organisatorischen Maßnahmen. Das KDM bietet mit seinen Gewährleistungszielen eine Transformationshilfe zwischen den gesetzlichen Anforderungen und der Umsetzung in der

[3] §§ 5 und 6 DSG-EKD / §§ 7 und 6 KDG
[4] § 5 Absatz 1 Ziff. 3 und § 27 Absatz 1 DSG-EKD / § 7 Absatz 1 lit. c) und § 26 Absatz 1 KDG

Praxis. Dieser Prozess läuft während des gesamten Lebenszyklus einer Verarbeitung und kann somit die Forderung nach regelmäßiger Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen unterstützen.

Bereits bei den ersten Planungen einer Verarbeitungstätigkeit mit personenbezogenen Daten müssen mögliche Risiken identifiziert und bewertet werden, um die Folgen der Verarbeitung beurteilen zu können.

Das KDM bietet mit der Risiko-Analyse (siehe D.3.2) auch eine Systematik, um eine Datenschutz-Folgenabschätzung (DSFA) in strukturierter Form zu erarbeiten.

Das KDM richtet sich sowohl an die Aufsichtsbehörden als auch an die datenverarbeitenden Stellen, die mit dem KDM die erforderlichen Funktionen und technischen und organisatorischen Maßnahmen systematisch planen, umsetzen und kontinuierlich überwachen können.

A2 Anwendungsbereich des KDM

Die Anwendungsbereiche des KDM sind Planung, Einführung und Betrieb von Verarbeitungstätigkeiten, sowie deren Prüfung und Beurteilung.

Solche Verarbeitungstätigkeiten sind dadurch gekennzeichnet, dass sie auf einen konkreten, abgrenzbaren und rechtlich legitimierten Verarbeitungszweck und auf die diesen Zweck verwirklichenden (Geschäfts-)Prozesse gerichtet sind (siehe Kapitel D2).

Die Datenschutzgesetze fordern, für jede Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen auszuwählen und umzusetzen, die nach dem Stand der Technik und nach dem Risiko der Rechte und Freiheiten natürlicher Personen erforderlich und angemessen sind.

A3 Struktur des KDM

Das KDM

- systematisiert datenschutzrechtliche Anforderungen mit Hilfe von Gewährleistungszielen,
- leitet systematisch aus den Gewährleistungszielen generische Maßnahmen ab, ergänzt um einen Referenzmaßnahmenkatalog,
- modelliert die Verarbeitungstätigkeit mit ihren Elementen Daten, Systeme und Dienste sowie deren Teilprozesse
- systematisiert die Feststellung von Schutzbedarf und Risiken betroffener Personen (siehe Anlage „Richtlinie Risikoanalyse und Risikobehandlung“) und
- bietet ein Vorgehensmodell für eine Modellierung, Umsetzung und kontinuierliche Kontrolle und Prüfung von Verarbeitungstätigkeiten.

A4 Funktion der Gewährleistungsziele des KDM

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 sollen Abweichungen von datenschutzrechtlichen Anforderungen vermieden werden. Die zu vermeidenden Abweichungen schließen die unbefugte Verarbeitung durch Dritte und die Nichtdurchführung vorgeschriebener Verarbeitungen ein. Die Gewährleistungsziele bündeln und strukturieren die datenschutzrechtlichen Anforderungen und können durch verknüpfte und skalierbare Maßnahmen erreicht werden. Auf diese Weise wird die Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung minimiert und ein wirksamer Schutz betroffener Personen durch die Minderung von Risiken für die Rechte und Freiheiten natürlicher Personen aufgebaut.

Das KDM benennt für den Datenschutz sieben elementare Gewährleistungsziele, die in Kapitel C detailliert vorgestellt werden:

- Datenminimierung
- Verfügbarkeit,
- Integrität,
- Vertraulichkeit,
- Nichtverkettung,
- Transparenz und
- Intervenierbarkeit.

Die Gewährleistungsziele beziehen sich nicht auf die Perspektive der Organisation, sondern auf die Perspektive der betroffenen Personen und umfassen die Erfüllung der Gesamtheit der datenschutzrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten. Das KDM betrachtet daher die o. g. Gewährleistungsziele in ihrer Gesamtheit und erfüllt somit auch die Funktion, die bekannten Schutzziele der Informationssicherheit und die datenschutzrechtlichen Anforderungen als Gewährleistungsziele zusammenzuführen.

Der europäische Gesetzgeber hat in der Datenschutz-Grundverordnung das Konzept der Gewährleistungsziele aufgegriffen. Die kirchlichen Gesetze regeln Grundsätze der Verarbeitung[5], die im Anwendungsbereich dieser Gesetze allgemeine Geltung beanspruchen. Die zentralen datenschutzrechtlichen Anforderungen (siehe Abschnitt B2) lassen sich mit Hilfe der Gewährleistungsziele vollständig systematisieren (siehe Abschnitt C). Das KDM stellt dabei keine über das geltende Datenschutzrecht hinausgehenden Anforderungen dar.

[5] § 5; § 27 Absatz 1 S. 2 Ziff. 2 DSG-EKD / § 7; § 26 Absatz 1 S. 2 lit. c) KDG

Teil B: Anforderungen der kirchlichen Datenschutzgesetze

Mit dem KDM wird das Ziel verfolgt, die in den kirchlichen Datenschutzgesetzen formulierten Anforderungen praktisch umzusetzen. Daher ist es erforderlich, aus den gesamten Vorschriften dieser Regularien diejenigen rechtlichen Anforderungen systematisch herauszuarbeiten, die durch technische und organisatorische Maßnahmen zu erfüllen sind. Dies ist erstens mit der Schwierigkeit verbunden, dass sich diese Anforderungen in den kirchlichen Datenschutzgesetzen an vielen verschiedenen Stellen finden und nicht an einer Stelle gebündelt worden sind. Zweitens besteht das Problem, dass die Anforderungen der Datenschutzgesetze keinen einheitlichen Konkretisierungsgrad aufweisen. Teilweise formulieren die Normen bereits konkrete Anforderungen wie Transparenz, Datenminimierung und Zweckbindung[6]. Teilweise müssen die rechtlichen Anforderungen aber erst aus den Rechten, Pflichten und sonstigen Vorgaben abgeleitet werden. Häufig ist daher ein Zwischenschritt vom Gesetzestext zur Anforderung erforderlich, wie bei der Vorgabe datenschutzfreundlicher Voreinstellungen.

Das KDM legt die im Folgenden erläuterten datenschutzrechtlichen Anforderungen zugrunde, die aus den kirchlichen Datenschutzgesetzen systematisch herausgearbeitet worden sind. Die Anforderungen werden in die folgenden drei Bereiche unterteilt:

1. Zentrale datenschutzrechtliche Anforderungen,
2. Einwilligungsmanagement und
3. Umsetzung aufsichtsbehördlicher Anforderungen.

Die zentralen datenschutzrechtlichen Anforderungen sind grundsätzlich bei jeder Verarbeitung personenbezogener Daten umzusetzen. Im Einwilligungsmanagement werden die Anforderungen zusammengefasst, die zusätzlich zu erfüllen sind, wenn die Rechtmäßigkeit der Verarbeitung auf die Einwilligung der betroffenen Person gestützt wird[7]. Schließlich müssen gegebenenfalls für die Umsetzung aufsichtsbehördlicher Maßnahmen weitere Anforderungen berücksichtigt werden.

Im Folgenden wird übersichtlich dargestellt, aus welchen Vorschriften der kirchlichen Datenschutzgesetze welche Anforderungen abgeleitet wurden.[8]

[6] § 5 Absatz 1 DSG-EKD / § 7 Absatz 1 KDG
[7] § 6 Nr. 2 DSG-EKD / § 6 Absatz 1 lit. b) KDG
[8] Das KDM betrachtet weder grundlegende Fragen der materiellen Rechtmäßigkeit einer Verarbeitung noch spezialgesetzliche Regelungen oder Regelungen auf einem hohen Detaillierungsgrad. Daher ist aus dieser rechtlichen Vorgabe keine Anforderung abzuleiten, die im KDM aufgenommen wird. Die Orientierung an den allgemein geltenden Grundsätzen des Datenschutzes erübrigt daher nicht die Kenntnisnahme der datenschutzrechtlichen Regelungen, auch nicht im Bereich der technischen und organisatorischen Maßnahmen.

Die folgenden Anforderungen ergeben sich unmittelbar aus DSG-EKD und KDG[9]:

- Transparenz für Betroffene von Verarbeitungen personenbezogener Daten
- Zweckbindung einer Verarbeitung personenbezogener Daten
- Datenminimierung einer Verarbeitung personenbezogener Daten
- Richtigkeit personenbezogener Daten
- Speicherbegrenzung personenbezogener Daten
- Integrität personenbezogener Daten
- Vertraulichkeit personenbezogener Daten

Übergreifend ergibt sich die Vorgabe, dass der bzw. die Verantwortliche die Einhaltung der Grundsätze nachweisen können muss[10].

- Rechenschafts- und Nachweisfähigkeit

Die kirchlichen Datenschutzgesetze erkennen verschiedene Rechte der Betroffenen an. Die Rechte der Betroffenen ergeben sich explizit aus DSG-EKD und KDG[11]. Die Verantwortlichen müssen die Voraussetzungen für die Gewährung dieser Rechte durch technische und organisatorische Maßnahmen schaffen[12].

Aus der rechtlichen Vorgabe der Berücksichtigung der Betroffenenrechte ergeben sich im Einzelnen die folgenden Anforderungen[13]:

- Unterstützung bei der Wahrnehmung von Betroffenenrechten
- Identifizierung und Authentifizierung des Auskunftsersuchenden
- Berichtigungsmöglichkeiten von Daten
- Löschbarkeit von Daten
- Einschränkbarkeit der Verarbeitung von Daten (ehemals Sperrung)
- Datenübertragbarkeit
- Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen
- Fehler- und Diskriminierungsfreiheit beim Profiling

Durch die kirchlichen Datenschutzgesetze wird der Datenschutz durch den Einsatz von Technik stark gefördert. Dieses wird in DSG-EKD und KDG bereits zu mehreren Anforderungen ausdifferenziert[14]:

- Datenschutz durch Voreinstellungen
- Verfügbarkeit der Systeme, Dienste und Daten
- Belastbarkeit der Systeme und Dienste

[9] § 5 Absatz 1 DSG-EKD / § 7 Absatz 1 KDG
[10] §§ 5 Absatz 2 und 27 Absatz 1 DSG-EKD / §§ 7 Absatz 2 und 26 Absatz 1 KDG
[11] Kapitel 3 DSG-EKD (§§ 16 – 25 DSG-EKD) / Kapitel 3 Abschnitt 2 KDG (§§ 17-24 KDG)
[12] §§ 16, 27 DSG-EKD / §§ 14, 26 KDG
[13] Die Prüfung der Voraussetzungen der Betroffenenrechte muss erfolgen, ist aber nicht Gegenstand des KDM.
[14] §§ 27 und 28 DSG-EKD / §§ 26 und 27 KDG

- Wiederherstellbarkeit der Daten und des Datenzugriffs
- Evaluierbarkeit

Gegenüber Aufsichtsbehörden und Betroffenen besteht für Verantwortliche eine Meldepflicht bzw. Benachrichtigungspflicht beim Auftreten von Verletzungen des Schutzes personenbezogener Daten (Datenschutzverletzungen)[15]. Daraus ergeben sich Anforderungen an einen ordnungsgemäßen Umgang mit Datenschutzverletzungen, der nur dann erfolgen kann, wenn Fähigkeiten zur Feststellung von Datenschutzverletzungen[16], zur Klassifikation von Datenschutzverletzungen, zur Meldung von Datenschutzverletzungen an Aufsichtsbehörden und zur Benachrichtigung der von Datenschutzverletzungen Betroffenen vorhanden sind. Daraus resultieren die folgenden Anforderungen:

- Behebung und Abmilderung von Datenschutzverletzungen
- angemessene Überwachung der Verarbeitung

Beruht die Verarbeitung auf einer Einwilligung, dann sind zusätzlich zu den allgemeinen Anforderungen weitere spezifische Anforderungen einzuhalten[17] (siehe B2).

- Einwilligungsmanagement

Die kirchlichen Datenschutzgesetze räumen Aufsichtsbehörden verschiedene Befugnisse im Rahmen ihrer Aufgabenerfüllung ein[18] (siehe Kapitel B3):

- Umsetzung aufsichtsbehördlicher Anordnung

B1 Zentrale datenschutzrechtliche Anforderungen der kirchlichen Datenschutzgesetze

B1.1 Transparenz für Betroffene

Transparenz als tragender Grundsatz des Datenschutzrechts[19] findet sich in zahlreichen Regelungen der kirchlichen Datenschutzgesetze. Insbesondere die Informations- und Auskunftspflichten[20] tragen ihm Rechnung. Die Verantwortlichen haben geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln[21]. Die Betroffenen müssen

[15] §§ 32 und 33 DSG-EKD / §§ 33 und 34 KDG
[16] vgl. Erwägungsgrund 87 DSGVO
[17] § 11 und ggfs. § 12 DSG-EKD / § 8 KDG
[18] § 44 DSG-EKD / § 47 KDG
[19] § 5 Absatz 1 Nr. 1 DSG-EKD / § 7 Absatz 1 lit. a) KDG
[20] §§ 16 ff. DSG-EKD / §§ 14 ff. KDG
[21] § 16 Absatz 1 DSG-EKD / § 14 Absatz 1 KDG

innerhalb von drei Monaten (DSG-EKD)[22] / unverzüglich und auf jeden Fall innerhalb eines Monats (KDG)[23] über den Stand der Bearbeitung und der ergriffenen Maßnahmen bezüglich ihres Antrags informiert werden. Auch die Benachrichtigungspflicht bei einer Verletzung des Schutzes personenbezogener Daten[24], einer sogenannten Datenpanne, dient dem Grundsatz der Transparenz.

B1.2 Zweckbindung

Die Verpflichtung, Daten nur für den Zweck zu verarbeiten, zu dem sie erhoben wurden, ist insbesondere den einzelnen Verarbeitungsbefugnissen zu entnehmen, die die Geschäftszwecke, die Forschungszwecke etc. zum Maßstab machen und findet über den Zweckbindungsgrundsatz[25] Eingang in die kirchlichen Datenschutzgesetze. Eine darauffolgende Verarbeitung für weitere Zwecke muss (sofern keine der in den Vorschriften[26] genannten Voraussetzungen zutreffen) mit dem ursprünglichen Zweck kompatibel sein und die Umstände der Verarbeitung berücksichtigen[27]. Über eine Weiterverarbeitung über den ursprünglichen Zweck hinaus sind die betroffenen Personen ggfs. zu informieren, so dass sie von ihrem Widerspruchsrecht Gebrauch machen können.

B1.3 Datenminimierung

In einem engen Zusammenhang mit dem Grundsatz der Zweckbindung steht der Grundsatz der Datenminimierung. Die Gesetzgeber fordern, die Erhebung personenbezogener Daten und ihre Weiterverarbeitung auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken[28]. Diese grundlegende Anforderung entspricht weitgehend dem aus dem deutschen Recht bekannten Grundprinzip der Datensparsamkeit. Es ist nur bedingt möglich, zwischen den drei Voraussetzungen dem Zweck angemessen, für den Zweck erheblich und für die Zwecke der Verarbeitung auf das notwendige Maß beschränkt zu differenzieren.

Angemessen sind Daten, die einen konkreten inhaltlichen Bezug zum Verarbeitungszweck aufweisen. Es soll eine wertende Entscheidung über die Zuordnung von Datum und Zweck vorgenommen werden.

Erheblich sind Daten, deren Verarbeitung einen Beitrag zur Zweckerreichung leistet. Dieses Merkmal entspricht der Geeignetheit bei der Verhältnismäßigkeitsprüfung.

Auf das notwendige Maß beschränkt sind nur die Daten, die zur Erreichung des Zwecks erforderlich sind, ohne deren Verarbeitung der Verarbeitungszweck also nicht erreicht werden kann. Diese Definition ergibt sich auch aus Erwägungsgrund 39 DSGVO. Die Verarbeitung personenbezogener Daten ist demnach nur dann erforderlich, wenn der Zweck

[22] § 16 Absatz 3 DSG-EKD
[23] § 14 Absatz 3 KDG
[24] § 33 DSG-EKD / § 34 KDG
[25] § 5 Absatz 1 Nr. 2 DSG-EKD / § 7 Absatz 1 lit. b) KDG
[26] § 7 Absatz 1 DSG-EKD / § 6 Absatz 2 KDG
[27] § 7 Absatz 2 DSG-EKD / § 6 Absatz 4 KDG
[28] § 5 Absatz 1 Nr. 3 DSG-EKD / § 7 Absatz 1 lit. c) KDG

der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Der Eingriff in das Grundrecht auf Datenschutz ist nur zulässig, soweit er auf das geringstmögliche Maß begrenzt ist.

Die Erforderlichkeit ist ein allgemeiner Grundsatz des Unionsrechts, der durch den Europäischen Gerichtshof (EuGH) in jahrelanger Rechtsprechung anerkannt und ausgeprägt worden ist. Die Vorgabe, nur erforderliche Daten zu verarbeiten, wird in den kirchlichen Datenschutzgesetzen von dem Grundsatz der Datenminimierung erfasst. Sie wird zudem als Voraussetzung unmittelbar in den Erlaubnisvorschriften zur Rechtmäßigkeit der Verarbeitung und zur Verarbeitung besonderer Kategorien personenbezogener Daten gefordert[29].

Der Grundsatz der Datenminimierung ist nicht nur vor dem Beginn der Verarbeitung zu berücksichtigen, sondern auch fortlaufend. So kann die Anforderung der Beschränkung auf das notwendige Maß dazu führen, dass personenbezogene Daten zu einem bestimmten Zeitpunkt zu anonymisieren sind.

Der Grundsatz der Datenminimierung geht davon aus, dass der beste Datenschutz darin besteht, keine oder möglichst wenige personenbezogene Daten zu verarbeiten. Das Optimierungsziel ist mit dem Bewertungskriterium der Minimierung von Verfügungsgewalt und Kenntnisnahme gegeben. An ihm orientiert kann die optimale Abfolge von Verarbeitungsschritten gewählt und in der Folge an sich verändernde Bedingungen angepasst werden. Im Laufe der Verarbeitung ist schließlich mit technischen und organisatorischen Maßnahmen zu gewährleisten, dass sich die Datenverarbeitung nur innerhalb des a priori gesteckten Rahmens bewegt.

Die frühestmögliche Löschung nicht weiter benötigter und damit nicht mehr erforderlicher personenbezogener Daten ist eine solche Maßnahme. Zuvor jedoch können bereits einzelne Datenfelder oder Attribute von bestimmten Formen der Verarbeitung ausgenommen oder die Zahl der Datensätze, auf die eine Funktionalität anwendbar ist, beschränkt werden. Datenfelder, welche die Identifizierung der Betroffenen ermöglichen, können gelöscht oder transformiert (Anonymisierung, Pseudonymisierung) oder ihre Anzeige in Datenmasken unterdrückt werden, sodass sie den handelnden Personen nicht zur Kenntnis gelangen, vorausgesetzt, diese Kenntnis ist für den jeweiligen Verarbeitungszweck entbehrlich.

B1.4 Richtigkeit

DSG-EKD und KDG formulieren die Anforderung der Richtigkeit personenbezogener Daten[30]. Dies bedingt, dass die von einer Verarbeitung betroffenen personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen. Um diese Anforderung sicherzustellen, sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene

[29] § 6 Nr. 3 bis 8 und § 13 Absatz 2 Nr. 2, 3, 6 bis 9 DSG-EKD / § 6 Absatz 1 lit. a) und lit. c) bis g) und § 11 Absatz 2 lit. b), c), f) bis j) KDG
[30] § 5 Absatz 1 Nr. 4 DSG-EKD / § 7 Absatz 1 lit. d) KDG

Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

B1.5 Speicherbegrenzung

Der Grundsatz der Speicherbegrenzung[31] bestimmt, dass personenbezogene Daten nur so lange in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Hieraus leitet sich die Notwendigkeit von Maßnahmen der Pseudonymisierung, Anonymisierung bzw. Löschung ab. Eine Ausnahme von diesem Grundsatz ist zulässig, soweit die personenbezogenen Daten ausschließlich für Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden[32].

B1.6 Integrität

Die Anforderung der Integrität ist ein Grundsatz für die Verarbeitung von personenbezogenen Daten[33] und, angewendet auf Systeme und Dienste, ein Aspekt der zu gewährleistenden Sicherheit der Datenverarbeitung[34]. So sind u. a. unbefugte Veränderungen und Entfernungen auszuschließen. Personenbezogene Daten dürfen nur in einer Weise verarbeitet werden, die einen Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen gewährleistet. Es sollen jegliche Veränderungen an den gespeicherten Daten durch unberechtigte Dritte ausgeschlossen oder zumindest so erkennbar gemacht werden, dass sie korrigiert werden können.

B1.7 Vertraulichkeit

Die Verpflichtung zur Wahrung der Vertraulichkeit besteht als Grundsatz bei der Verarbeitung personenbezogener Daten[35] und in Bezug auf die zur Verarbeitung eingesetzten Systeme und Dienste[36], und zwar sowohl für die Verantwortlichen als auch für die Auftragsverarbeiter und die Personen, die den Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind. Ferner ergibt sie sich aus der Bindung an die Weisungen des oder der Verantwortlichen[37], der Verpflichtung auf das Datengeheimnis[38] bzw. einer gesonderten Vertraulichkeitsverpflichtung[39] und ggf. gesetzlichen Verschwiegenheitspflichten. Für örtlich Beauftragte für den Datenschutz (DSG-EKD) bzw. betriebliche Datenschutzbeauftragte (KDG)

[31] § 5 Absatz 1 Nr. 5 DSG-EKD / § 7 Absatz 1 lit. e) KDG
[32] § 21 Absatz 3 Nr. 4 DSG-EKD / § 19 Absatz 3 lit. d) KDG
[33] § 5 Absatz 1 Nr. 6 DSG-EKD / § 7 Absatz 1 lit. f) KDG
[34] § 27 Absatz 1 Nr. 2 DSG-EKD / § 26 Absatz 1 lit. b) KDG und § 6 Absatz 1 lit. c) KDG-DVO
[35] § 5 Absatz 1 Nr. 6 DSG-EKD / § 7 Absatz 1 lit. f) KDG
[36] § 27 Absatz 1 Nr. 2 DSG-EKD / § 26 Absatz 1 lit. b) und § 6 Absatz 1 lit. c) KDG-DVO
[37] § 27 Absatz 5, § 30 Absatz 4 DSG-EKD / § 26 Absatz 5, § 30 KDG
[38] § 26, § 30 Absatz 3 Nr. 5 DSG-EKD / § 5 KDG
[39] § 29 Absatz 4 lit. b) KDG

ergibt sie sich zudem aus deren Verschwiegenheitspflicht[40]. Unbefugte dürfen keinen Zugang zu den Daten haben und weder die Daten noch Geräte, mit denen diese verarbeitet werden, benutzen können[41]. Eine Verletzung der Vertraulichkeit ist insbesondere dann anzunehmen, wenn eine Verarbeitung personenbezogener Daten unbefugt erfolgt.

B1.8 Rechenschafts- und Nachweisfähigkeit

Die Verantwortlichen sind verpflichtet, die Einhaltung der Grundsätze zur Verarbeitung personenbezogener Daten nachzuweisen[42]. In den Vorschriften zu den technischen und organisatorischen Maßnahmen wird diese Pflicht noch dahingehend erweitert, dass der bzw. die Verantwortliche insgesamt sicherzustellen und den Nachweis dafür zu erbringen hat, dass bei der Verarbeitung ein dem Risiko angemessenes Schutzniveau eingehalten wird[43]. Diese umfassenden Rechenschafts- und Nachweispflichten werden an mehreren Stellen in den kirchlichen Datenschutzgesetzen konkretisiert. Wenn die Verarbeitung personenbezogener Daten auf der Einwilligung der Betroffenen gründet, so sind die Verantwortlichen dazu verpflichtet, die Einwilligung der Betroffenen nachweisen zu können[44]. Damit die Verarbeitungstätigkeiten der Verantwortlichen oder des Auftragsverarbeiters geprüft werden können, fordern die Datenschutzgesetze die Anlage eines Verzeichnisses von Verarbeitungstätigkeiten, in dem die einzelnen Verarbeitungstätigkeiten beschrieben werden und Verantwortliche insbesondere den Zweck jeder Verarbeitungstätigkeit angeben müssen[45]. Die Verantwortlichen sind darüber hinaus dazu verpflichtet, jede Verletzung des Schutzes personenbezogener Daten für eine etwaige Überprüfung einer Aufsichtsbehörde zu dokumentieren[46]. Die Verantwortlichen müssen prüfen, ob ihre Verarbeitungstätigkeit wahrscheinlich zu einem hohen Risiko für die Betroffenen führen kann. In diesen Fällen müssen die Verantwortlichen nachweisen können, dass sie eine Datenschutz-Folgenabschätzung durchgeführt haben[47]. Die Verantwortlichen müssen den Aufsichtsbehörden alle Informationen zur Erfüllung ihrer Aufgaben auf Anfrage bereitstellen können[48]. Datenschutzverletzungen müssen die Verantwortlichen unter den in den kirchlichen Datenschutzgesetzen geregelten Umständen[49] an die Aufsichtsbehörden melden.

[40] 37 Absatz 1 Satz 6 i. V. m. § 42 Absätze 6 und 7 DSG-EKD / § 37 Absatz 2 Satz 4 i. V. m. § 43 Absätze 9 und 10 KDG
[41] § 27 Absatz 1 Nr. 2 DSG-EKD / § 26 Absatz 1 lit. b) und § 6 Absatz 1 lit. c) KDG-DVO (siehe auch ErwGr. 39 S.12 DSGVO)
[42] § 5 Absatz 2 DSG-EKD / § 7 Absatz 2 KDG
[43] § 27 Absatz 1 DSG-EKD / § 26 Absatz 1
[44] § 11 Absatz 1 DSG-EKD / § 8 Absatz 5 KDG
[45] § 31 DSG-EKD / § 31 KDG und § 1 KDG-DVO
[46] § 32 Absatz 5 DSG-EKD / § 33 Absatz 5 KDG
[47] § 34 DSG-EKD / § 35 KDG
[48] § 44 Absatz 1 DSG-EKD / § 44 Absatz 2 lit. b) KDG
[49] § 32 DSG-EKD / § 33 KDG

B1.9 Identifizierung und Authentifizierung

Bei begründeten Zweifeln kann der bzw. die Verantwortliche von einer natürlichen Person, die Betroffenenrechte[50] ihm gegenüber ausüben möchte, Informationen anfordern, die zur Bestätigung der Identität der Person erforderlich sind. Daraus ergibt sich die Anforderung, dass der bzw. die Verantwortliche eine Vorgehensweise zur Authentifizierung von Personen, die die Betroffenenrechte geltend machen, festlegen und umsetzen muss[51].

B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten

Die Verantwortlichen müssen Betroffenen die Ausübung ihrer Rechte erleichtern[52]. In jedem Fall müssen Anträge von Betroffenen zur Wahrnehmung ihrer Rechte entgegengenommen und geprüft werden. Maßnahmen zur Umsetzung der Betroffenenrechte müssen ausgewählt und umgesetzt werden.

B1.11 Berichtigungsmöglichkeit von Daten

Von dem Grundsatz der Richtigkeit der Daten[53] ist rechtlich die Berichtigungsmöglichkeit von Daten zu unterscheiden. Diese Anforderung ergibt sich unmittelbar aus dem Recht der Betroffenen auf unverzügliche Berichtigung sie betreffender unrichtiger Daten[54], das auch von Aufsichtsbehörden eingefordert werden kann[55]. Mit diesem Recht korrespondiert für die Verantwortlichen die Pflicht, bei Vorliegen der Voraussetzungen die Berichtigung faktisch durchzuführen und die Berichtigung unverzüglich vorzunehmen. Soweit dies nicht ohne Weiteres zu realisieren ist, haben die Verantwortlichen hierfür geeignete Vorgehensweisen festzulegen[56].

B1.12 Löschbarkeit von Daten

Betroffene haben das Recht auf Löschung ihrer Daten, sofern die genannten Voraussetzungen erfüllt sind[57] und keine der genannten Ausnahmen[58] vorliegt. Die Verantwortlichen sind verpflichtet, die Löschung der Daten unverzüglich vorzunehmen. Die kirchlichen Datenschutzgesetze definieren den Vorgang der Löschung nicht. Nicht die Löschungshandlung, sondern deren Ergebnis ist rechtlich entscheidend. Eine datenschutzkonforme Löschung muss dazu führen, dass die Daten nicht mehr verarbeitet werden können. Es muss unverzüglich gelöscht werden. Soweit dies nicht ohne weiteres zu

[50] §§ 19 bis 25 DSG-EKD / §§ 17 bis 24 KDG
[51] § 14 Absatz 6 KDG
[52] § 16 Absatz 2 DSG-EKD / § 14 Absatz 2 KDG
[53] § 5 Absatz 1 Nr. 4 DSG-EKD / § 7 Absatz 1 lit. d) KDG
[54] § 20 DSG-EKD / § 18 KDG
[55] § 44 Absatz 3 Nr. 4 DSG-EKD / § 47 Absatz 5 lit. d) KDG
[56] § 28 Absatz 1 i. V. m. § 5 Absatz 1 Nr. 4 DSG-EKD / §§ 26, 27 Absatz 1 i. V. m. § 7 Absatz 1 lit. d) KDG
[57] § 21 Absatz 1 DSG-EKD / § 19 Absatz 1 KDG
[58] § 21 Absatz 3 DSG-EKD / § 19 Absatz 3 KDG

realisieren ist, haben die Verantwortlichen hierfür geeignete Vorgehensweisen festzulegen[59]. Aufsichtsbehörden können die Löschung anordnen[60].

B1.13 Einschränkbarkeit der Verarbeitung von Daten

Die Datenschutzgesetze sehen als Ergänzung der Löschung von Daten die Einschränkung ihrer Verarbeitung als Betroffenenrecht vor[61]. Gemäß Definition[62] bezeichnet Einschränkung der Verarbeitung die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung so einzuschränken, dass sie nur noch unter den in den Vorschriften genannten Bedingungen[63] (mit Einwilligung oder für die dort bestimmten Zwecke) erfolgen. Die Markierung muss eine technische Maßnahme darstellen, durch die faktisch sichergestellt wird, dass die Daten nur noch begrenzt verarbeitet werden können. Die Aufsichtsbehörden können die Einschränkung der Verarbeitung anordnen[64].

B1.14 Datenübertragbarkeit

Die Datenübertragbarkeit ist ein neu durch die kirchlichen Datenschutzgesetze eingeführtes Betroffenenrecht[65]. Die betroffene Person hat das Recht, die sie betreffenden Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten[66]. Aus der Vorschrift ergeben sich bereits konkrete Anforderungen, die der zu übermittelnde Datensatz erfüllen muss. Daten gelten als maschinenlesbar, wenn sie in einem Dateiformat vorliegen, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten einfach identifizieren, erkennen und extrahieren können.[67]

B1.15 Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen

Das katholische Datenschutzgesetz regelt ein zusätzliches Betroffenenrecht bezogen auf automatisierte Verarbeitungen – einschließlich Profiling –, die zu rechtsverbindlichen Entscheidungen im Einzelfall führen[68]. Daraus resultiert in bestimmten Fällen die Pflicht des oder der Verantwortlichen, angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des oder der Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört[69]. Das Recht einzugreifen setzt voraus, dass in Prozesse automatisierter

[59] § 28 Absatz 1 i. V. m. § 5 Absatz 1 Nr. 5 DSG-EKD / §§ 26, 27 Absatz 1 i. V. m. § 7 Absatz 1 lit. e) KDG
[60] § 44 Absatz 3 Nr. 4 DSG-EKD / § 47 Absatz 5 lit. d) KDG
[61] § 22 DSG-EKD / § 20 KDG
[62] § 4 Nr. 4 DSG-EKD / § 4 Nr. 4 KDG
[63] § 22 Absatz 2 DSG-EKD / § 20 Absatz 2 KDG
[64] § 44 Absatz 3 Nr. 4 DSG-EKD / § 47 Absatz 5 lit. d) KDG
[65] § 24 DSG-EKD / § 22 KDG
[66] § 24 Absatz 1 DSG-EKD / § 22 Absatz 1 KDG
[67] ErwGr. 21 der RL 2013/37/EU
[68] § 24 KDG
[69] § 24 Absatz 3 KDG

Entscheidungen manuell eingegriffen und eine Entscheidung im Einzelfall korrigiert werden kann.

B1.16 Fehler- und Diskriminierungsfreiheit beim Profiling

Es ist eine faire und transparente Verarbeitung zu gewährleisten. Daher sind für das Profiling technische und organisatorische Maßnahmen zu treffen, mit denen in geeigneter Weise sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten oder zu Entscheidungen führen, die die betroffene Person diskriminieren, korrigiert werden und das Risiko von Fehlern minimiert wird. Im Ergebnis soll der Datenverarbeitungsprozess fehler- und diskriminierungsfrei sein. Die Anforderungen an den Verarbeitungs- und Bewertungsprozess für das Profiling werden auch in Erwägungsgrund 71 DSGVO entsprechend konkretisiert.

B1.17 Datenschutz durch Voreinstellungen

Die kirchlichen Datenschutzgesetze sehen eine neue datenschutzrechtliche Verpflichtung der Verantwortlichen zur Umsetzung des Prinzips Datenschutz durch Voreinstellungen (Data Protection by Default) vor[70]. Die Verantwortlichen müssen geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch entsprechende Voreinstellungen nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Hierzu ist nicht nur die Menge der verarbeiteten Daten zu minimieren, sondern auch der Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Von den Voreinstellungen kann nur dann in Einzelfällen derart abgewichen werden, dass eine umfassendere Datenverarbeitung vorgenommen bzw. eine breitere Zugänglichkeit ermöglicht werden, wenn Umstände dieser Einzelfälle ein Abweichen erfordern oder die jeweilige betroffene Person ein Abweichen explizit wünscht. Der letztgenannte Fall ist von besonderer Bedeutung, wenn die betroffene Person als Nutzer eines informationstechnischen Systems auf dieses Einfluss nehmen kann und ihr die Möglichkeit eingeräumt wird, Verarbeitungsoptionen zu wählen. Falls umfangreichere Verarbeitungsoptionen zur Verfügung stehen, dürfen sie dann nur durch Betroffene eingeschaltet und aktiviert werden können.

B1.18 Verfügbarkeit

Verfügbarkeit ist als Grundsatz für die Verarbeitung personenbezogener Daten in den kirchlichen Datenschutzgesetzen verankert[71] und ist darin zudem explizit im Kontext der Sicherheit von Datenverarbeitungen aufgenommen[72]. Die Verfügbarkeit der Daten muss zu dem jeweiligen Zweck gewährleistet sein, solange dieser noch besteht. Der Grundsatz kommt auch zum Tragen bei den Informations- und Auskunftspflichten gegenüber den Betroffenen[73].

[70] § 28 Absatz 2 DSG-EKD / § 27 Absatz 2 KDG
[71] § 5 Absatz 1 Nr. 6 DSG-EKD / § 7 Absatz 1 lit. f) KDG
[72] § 27 Absatz 1 Nr. 2 und 3 DSG-EKD / § 26 Absatz 1 lit. b) und c) KDG
[73] §§ 17, 18 und 19 DSG-EKD / §§ 15, 16 und 17 KDG

Für die Umsetzung des Rechts auf Datenübertragbarkeit[74] ist die Anforderung der Verfügbarkeit ebenso Grundvoraussetzung.

B1.19 Belastbarkeit

Die kirchlichen Datenschutzgesetze fordern die Belastbarkeit der Systeme und Dienste[75]. Das Ziel der Belastbarkeit war bisher weder aus dem Datenschutzrecht bekannt, noch ist es ein klassisches Ziel der IT-Sicherheit und wird auch insbesondere im IT-Grundschutzkatalog des BSI nicht als Schutzziel aufgegriffen. In der englischen Fassung wird der Begriff „Resilience“ verwendet, der in der deutschen Literatur der Informatik regelmäßig mit „Widerstandsfähigkeit“ oder „Ausfallsicherheit“ übersetzt wird. In diesem Sinne bedeutet er, dass die zur Verarbeitung verwendeten Systeme und Dienste auch unter widrigen Einflüssen, die insbesondere von Dritten herrühren können, die Eigenschaften aufrechterhalten, die eine rechtmäßige Verarbeitung gewährleisten.

B1.20 Wiederherstellbarkeit

Die kirchlichen Datenschutzgesetze fordern zur Gewährleistung der Sicherheit der Verarbeitung die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen[76]. Darunter sind sowohl gezielte Angriffe zu fassen als auch Unfälle und unvorhersehbare Ereignisse, die zum Beispiel durch Naturphänomene hervorgerufen werden. Der Schwerpunkt der zu treffenden Maßnahmen liegt auf dem zeitlichen Aspekt der Wiederherstellbarkeit, d. h. die Vorschrift fordert insbesondere eine prozessorientierte Notfallplanung mit zugeordneten Wiederanlaufzeiten. Die Wiederherstellbarkeit der Daten und des Datenzugriffs geht also über die allgemein geforderte Verfügbarkeit[77] hinaus. Die Verfasser der kirchlichen Datenschutzgesetze gehen insofern davon aus, dass für das Ziel der unverzüglichen Wiederherstellbarkeit nach einem Zwischenfall zusätzliche technische und organisatorische Maßnahmen zu ergreifen sind.

B1.21 Evaluierbarkeit

Die in den kirchlichen Datenschutzgesetzen geforderte Evaluierung[78] dient nicht unmittelbar, sondern mittelbar dem operativen Datenschutz und der Datensicherheit. Es soll ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung entwickelt und umgesetzt werden.

[74] § 24 DSG-EKD / § 22 KDG
[75] § 27 Absatz 1 Nr. 2 DSG-EKD, § 1 Absatz 1 ITSVO-EKD / § 26 Absatz 1 lit. b) KDG und § 6 Absatz1 lit. c) KDG-DVO
[76] § 27 Absatz 1 Nr. 3 DSG-EKD / § 26 Absatz 1 lit. c) KDG und § 6 Absatz 1 lit. d) KDG-DVO
[77] § 27 Absatz 1 Nr. 2 DSG-EKD / § 26 Absatz 1 lit. b) KDG
[78] § 27 Absatz 1 Nr. 4 DSG-EKD / § 26 Absatz 1 lit. d) KDG und § 7 Absatz 1 KDG-DVO

B1.22 Behebung und Abmilderung von Datenschutzverletzungen

Die Verantwortlichen müssen bei Datenschutzverletzungen technische und organisatorische Maßnahmen umsetzen, die die Datenpanne beheben und eventuelle Folgen für die Betroffenen abmildern.[79]

B1.23 Angemessene Überwachung der Verarbeitung

Um u. a. eine wirksame Behebung und Abmilderung sicherstellen zu können, können Verantwortliche und der Auftragsverarbeiter ggf. dazu verpflichtet sein, als technische und organisatorische Maßnahme im Sinne der Datenschutzgesetze[80] eine Überwachung der Verarbeitung durchzuführen. Zudem kann mit einer angemessenen Überwachung der Verarbeitung dafür gesorgt werden, dass Datenschutzverletzungen sofort festgestellt und klassifiziert werden können.

B2 Einwilligungsmanagement

Eine besondere Rechtsgrundlage stellt die Einwilligung[81] dar. Sofern die Zulässigkeit der Datenverarbeitung auf einer wirksamen Einwilligung basieren soll, ergeben sich aus diesen Vorschriften datenschutzrechtliche Anforderungen an das Einwilligungsmanagement, welches das vollständige Verfahren der Einholung, der Speicherung, der Dokumentation, des Nachweises sowie der Umsetzung eines Widerrufs der Einwilligung umfasst. Im Einzelnen ist die Einwilligung nur wirksam, wenn

- eine vorherige umfassende Information des Betroffenen über die Datenverarbeitung erfolgt ist,
- der Einwilligungstext konkrete Datenverarbeitungen klar und eindeutig benennt,
- die Einwilligung freiwillig erklärt wird und
- eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, erfolgt.

Schließlich muss ein jederzeitiger Widerruf der Einwilligung möglich sein mit der Konsequenz, dass die personenbezogenen Daten dann nicht mehr weiterverarbeitet und unter Einhaltung gesetzlicher Fristen gelöscht werden.

Der Widerruf einer Einwilligung muss so einfach sein wie ihre Erteilung[82]. Die Verantwortlichen haben geeignete Vorgehensweisen für die Entgegennahme und die Umsetzung des Widerrufs festzulegen. Insbesondere wenn Einwilligungen über elektronische

[79] § 32 Absatz 3 Nr. 4 und § 33 Absatz 2 DSG-EKD / § 33 Absatz 3 lit. d) und § 34 Absatz 2 KDG
[80] § 27 DSG-EKD / § 26 KDG
[81] § 6 Nr. 2 i. V. m. § 4 Nr. 13 DSG-EKD / § 6 Absatz 1 lit. b) i. V. m. § 4 Nr. 13 KDG
[82] § 11 Absatz 3 DSG-EKD / § 8 Absatz 6 KDG

Kommunikationsmittel eingeholt werden, folgen aus diesen rechtlichen Vorgaben Anforderungen an die Ausgestaltung des Verfahrens.

B3 Umsetzung aufsichtsbehördlicher Anordnungen

Die Aufsichtsbehörden haben das Recht, gegenüber den Verantwortlichen die Beschränkung einer Verarbeitung zu verhängen[83], die dazu führen kann, dass die Verarbeitung nicht in der vorgesehenen Art und Weise fortgesetzt werden darf. Die Beschränkung kann qualitativ oder quantitativ ausgerichtet sein. Als qualitative Beschränkungen können z. B. Anordnungen getroffen werden, dass nur bestimmte Daten oder Daten nur zu bestimmten Zwecken verarbeitet werden dürfen sowie räumliche und zeitliche Verarbeitungsgrenzen festgelegt werden. Als eine quantitative Beschränkung kommt z. B. die Begrenzung von Zugriffsberechtigungen auf Datenbanken in Betracht. Beschränkungen können somit sehr unterschiedlich ausgestaltet sein. Aufgrund dieser Vielgestaltigkeit kann nur die recht abstrakte Anforderung der Umsetzbarkeit aufsichtsbehördlicher Maßnahmen formuliert werden.

Die Aufsichtsbehörden haben auch das Recht anzuordnen, dass eine Übermittlung von Daten an Empfänger in Drittländern ausgesetzt wird[84]. Die Umsetzung dieser Anordnung setzt voraus, dass die Empfänger von personenbezogenen Daten lokalisiert werden können und Datenübermittlungen nach dem Kriterium des Empfängerlandes gesteuert werden können.

[83] § 44 Absatz 3 Nr. 2 DSG-EKD / § 47 Absatz 5 lit. c) KDG
[84] § 44 Absatz 3 Nr. 3 DSG-EKD / § 47 Absatz 5 lit. e) KDG

Teil C: Gewährleistungsziele

Nachfolgend werden die Gewährleistungsziele kurz beschrieben, mit deren Hilfe die Anforderungen des DSG-EKD/des KDG systematisiert werden können (siehe Kapitel C2).

C1 Systematisierung der Gewährleistungsziele

C1.1 Datenminimierung

Das Gewährleistungsziel Datenminimierung erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken. Das bedeutet insbesondere, nicht mehr personenbezogene Daten zu verarbeiten, als für das Erreichen des Verarbeitungszwecks benötigt werden. (B1.3 Datenminimierung) und diese auch nur so lange und in dem Umfang zu speichern, wie es für den Zweck der Verarbeitung erforderlich ist (B1.5 Speicherbegrenzung). Datenminimierung betrifft u.a. das Design der Informationstechnik durch den Hersteller sowie ihre Konfiguration (B1.17 Datenschutzfreundliche Voreinstellungen) und auch die unterstützenden Prozesse zum Beispiel bei der Wartung der verwendeten Systeme, müssen berücksichtigt werden.

C1.2 Verfügbarkeit

Das Gewährleistungsziel Verfügbarkeit bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten durch den Berechtigten und ihre Verarbeitung mit den vorgesehenen Methoden unverzüglich möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet werden können. Die Verfügbarkeit umfasst zum einen die konkrete Auffindbarkeit und Verwendbarkeit von Daten z. B. in der für die Verarbeitungstätigkeit genutzten Anwendung (B1.18 Verfügbarkeit). 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 (B1.20 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 (B1.19 Belastbarkeit). Für den (Ausnahme-)Fall der Störung der Verfügbarkeit personenbezogener Daten ist sicherzustellen, dass Maßnahmen zur Behebung und Abmilderung der Verletzung getroffen werden (B1.22 Behebung und Abmilderung von Datenschutzverletzungen).

C1.3 Integrität

Das Gewährleistungsziel Integrität bezeichnet die Eigenschaft, dass die zu verarbeitenden Daten unversehrt (B1.6 Integrität), vollständig, richtig und aktuell (B1.4 Richtigkeit) bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein (B1.23 Angemessene Überwachung der Verarbeitung), damit sie

berücksichtigt und korrigiert werden können (B1.22 Behebung und Abmilderung von Datenschutzverletzungen).

C1.4 Vertraulichkeit

Das Gewährleistungsziel Vertraulichkeit 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 (B1.7 Vertraulichkeit). Die Vertraulichkeit personenbezogener Daten ist auch dann sicherzustellen, wenn die unterliegenden Systeme und Dienste unerwartet hoher Last unterliegen (B1.19 Belastbarkeit). Für den (Ausnahme-) Fall der Störung der Vertraulichkeit, so ist sicherzustellen, dass Maßnahmen zur Behebung und Abmilderung der einhergehenden Verletzung des Schutzes personenbezogener Daten getroffen werden (B1.22 Behebung und Abmilderung von Datenschutzverletzungen).

C1.5 Nichtverkettung

Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass Datenbestände mit personenbezogenen Daten, die für einen jeweils spezifischen Zweck erhoben worden sind, nicht zusammengeführt, also verkettet, werden (B1.2 Zweckbindung). Neben der Pseudonymisierung sind hierfür auch Maßnahmen geeignet, mit denen die Weiterverarbeitung organisations- bzw. systemseitig getrennt von der Ursprungsverarbeitung geschieht.

C1.6 Transparenz

Das Gewährleistungsziel Transparenz bezeichnet die Anforderung, dass sowohl Betroffene (B1.1 Transparenz für Betroffene), als auch die Betreiber von Systemen (B1.23 Angemessene Überwachung der Verarbeitung) sowie zuständige Kontrollinstanzen (B1.8 Rechenschafts- und Nachweisfähigkeit) erkennen können, welche Daten wann (Eingabekontrolle) und für welchen Zweck (Zweckbindung) bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, 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. Erst wenn dies bekannt ist, ist ein rechtskonformer Betrieb und eine informierte Einwilligung durch die betroffenen Personen möglich (B2 Einwilligungsmanagement). Auf diese Weise können betroffene Personen und Kontrollinstanzen Mängel erkennen und ggf. entsprechende Änderungen an der Verarbeitung einfordern.

C1.7 Intervenierbarkeit

Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung (B1.11 Berichtigungsmöglichkeit von Daten), Löschung (B1.12 Löschbarkeit von Daten), Einschränkung (B1.13 Einschränkbarkeit der Verarbeitung von Daten), Datenübertragbarkeit (B1.14 Datenübertragbarkeit), Widerspruch und Erwirkung des Eingriffs in automatisierte

Einzelentscheidungen (B1.15 Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen) bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten) und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen. Zur Umsetzung der Betroffenenrechte und aufsichtsbehördlicher Anordnungen (B3 Umsetzung aufsichtsbehördlicher Anordnungen) sowie der Behebung und Abmilderung von Datenschutzverletzungen (B1.22 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.

Verfügen Verantwortliche über Informationen, die es erlauben, Betroffene zu identifizieren, so sollte er für den Fall, dass Betroffene ihre Rechte bspw. im Rahmen von Auskunftsersuchen geltend machen wollen, dieses Wissen zum Schutz eben dieser Betroffenen bspw. für die eindeutige Identifizierung und Authentifizierung der Anfragenden nutzen (B1.9 Identifizierung und Authentifizierung).

C2 Systematisierung der rechtlichen Anforderungen mit Hilfe der Gewährleistungsziele

Im folgenden Abschnitt werden alle im Abschnitt B1 aufgeführten datenschutzrechtlichen Anforderungen den in Abschnitt C1 beschriebenen Gewährleistungszielen des KDM zugeordnet. Diese Zuordnung dient der in Abschnitt A4 erläuterten Systematisierung der Anforderungen in Bezug auf die technische und organisatorische Ausgestaltung von Verarbeitungstätigkeiten.

Nr.	Anforderungen	Fundstelle im Gesetz	Gewährleistungsziel
B1.1	Transparenz für Betroffene	§ 5 Absatz 1 Nr. 1, § 16 Absatz 1 und 3 bis § 19, § 33 DSG-EKD / § 7 Absatz1 lit a, § 14, Absatz 1 und 3 bis § 17, § 34 KDG	Transparenz
B1.2	Zweckbindung	§ 5 Absatz 1 Nr. 2 und § 50 DSG-EKD / § 7 Absatz 1 lit. b und § 54 KDG	Nichtverkettung
B1.3	Datenminimierung	§ 5 Absatz 1 Nr. 3 DSG_EKD / § 7 Absatz 1 lit. c KDG	Datenminimierung
B1.4	Richtigkeit	§ 5 Absatz 1 Nr. 4 DSG-EKD / § 7 Absatz 1 lit. d KDG	Integrität
B1.5	Speicherbegrenzung	§ 5 Absatz 1 Nr. 5 DSG-EKD / § 7 Absatz 1 lit. e und § 54 KDG	Datenminimierung
B1.6	Integrität	§ 5 Absatz 1 Nr. 6, § 27 Absatz 1 Nr. 2 DSG-EKD / § 7 Absatz 1 lit. f, § 26 Absatz1 lit b KDG, § 6 Absatz1 lit. c KDG-DVO	Integrität

B1.7	Vertraulichkeit	§ 5 Absatz 1 Nr. 6, § 30 Absatz 3 Nr. 5, § 27 Absatz 1 Nr. 2, § 27 Absatz 5 DSG-EKD / § 7 Absatz 1 lit. f, § 29 Absatz 4 lit. b, § 30, §26 Absatz 1 lit. b, § 26 Absatz 5 KDG, § 6 Absatz 1 lit. c KDG-DVO	Vertraulichkeit
B1.8	Rechenschafts- und Nachweisfähigkeit	§ 5 Absatz 2, § 11 Absatz 1, § 27 Absatz 1, § 31, § 32 Absatz 5, § 34, § 44 Absatz 1 DSG-EKD / § 7 Absatz 2, § 8 Absatz 5, § 26 Absatz 1, § 29 Absatz 4 lit. a, § 31, § 33 Absatz 5, § 35, § 44 Absatz 2 lit. a, b KDG, § 7 Absatz 1 KDG-DVO	Transparenz
B1.9	Identifizierung und Authentifizierung	§ 15 DSG-EKD, § 14 Absatz 6 KDG	Intervenierbarkeit
B1.10	Unterstützung bei der Wahrnehmung von Betroffenenrechten	§ 16 Absatz 2 DSG-EKD / § 14 Absatz 2 KDG	Intervenierbarkeit
B1.11	Berichtigungsmöglichkeit von Daten	§ 5 Absatz 1 Nr. 4, § 20 Absatz 1 DSG-EKD / § 7 Absatz1 lit. d, § 18 KDG	Intervenierbarkeit
B1.12	Löschbarkeit von Daten	§ 21 Absatz 1 DSG-EKD / § 19 Absatz 1 KDG	Intervenierbarkeit
B1.13	Einschränkbarkeit der Verarbeitung von Daten	§ 21 Absatz 4, § 22 DSG-EKD / § 20 KDG	Intervenierbarkeit
B1.14	Datenübertragbarkeit	§ 24 DSG-EKD / § 22 Absatz 1 KDG	Intervenierbarkeit
B1.15	Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen	§ 25 Absatz 1 DSG-EKD, § 24 Absatz 3 KDG	Intervenierbarkeit
B1.16	Fehler- und Diskriminierungsfreiheit beim Profiling	§ 25 Absatz 1 DSG-EKD, § 24 Absatz 3, 4 KDG	Integrität
B1.17	Datenschutzfreundliche Voreinstellungen	§ 28 Absatz 2 DSG-EKD / § 27 Absatz 2 KDG	Datenminimierung, Intervenierbarkeit
B1.18	Verfügbarkeit	§ 27 Absatz 1 Nr. 2 DSG-EKD, § 1 Absatz 1 ITSVO-EKD / § 7 Absatz 1 lit f, § 26 Absatz 1 lit. b KDG, § 6 Absatz1 lit. c KDG-DVO	Verfügbarkeit
B1.19	Belastbarkeit	§ 27 Absatz 1 Nr. 2 DSG-EKD, § 1 Absatz 1 ITSVO-EKD / § 26 Absatz 1 lit. b KDG, § 6 Absatz1 lit. c KDG-DVO	Verfügbarkeit, Integrität, Vertraulichkeit

B1.20	Wiederherstellbarkeit	§ 27 Absatz 1 Nr. 2, 3 DSG-EKD / § 26 Absatz 1 lit. b, c KDG, § 6 Absatz 1, lit. d KDG-DVO	Verfügbarkeit
B1.21	Evaluierbarkeit	§ 27 Absatz 1 Nr. 4 DSG-EKD / § 26 Abs, 1 lit. d KDG, § 7 Absatz 1 KDG-DVO.	Sie ist als ein Prozess umzusetzen, der alle Anforderungen umfasst (siehe Kap. D4 Datenschutzmanagement mit dem KDM).
B1.22	Behebung und Abmilderung von Datenschutzverletzungen	§ 32 Absatz 3 Nr. 4, § 33 Absatz 2 DSG-EKD / § 33 Absatz 3 lit. d, § 34 Absatz 2 KDG.	Integrität, Intervenierbarkeit, Vertraulichkeit, Verfügbarkeit
B1.23	Angemessene Überwachung der Verarbeitung	§ 32 DSG-EKD / § 33 KDG	Transparenz, Integrität
B2	Einwilligungsmanagement	§ 4 Nr. 13, § 11 Nr. 4 DSG-EKD / § 4 Nr. 13, § 8 Absatz 7 KDG	Transparenz, Intervenierbarkeit
B3	Umsetzung aufsichtsbehördlicher Anordnungen	§ 44 Absatz 3 Nr. 2 und Nr. 3, / § 47 Absatz 5 lit. c, § 47 Absatz 6 KDG	Intervenierbarkeit

Teil D: Praktische Umsetzung

D1 Generische Maßnahmen

In diesem Abschnitt werden generische technische und organisatorische Maßnahmen aufgeführt, die in der Datenschutzprüfpraxis 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.

Zudem werden für jede der vom KDM zu betrachtenden Komponente (Daten, Systeme und Dienste sowie Prozesse) für jedes der Gewährleistungsziele in den zugehörigen Bausteinen Referenzmaßnahmen benannt und beschrieben. Für jede der Maßnahmen sind auch die Auswirkungen auf den Erreichungsgrad anderer, von der Maßnahme nicht direkt betroffener Gewährleistungsziele zu betrachten. So können bestimmte Einzelmaßnahmen zur Erreichung mehrerer Gewährleistungsziele beitragen.

Die Anforderung an die Evaluierbarkeit (siehe Abschnitt B1.21) ist nicht in einem Gewährleistungsziel im KDM abzubilden, sondern in einem zyklischen Prozess (Datenschutzmanagementprozess, siehe das Kap. D4 Datenschutzmanagement mit KDM) umzusetzen. Es wird gefordert, dass die technischen und organisatorischen Maßnahmen nicht nur einmalig zu implementieren sind, sondern dass sie regelmäßig auf ihre Wirksamkeit hin zu überprüfen sind. In diesem regelmäßig zu wiederholenden Prozess ist beispielsweise zu prüfen, ob die Maßnahmen noch angemessen sind.

D1.1 Verfügbarkeit

Typische Maßnahmen zur Gewährleistung der Verfügbarkeit sind:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien, Programmstände u. ä.[85] gemäß eines getesteten Konzepts (B1.20 Wiederherstellbarkeit)
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt) (B1.18 Verfügbarkeit, B1.19 Belastbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen),
- Dokumentation der Syntax der Daten (B1.18 Verfügbarkeit, B1.20 Wiederherstellbarkeit),
- Redundanz von Hard- und Software sowie Infrastruktur (B1.20 Verfügbarkeit, B1.19 Belastbarkeit),

[85] im Bereich der Katholischen Kirche in Deutschland gesetzlich geregelt in § 16 Absatz 2 lit. a KDG-DVO; im Bereich der Evangelische Kirche in Deutschland EKD gibt es bis jetzt noch keine für alle Gliedkirchen vergleichbare Regelung, sofern die IT-Sicherheitsverordnung (IT-SVO) nicht als solche angesehen wird. Für den Bereich einzelner ev. Landeskirchen können spezifische Regelungen festgelegt sein.

- Umsetzung von Reparaturstrategien und Ausweichprozessen (B1.19 Belastbarkeit, B1.20 Wiederherstellbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen),
- Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit (B1.19 Belastbarkeit, B1.20 Wiederherstellbarkeit),
- Vertretungsregelungen für abwesende Mitarbeitende (B1.18 Verfügbarkeit).

D1.2 Integrität

Typische Maßnahmen zur Gewährleistung der Integrität oder zur Feststellung von Integritätsverletzungen sind:

- Einschränkung von Schreib- und Änderungsrechten (B1.6 Integrität),
- Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts (B1.6 Integrität, B1.4 Richtigkeit, B1.23 Angemessene Überwachung der Verarbeitung, B1.22 Behebung und Abmilderung von Datenschutzverletzungen),
- dokumentierte Zuweisung von Berechtigungen und Rollen (B1.6 Integrität),
- Löschen oder Berichtigen falscher Daten (B1.4 Richtigkeit),
- Härten von IT-Systemen, so dass diese keine oder möglichst wenige Nebenfunktionalitäten aufweisen (B1.6 Integrität, B1.19 Belastbarkeit),
- Prozesse zur Aufrechterhaltung der Aktualität von Daten (B1.4 Richtigkeit),
- Prozesse zur Identifizierung und Authentifizierung von Personen und Gerätschaften (B1.6 Integrität),
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen (B1.6 Integrität, B1.16 Fehler- und Diskriminierungsfreiheit beim Profiling, B1.19 Belastbarkeit),
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen (B1.6 Integrität, B1.16 Fehler- und Diskriminierungsfreiheit beim Profiling, B1.23 Angemessene Überwachung der Verarbeitung, B1.19 Belastbarkeit),
- Schutz vor äußeren Einflüssen (Spionage, Hacking) (B1.6 Integrität, B1.19 Belastbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen).

D1.3 Vertraulichkeit

Typische Maßnahmen zur Gewährleistung der Vertraulichkeit sind:

- Festlegung eines Rechte- und Rollenkonzeptes nach dem Prinzip der Erforderlichkeit auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle (B1.7 Vertraulichkeit),
- Implementierung eines sicheren Authentifizierungsverfahrens (B1.7 Vertraulichkeit),

- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen (B1.7 Vertraulichkeit),
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle (B1.7 Vertraulichkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen),
- spezifizierte, für die Verarbeitungstätigkeit ausgestattete Umgebungen (Gebäude, Räume) (B1.7 Vertraulichkeit),
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen usw.) (B1.7 Vertraulichkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen),
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept) (B1.7 Vertraulichkeit),
- Schutz vor äußeren Einflüssen (Spionage, Hacking) (B1.7 Vertraulichkeit, Belastbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen).

D1.4 Nichtverkettung

Typische Maßnahmen zur Gewährleistung der Nichtverkettung sind:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten (B1.2 Zweckbindung),
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten (B1.2 Zweckbindung),
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung (B1.2 Zweckbindung),
- Trennung nach Organisations-/Abteilungsgrenzen (B1.2 Zweckbindung),
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentifizierungsverfahrens (B1.2 Zweckbindung),
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle (B1.2 Zweckbindung),
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials[86], Verarbeitung pseudonymer bzw. anonymisierter Daten (B1.2 Zweckbindung),
- geregelte Zweckänderungsverfahren (B1.2 Zweckbindung).

[86] „Credentials“ i. S. v. Referenz bzw. Berechtigungsnachweis z.B. in Anmeldeprozessen zum Erlangen eines Zugriffs auf Daten oder um Daten miteinander zu verbinden

D1.5 Transparenz

Typische Maßnahmen zur Gewährleistung der Transparenz sind:

- Dokumentation im Sinne einer Inventarisierung aller Verarbeitungstätigkeiten[87] (B1.8 Rechenschafts- und Nachweisfähigkeit),
- Dokumentation der Bestandteile von Verarbeitungstätigkeiten insbesondere der Geschäftsprozesse, Datenbestände, Datenflüsse und Netzpläne, dafür genutzte IT-Systeme, Betriebsabläufe, Beschreibungen von Verarbeitungstätigkeiten, Zusammenspiel mit anderen Verarbeitungstätigkeiten (B1.8 Rechenschafts- und Nachweisfähigkeit),
- Dokumentation von Tests, der Freigabe und ggf. der Datenschutz-Folgenabschätzung von neuen oder geänderten Verarbeitungstätigkeiten (B1.8 Rechenschafts- und Nachweisfähigkeit),
- Dokumentation der Faktoren, die für eine Profilbildung, zum Scoring oder für teilautomatisierte Entscheidungen genutzt werden (B1.8 Rechenschafts- und Nachweisfähigkeit),
- Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen (B1.8 Rechenschafts- und Nachweisfähigkeit),
- Dokumentation von Einwilligungen, deren Widerruf sowie Widersprüchen (B2 Einwilligungsmanagement),
- Protokollierung von Zugriffen und Änderungen (B1.23 Angemessene Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit),
- Versionierung (B1.23 Angemessene Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit),
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts (B1.23 Angemessene Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit),
- Dokumentation der Quellen von Daten, bspw. des Umsetzens der Informationspflichten gegenüber Betroffenen, wo deren Daten erhoben wurden sowie des Umgangs mit Datenpannen (B1.1 Transparenz für Betroffene, B1.8 Rechenschafts- und Nachweisfähigkeit),
- Benachrichtigung von Betroffenen bei Datenpannen oder bei Weiterverarbeitungen zu einem anderen Zweck (B1.1 Transparenz für Betroffene),
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte (B1.1 Transparenz für Betroffene),
- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept (B1.1 Transparenz für Betroffene),

[87] Kap. 3 DSG-EKD / Kap. 3 KDG

- Bereitstellung von Informationen über die Verarbeitung von personenbezogenen Daten an Betroffene (B1.1 Transparenz für Betroffene).

D1.6 Intervenierbarkeit

Typische Maßnahmen zur Gewährleistung der Intervenierbarkeit sind:

- Maßnahmen für differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten (B2 Einwilligungsmanagement),
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen (B1.11 Berichtigungsmöglichkeit von Daten, B1.13 Einschränkbarkeit der Verarbeitung, B1.17 Datenschutz durch Voreinstellungen, B2 Einwilligungsmanagement, B3 Umsetzung aufsichtsbehördlicher Anordnungen),
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an Verarbeitungstätigkeiten sowie an den technischen und organisatorischen Maßnahmen (B1.22 Behebung und Abmilderung von Datenschutzverletzungen, B1.13 Einschränkbarkeit der Verarbeitung, B3 Umsetzung aufsichtsbehördlicher Anordnungen),
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem (B1.22 Behebung und Abmilderung von Datenschutzverletzungen, B1.13 Einschränkbarkeit der Verarbeitung, B3 Umsetzung aufsichtsbehördlicher Anordnungen),
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten),
- Betreiben einer Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten, B1.14 Datenübertragbarkeit),
- Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten (B1.9 Identifizierung und Authentifizierung),
- Einrichtung eines Single Point of Contact (SPoC), Kontaktmöglichkeit für Betroffene (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten),
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten (B1.11 Berichtigungsmöglichkeit von Daten, B1.12 Löschbarkeit von Daten, B1.13 Einschränkbarkeit der Verarbeitung von Daten, B1.14 Datenübertragbarkeit, B3 Umsetzung aufsichtsbehördlicher Anordnungen),
- Bereitstellen von Optionen für Betroffene, um Programme datenschutzgerecht einstellen zu können (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten, B1.17 Datenschutz durch Voreinstellung).

D1.7 Datenminimierung

Das Gewährleistungsziel Datenminimierung kann erreicht werden durch:

- Reduzierung von erfassten Attributen der betroffenen Personen (B1.3 Datenminimierung),
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten (B1.3 Datenminimierung),
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten (B1.3 Datenminimierung),
- Festlegung von Voreinstellungen für betroffene Personen, die die Verarbeitung ihrer Daten auf das für den Verarbeitungszweck erforderliche Maß beschränken. (B1.17 Datenschutz durch Voreinstellungen),
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen (B1.3 Datenminimierung),
- Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren (B1.3 Datenminimierung, B1.5 Speicherbegrenzung),
- Festlegung und Umsetzung eines Löschkonzepts (B1.5 Speicherbegrenzung),
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten (B1.3 Datenminimierung).

D1.8 Gewährleistungsziele als Design-Strategie

Bereits bei der Konzeptionierung von Verarbeitungstätigkeiten müssen die Anforderungen[88] des DSG-EKD und des KDG berücksichtigt werden. Der dort formulierte Grundsatz des Datenschutzes durch Technikgestaltung („Data Protection by Design“) und datenschutzfreundlicher Voreinstellungen („Data Protection by Default“) verlangt eine Beachtung der Datenschutzanforderungen für den späteren Betrieb bereits während der Planungsphase einer Verarbeitung. Demnach sollen technische und organisatorische Maßnahmen nicht erst nachträglich festgelegt und umgesetzt werden, um ggf. nicht rechtskonforme Funktionalitäten abzustellen. Datenschutzfreundliche Voreinstellungen verlangen auch, dass eine Fachapplikation von vornherein datenschutzkonform konfiguriert werden muss. Diese Grundsätze schließen das Prinzip der Datenminimierung als Design-Strategie ein.

Zur datenschutzgerechten Gestaltung der Funktionen der Verarbeitungstätigkeiten im Sinne von „Data Protection by Design“ können die Gewährleistungsziele des KDM als Design-Prinzip oder Design-Strategie interpretiert werden.

[88] § 28 DSG-EKD / § 27 KDG

So verlangt das Gewährleitungsziel **Datenminimierung**, dass nicht mehr und nicht andere Daten erhoben werden als vom Zweck gedeckt sind. Datenschutzfreundliche Voreinstellungen sollen dazu führen, dass standardmäßig nur die personenbezogenen Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit[89]. Die Gewährleistungsziele Datenminimierung und **Nichtverkettung** sind schon durch entsprechendes Design der für die Verarbeitung erforderlichen Informationstechnik umsetzbar. Beispielsweise muss der Funktionsumfang einer Fachapplikation allein auf die erforderlichen Funktionen reduziert werden. Zur Umsetzung des Gewährleistungsziels **Intervenierbarkeit** muss sichergestellt werden, dass die Betroffenenrechte tatsächlich von der Fachapplikation und allen weiteren IT-Diensten, die diese Applikation bspw. auf der Ebene der Infrastruktur nutzen, umsetzbar sind. Dies erfordert auch ausgereifte Changemanagement-Prozesse der Organisation. Diese Prozesse sind auch erforderlich, um auf Änderungen der rechtlichen Rahmenbedingungen reagieren zu können oder um neue, datenschutzfreundlichere Techniken in vorhandenen Verarbeitungen einsetzen zu können. Die Umsetzung des Gewährleitungsziels **Transparenz** bedeutet, dass von vornherein darauf geachtet wird, dass alle an Verarbeitungstätigkeiten direkt oder indirekt Beteiligten bzw. von diesen Betroffenen (Verantwortliche, Auftragsverarbeiter, die betroffenen Personen und Aufsichtsbehörden) entsprechend ihrer speziellen Interessen die Verarbeitungstätigkeiten prüfen können.

D2 Verarbeitungstätigkeiten

Das DSG-EKD wie auch das KDG verwenden jeweils[90] „Verarbeitungstätigkeit“ als zentralen Begriff des Datenschutzmanagements und definieren den Begriff der „Verarbeitung“[91]:

„Im Sinne dieses […]Gesetzes [DSG-EKD/KDG] bezeichnet der Ausdruck […]„Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; […]“

DSG-EKD und KDG listen in § 31 die Angaben auf, die in das Verzeichnis der Verarbeitungstätigkeiten, das von Verantwortlichen oder Auftragsverarbeitern zu führen ist, aufzunehmen sind. Genannt werden dort u. a.:

[89] vgl. § 28 Absatz 2 DSG-EKD / § 27 Absatz 2 KDG
[90] § 31 DSG-EKD / § 31 KDG
[91] § 4 Nr. 3 DSG-EKD / § 4 Absatz 3 KDG

- Namen und die Kontaktdaten des oder der Verantwortlichen, und ggf. des oder der gemeinsam mit ihm Verantwortlichen sowie des Datenschutzbeauftragten,
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien betroffener Personen, personenbezogener Daten und Empfänger sowie ggfs. die Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation,
- die vorgesehenen Fristen für die Löschung,
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen[92].

Diese allgemeine Beschreibung einer Verarbeitung stellt noch keine ausreichende Dokumentation von Verarbeitungstätigkeiten dar und erfüllt allein noch nicht die Anforderungen an den Grundsatz der Transparenz.[93]

Die Funktion der vollständigen Dokumentation einer Verarbeitung besteht darin, dass alle relevanten Komponenten einer Verarbeitungstätigkeit aufgrund der bestehenden Rechenschaftspflicht prüffähig sind, um diese einer datenschutzrechtlichen Beurteilung unterziehen zu können. Prüffähigkeit bedeutet dabei, dass die Funktionen aller Bestandteile einer Verarbeitungstätigkeit, insbesondere in den Bereichen der elektronischen Datenverarbeitung und Kommunikation, einer Soll-Ist-Bilanzierung zugänglich sind.

Diese Prüfbilanz bezüglich funktionaler Eigenschaften sowie der getroffenen technischen und organisatorischen Maßnahmen der Verarbeitungstätigkeit muss dann wiederum einer rechtlichen Beurteilung der Rechtskonformität bzw. Ordnungsmäßigkeit insgesamt unterzogen werden können unter der Fragestellung, ob die richtigen Maßnahmen zweckgemäß ausgewählt und mit der korrekten Wirkintensität betrieben werden.

D2.1 Ebenen einer Verarbeitung bzw. Verarbeitungstätigkeit

Um eine personenbezogene Verarbeitung vollständig zu erfassen, hat es sich bewährt, bei der Gestaltung oder Prüfung von Verarbeitungstätigkeiten zumindest drei verschiedene Ebenen der Darstellung wesentlicher Einflussgrößen oder Bestandteile zu unterscheiden. Wesentlich ist das Verständnis, dass eine „Verarbeitungstätigkeit“ bspw. nicht deckungsgleich mit der Verwendung einer bestimmten Technik oder eines bestimmten Fachprogramms ist.

[92] hierzu insbesondere § 27 DSG-EKD / § 26 KDG
[93] § 5 Absatz 2 DSG-EKD / § 7 Absatz 2 KDG

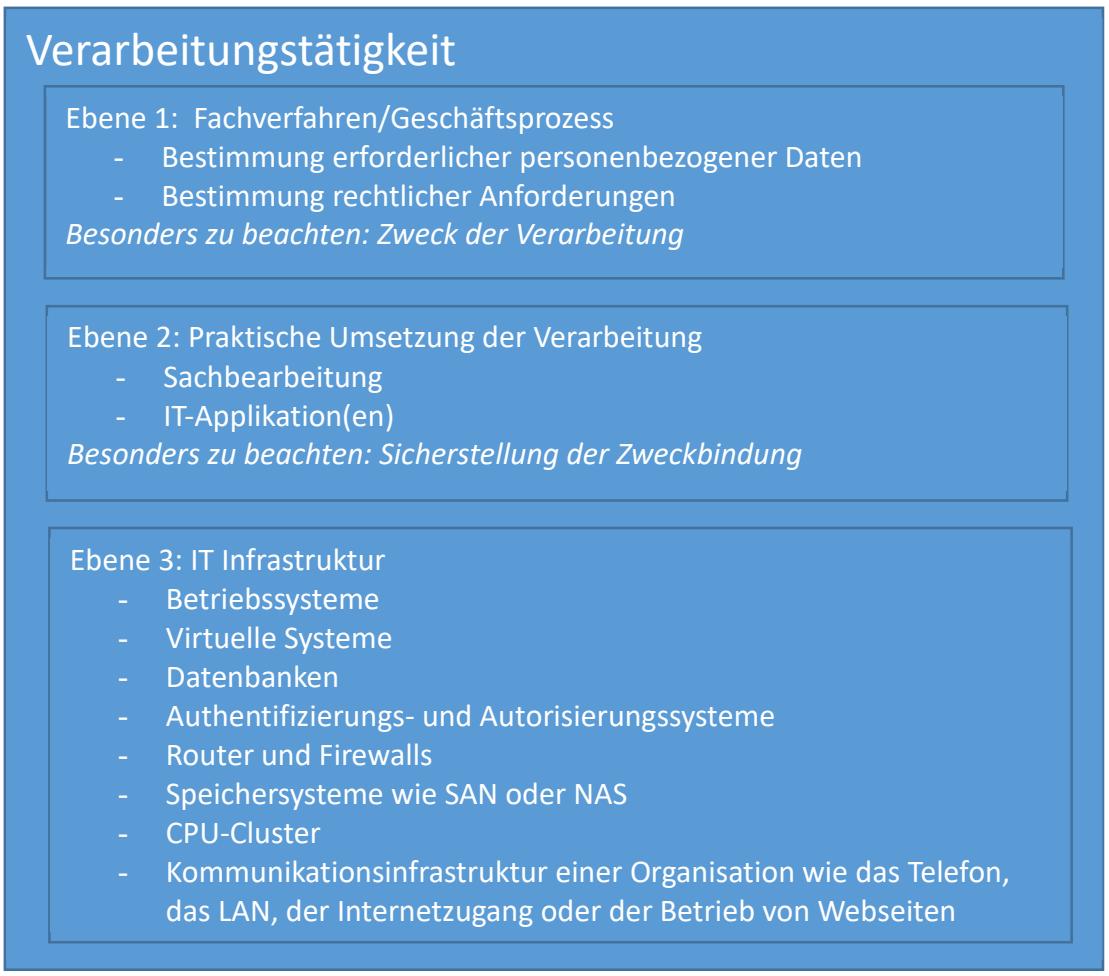


Abbildung: Erfassung von Verarbeitungstätigkeiten anhand der Ebenen gemäß Abschnitt D 2.1

Auf der **Ebene 1** ist eine personenbezogene Verarbeitung im datenschutzrechtlichen Sinne angesiedelt. Diese Verarbeitung findet bspw. im Rahmen einer kirchlichen, diakonischen oder caritativen Stelle oder Einrichtung statt, für deren Aktivitäten der bzw. die Verantwortliche verantwortlich ist. Diese Ebene entspricht dem, was vielfach als ein „Fachverfahren“ und „Geschäftsprozess“ mit einem bestimmten funktionalen Ablauf der Verarbeitungstätigkeit verstanden wird. Auf dieser Ebene des Verständnisses einer Verarbeitung werden die für eine Verarbeitungstätigkeit erforderlichen personenbezogenen Daten sowie die gesetzlichen Anforderungen bestimmt. Der bzw. die Verantwortliche definiert entsprechende Rollen und Berechtigungen an den personenbezogenen Daten und bestimmt die zu verwendenden IT-Systeme und Prozesse. Wesentlich für die datenschutzrechtlich angemessen funktionale Gestaltung dieser Ebene ist die **Bestimmung des Zwecks** oder der Zwecke der Verarbeitungstätigkeit.

Auf der **Ebene 2** ist die praktische Umsetzung der Verarbeitung und des Zwecks angesiedelt. Diese umfasst zum einen in der Regel die Rolle der Sachbearbeitung sowie die IT-Applikation(en), die sich genauer auch als „Fachapplikation eines Fachverfahrens“ bezeichnen lässt. Die Sachbearbeitung und die Fachapplikation müssen die funktionalen und (datenschutz-)rechtlichen Anforderungen, denen die Verarbeitung unterliegt, vollständig erfüllen. Die **Fachapplikation muss die Zweckbindung sicherstellen**. Die Applikation muss die

Verarbeitung zusätzlicher Daten oder zusätzliche Verarbeitungsformen ausschließen, selbst wenn sie funktional besonders komfortabel sein mögen. Damit soll das Risiko minimiert werden, dass sie die Zweckbindung unterlaufen oder der Zweck überdehnt wird.

Auf der **Ebene 3** ist die IT-Infrastruktur angesiedelt, die Funktionen bereitstellt, die eine Fachapplikation der Ebene 2 nutzt. Zu dieser Ebene an „technischen Services" zählen Betriebssysteme, virtuelle Systeme, Datenbanken, Authentifizierungs- und Autorisierungssysteme, Router und Firewalls, Speichersysteme wie SAN oder NAS, CPU-Cluster, sowie die Kommunikationsinfrastruktur einer Organisation wie das Telefon, das LAN, der Internetzugang oder der Betrieb von Webseiten. Auch hier gilt, dass diese Systeme innerhalb einer Verarbeitungstätigkeit jeweils so zu gestalten und zu nutzen sind, dass die **Zweckbindung erhalten** bleibt. Damit die Zweckbindung bzw. Zwecktrennung auf dieser Ebene durchgesetzt werden kann, müssen typischerweise technische und organisatorische Maßnahmen getroffen werden.

D2.2 Zweck

Ob eine Verarbeitung einem legitim gesetzten Zweck folgt und ob der Zweck der Verarbeitung hinreichend bestimmt ist, muss vor der Anwendung des KDM geklärt sein (siehe Abschnitt D4.2).

Bei der Umsetzung des spezifischen Zwecks einer Verarbeitung hat es sich bewährt, zwei weitere Aspekte zu beachten, um auch zu einer hinreichenden Zweckbindung der Verarbeitungstätigkeit zu gelangen:

- Zusätzlich zur Zweckbestimmung sind die Aspekte der **Zweckabgrenzung** bzw. der **Zwecktrennung** zu betrachten. So sollte festgelegt werden, welche (verwandte) Zwecke nicht mit der Verarbeitungstätigkeit umgesetzt werden sollen. Das erleichtert eine rechtskonforme Abtrennung der Verarbeitungstätigkeiten untereinander sowie insbesondere die Trennung von Datenbeständen, Systemen und Diensten sowie Prozessen auf der IT-Ebene.
- Es ist auch der Aspekt der **Zweckbindung** zu beachten. Die Zweckbindung einer Verarbeitung muss einerseits durch deren geeignete Funktionalität und durch geeignete Auswahl der zu verarbeitenden Produktions- oder Nutzdaten sichergestellt werden (horizontale Gestaltung). Die Zweckbindung einer Verarbeitung muss aber auch durch eine geeignete, die Ebenen übergreifende Gestaltung (siehe Abschnitt D2.1) sichergestellt werden (vertikale Gestaltung). So ist es in der Regel nicht vom Zweck abgedeckt und operativ auch nicht notwendig, dass neben den befugten Sachbearbeitern und deren Vorgesetzte auch noch IT-Administratoren, die beispielsweise auf der Ebene einer Datenbank die Zugriffsrechte verwalten, Kenntnis von den Inhalten der Verarbeitungsdaten nehmen können.

D2.3 Komponenten einer Verarbeitung bzw. Verarbeitungstätigkeit

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

1. die personenbezogenen **Daten**,
2. die beteiligten technischen **Systeme und Dienste** (Hardware, Microservices, Software und Infrastruktur),
3. die technischen, organisatorischen und personellen **Prozesse** der Verarbeitung von Daten.

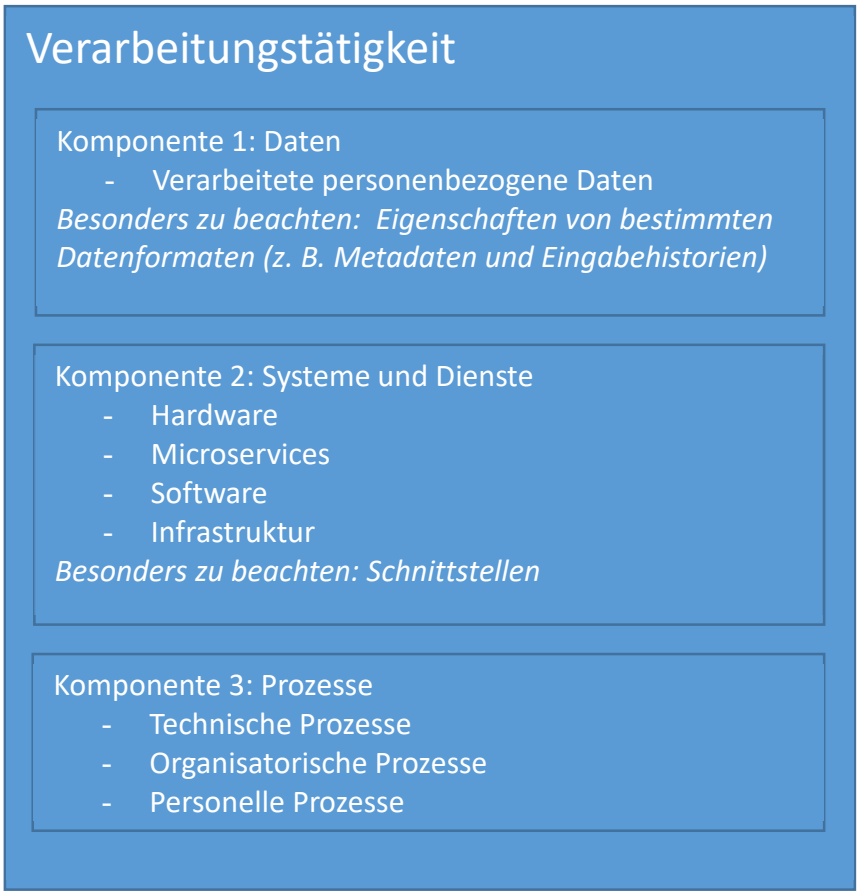


Abbildung: Modellierung von Verarbeitungstätigkeiten anhand der Komponenten gemäß Abschnitt D 2.3

Der Ausdruck „Prozess“ ist im DSG-EKD / im KDG nicht ausdrücklich enthalten. Jede Verarbeitungstätigkeit kann als Geschäftsprozess bzw. Fachverfahren modelliert werden; jede Verarbeitungstätigkeit besteht aus einzelnen Verarbeitungsschritten. Einzelne Verarbeitungen sind bspw. das Erheben, Erfassen, Ordnen oder Speichern bis zum Löschen oder Vernichten[94]. Diese Verarbeitungen werden als Teilprozesse modelliert bzw. implementiert.

[94] vgl. § 4 Nr. 3 DSG-EKD / § 4 Nr. 3 KDG

Methodisch stehen zunächst die Daten von Personen im Vordergrund, deren Erforderlichkeit der Verarbeitung an der Zweckbestimmung vorab zu bemessen ist.

Die konkrete funktionale Gestaltung geschieht auf der Ebene 1 (siehe D2.1), auf der anhand der Daten der Schutzbedarf durch die verantwortliche Stelle festzustellen bzw. festzusetzen ist. Diesen Schutzbedarf erben alle Daten, Systeme und Prozesse, die bei einer konkreten Verarbeitung auf den verschiedenen Ebenen zum Einsatz kommen. Anhand des Referenzmaßnahmenkatalogs kann überprüft werden, ob getroffene oder geplante technische und organisatorische Maßnahmen dem Schutzbedarf angemessen sind.

Bei diesen drei Kernkomponenten Daten, Systeme und Dienste sowie Prozesse spielen u. a. folgende spezielle Eigenschaften noch eine weitere zu beachtende Rolle:

Bei Daten sind Eigenschaften von **Datenformaten** zu betrachten, mit denen Daten erhoben und verarbeitet werden. Datenformate können Einfluss auf die Qualität der Umsetzung der Gewährleistungsziele haben, z. B. in den Fällen, in denen nicht als abschließend geklärt gelten darf, welche Inhalte Dateien mit bestimmten Formaten aufweisen. So können im Datenbestand von Textdateien vermeintlich gelöschte Daten enthalten sein, die im Ausdruck nicht erscheinen; Grafikdateien können Metadaten bspw. bzgl. Kameramodell, Ort und Zeit der Aufnahme enthalten oder es können wiederum relevante Informationen bei Grafik-, Video- und Audiodateien der Kompression zum Opfer fallen.

Bei den beteiligten Systemen sind die **Schnittstellen** zu betrachten, die eine Fachapplikation mit der Nutzung von IT-Systemen der Ebene 3 sowie insbesondere zu anderen Systemen, die nicht innerhalb der vom Zweck definierten Systemgrenze liegen, aufweist. Neben diesen vertikalen Schnittstellen sind auch horizontale Schnittstellen zu betrachten, mit denen ein Risiko für die Zweckbindung einhergeht. Der Ausweis der Existenz von Schnittstellen sowie die Dokumentation von deren Eigenschaften sind von entscheidender Bedeutung für die rechtliche Verantwortlichkeit, Beherrschbarkeit und Prüfbarkeit von Datenflüssen.

Für jede Verarbeitungstätigkeit und deren Komponenten, insbesondere für die manchmal schwierig fassbaren Prozesse über verschiedene Systeme hinweg gilt, die **Verantwortlichkeit** zu verdeutlichen und im Verzeichnis der Verarbeitungstätigkeiten[95] zu dokumentieren. Nach der gesetzlichen Begriffsbestimmung[96], ist ein Verantwortlicher „(…) eine natürliche oder juristische Person, Behörde oder Einrichtung (…), die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet; (…).“ Aufgaben, die aus der Verantwortlichkeit resultieren, können in Form von individuellen Zuständigkeiten delegiert werden. Diese Zuständigkeiten werden typischerweise als Rollen in einem umfassenden Berechtigungs- und Rollenkonzept formuliert und zugewiesen. Die Zuständigkeit eines Prozesseigentümers kann sich auf einzelne Verarbeitungen (Teilprozesse) oder auf die gesamte Verarbeitungstätigkeit über alle Prozessebenen hinweg im Sinne einer Gesamtzuständigkeit erstrecken. Diese Zuständigkeit kann auf unterschiedliche Rollen mit

[95] § 31 DSG-EKD / § 31 KDG
[96] § 4 Nr. 9 DSG-EKD / § 4 Nr. 9 KDG

jeweils Teilzuständigkeiten verteilt werden. Wenn die Verarbeitungstätigkeit eine Auftragsverarbeitung[97] beinhaltet, ist zu gewährleisten, dass der Auftragsverarbeiter seine Aufgaben gemäß den Weisungen des oder der Verantwortlichen datenschutzkonform erfüllt.

Die Verantwortung für eine Verarbeitung liegt immer bei den Verantwortlichen der Organisation, die diese Verarbeitung betreiben.

D3 Risiken und Schutzbedarf

Das kirchliche Datenschutzrecht knüpft die Anforderungen an technische und organisatorische Maßnahmen an das mit der Verarbeitung der personenbezogenen Daten verbundene Risiko für die Rechte und Freiheiten betroffener Personen.

Ein Risiko im Sinne der kirchlichen Normen ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das einen Schaden für die Rechte und Freiheiten natürlicher Personen (einschließlich ungerechtfertigter Beeinträchtigung der Rechte und Freiheiten) darstellt oder zu einem Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens für die Rechte und Freiheiten der betroffenen Personen und zweitens die Wahrscheinlichkeit, dass das Ereignis und der Schaden eintreten.

Schäden für die Rechte und Freiheiten natürlicher Personen können physischer, materieller oder immaterieller Natur sein. Im Folgenden wird allgemein von Schadensereignissen gesprochen. Unrechtmäßige Verarbeitungstätigkeiten, stellen in sich bereits ein Schadensereignis dar. Sie können zusätzliche Schäden wie bspw. die Diskriminierung natürlicher Personen nach sich ziehen.

Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden.

Aufgabe des oder der Verantwortlichen ist, diese Risiken zu identifizieren, zu analysieren und einzustufen und Maßnahmen zu deren Eindämmung zu treffen sowie diese kontinuierlich auf ihre Wirksamkeit zu überprüfen (siehe Kapitel D4 Datenschutzmanagement mit dem KDM).

Dieses Kapitel D3 gibt Hilfestellungen, um die Risiken einer Verarbeitung im Hinblick auf den Datenschutz einer Verarbeitungstätigkeit zu bestimmen. Es stellt außerdem den Zusammenhang her zwischen den Risiken durch eine Verarbeitungstätigkeit und dem Schutzbedarf natürlicher Personen bei der Verarbeitung personenbezogener Daten einerseits und dem durch die implementierten Maßnahmen erreichten Schutzniveau bzw. dem Restrisiko einer Verarbeitungstätigkeit andererseits, mit dem Ziel, die Bestimmung geeigneter und angemessener Maßnahmen zu ermöglichen. Die Bestimmung der Höhe des Risikos ist die

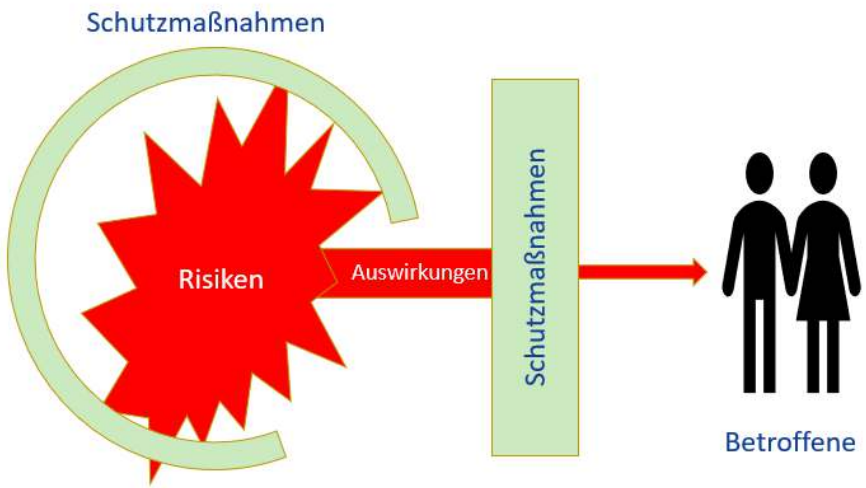
[97] § 30 DSG-EKD / § 29 KDG

Voraussetzung dafür, technische und organisatorische Maßnahmen und den notwendigen Grad ihrer Wirksamkeit festlegen zu können, mit denen sich Risiken eliminieren oder zumindest reduzieren lassen und eine Verarbeitung datenschutzkonform erfolgen kann. Grundsätzlich gilt die Regel: Je höher das Risiko, desto umsichtiger muss die Verarbeitungstätigkeit gestaltet sein und desto wirksamer müssen die entsprechenden, konkreten technischen und organisatorische Maßnahmen betrieben, kontrolliert und ggf. verbessert werden.

D3.1 Risiken für Betroffene

a) Ausgangspunkt von Überlegungen zum Risiko ist die Verarbeitungstätigkeit, die aus einem oder mehreren Verarbeitungsvorgängen besteht. Es wird der Begriff „Verarbeitungstätigkeit[98]“ verwendet, denn nach der Definition sind Verarbeitungen einzelne Vorgänge oder Vorgangsreihen. Für jede Verarbeitungstätigkeit müssen die Grundsätze der Verarbeitung personenbezogener Daten beachtet werden. Das KDM „verdichtet“ diese Grundsätze zu Gewährleistungszielen, die weitere operative Anforderungen der kirchlichen Datenschutzgesetze aufnehmen.

Im Bereich des Datenschutzes besteht daher grundsätzlich die Pflicht die entstehenden Risiken mit geeigneten und angemessenen technischen und organisatorischen Maßnahmen auf ein angemessenes Schutzniveau zu reduzieren. Spielraum besteht bei der Auswahl und der Art und Weise der Umsetzung von Anforderungen mit Hilfe von technischen und organisatorischen Maßnahmen, die in einem angemessenen Umfang gefordert[99] werden. Maßnahmen können gegen die Auswirkungen eines Risikos gerichtet sein oder die Eintrittswahrscheinlichkeit des Schadens begrenzen oder abwenden. Hier ist es geboten, bestehende Risiken für die Rechte und Freiheiten natürlicher Personen genauer zu analysieren.



[98] § 31 DSG-EKD / § 31 KDG u. § 4 Nr. 3 DSG-EKD / § 4 Nr. KDG
[99] § 5 Nr. 4 „angemessene Maßnahmen“ und Nr. 6 „angemessene Sicherheit“ DSG-EKD / § 26 Absatz 1-3 KDG

Abbildung: Schutzmaßnahmen können gegen das Risiko an sich gerichtet sein oder gegen die Auswirkungen des eingetretenen Schadens auf Betroffene

Erst wenn ein angemessenes Schutzniveau erreicht wurde, können die Restrisken vom Verantwortlichen als akzeptabel für den Betroffenen eingeschätzt werden

b) Die kirchlichen Datenschutzgesetze verlangen von den Verantwortlichen, bei einem „voraussichtlich hohen Risiko“ für die Rechte und Freiheiten natürlicher Personen eine Datenschutz-Folgenabschätzung (DSFA) [100] für die vorgesehene Verarbeitung durchzuführen.

Zur Bestimmung der Höhe des Risikos muss der bzw. die Verantwortliche daher zunächst eine „Schwellwertanalyse“ (Abgrenzung zwischen voraussichtlich normalem und hohem Risiko) durchführen. Diese Analyse muss für jede Verarbeitungstätigkeit, bestehend aus einem oder mehreren Verarbeitungsvorgängen, durchgeführt werden, um die Entscheidung für die Einstufung einer Verarbeitungstätigkeit gegenüber einer zuständigen Datenschutzaufsichtsbehörde begründen zu können.[101] Es wird empfohlen, innerhalb der Schwellwertanalyse zu prüfen, ob die vorgesehene Verarbeitungstätigkeit in der „Muss-Liste“ der Datenschutzaufsichtsbehörden enthalten ist[102], zu den besonders riskanten Verarbeitungstätigkeiten zählt[103], ein oder mehrere der neun Kriterien des Working Paper 248 rev. 01 des Europäischen Datenschutzausschusses erfüllt[104] oder Art, Umfang, Umstände oder Zwecke der Verarbeitungstätigkeit das Risiko für betroffene Personen erhöhen[105].

D3.2 Risikoanalyse und Risikobehandlung

Die Risikoidentifizierung, -bewertung und -behandlung wird in der gesonderten Anlage „Richtlinie zur Risikoanalyse und Risikobehandlung“ ausführlich behandelt.

D4 Datenschutzmanagement

Das Datenschutzmanagement ist eine umfassende Methode, um systematisch alle Anforderungen des Datenschutzrechts in einer Organisation umzusetzen. Im Folgenden wird ein Datenschutzmanagement im Zusammenspiel mit dem KDM näher beschrieben.

D4.1 Rechtliche Grundlagen des Datenschutzmanagements

Die Verantwortlichen sind für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und müssen den Nachweis darüber erbringen können. Konkret müssen Verantwortliche ein Verzeichnis[106] führen, in dem die personenbezogenen Verarbeitungstätigkeiten der Organisationen aufgelistet sind. Zudem

[100] § 34 DSG-EKD / § 35 KDG
[101] § 5 Absatz 2 DSG-EKD / § 7 Absatz 2 KDG
[102] § 34 Absatz 5 DSG-EKD / § 35 Absatz 5 KDG
[103] § 34 Absatz 3 DSG-EKD / § 35 Absatz 4 KDG
[104] Working Paper 248 rev. 01 des Europäischen Datenschutzausschusses vom 4. Oktober 2017, III B a) 1. bis 9.
[105] § 34 Absatz 1 DSG-EKD / § 35 Absatz 1 KDG, siehe auch Erwägungsgrund 76 DSGVO
[106] § 31 DSG-EKD / § 31 KDG „Verzeichnis der Verarbeitungstätigkeiten“

müssen sie bereits zum Zeitpunkt der Spezifikation der Verarbeitung[107] geeignete technische und organisatorische Maßnahmen treffen. Für Verarbeitungstätigkeiten, die ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, müssen sie darüber hinaus eine Datenschutz-Folgenabschätzung[108] (DSFA) durchführen. Aber auch ohne DSFA müssen geeignete technische und organisatorische Maßnahmen bestimmt und dauerhaft umgesetzt werden, um ein dem Risiko angemessenes Schutzniveau bei jeder Verarbeitung zu gewährleisten. Schließlich müssen die Verantwortlichen die Umsetzung und die Wirksamkeit der Maßnahmen nachweisen, evaluieren und ggf. verbessern können und auf diese Weise aktuell halten.

Damit die Verantwortlichen den detaillierten Anforderungen in Bezug auf die operative Umsetzung der Betroffenenrechte und ihren Rechenschafts- und Nachweispflichten nachkommen können, ist eine systematische Vorgehensweise bei der Prüfung und Beurteilung erforderlich. Diese Rechenschafts- und Nachweispflicht ist eine dauerhafte Aufgabe für die Verantwortlichen und sollte daher als dauerhafter, zyklischer Prozess etabliert werden. Mit dem aus dem Qualitätsmanagement bekannten und bewährten PDCA-Zyklus (Plan, Do, Check, Act) steht ein kontinuierlicher Verbesserungsprozess in vier Phasen zur Verfügung, der die Grundlage für den hier beschriebenen Datenschutzmanagementprozess (DSM-Prozess) bildet.

Der DSM-Prozess dient somit einerseits den Verantwortlichen bei der systematischen Planung, dem dauerhaften Betrieb, der regelmäßigen Überprüfung der Datenschutzkonformität und der Verbesserung von Verarbeitungstätigkeiten. Er schafft somit Transparenz für die Verantwortlichen. Andererseits hilft der DSM-Prozess auch der Datenschutzaufsichtsbehörde bei der Beratung von Verantwortlichen und bei der datenschutzrechtlichen Prüfung dieser Verarbeitungstätigkeiten.

D4.2 Vorbereitungen

Vor dem Start des DSM-Zyklus sind ebenso wie vor der Anwendung des KDM die folgenden drei 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, [109]
3. Weitere materiellrechtliche Beurteilungen der Rechtmäßigkeit dieser Verarbeitung.

Zur Feststellung der sachlichen Verhältnisse bei der oder dem Verantwortlichen der Verarbeitungstätigkeit sind beispielsweise folgende Fragen zu klären:

- Welche Stellen sind an der Verarbeitung beteiligt?
- Wer trägt für welche Teile der Verarbeitung die Verantwortung?

[107] § 28 Absatz 1 DSG-EKD / § 27 Absatz 1 KDG „Datenschutz durch Technikgestaltung“
[108] § 34 DSG-EKD / § 35 KDG
[109] Zur Differenzierung zwischen Zulässigkeit und Rechtmäßigkeit s. Kapitel A1.

- 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 Verarbeitungstätigkeit betrieben?

Im Rahmen der Prüfung der Zulässigkeit der Verarbeitung ist die Rechtsgrundlage für die Verarbeitung zu bestimmen. Dazu können bei der Verarbeitung personenbezogenen Daten[110] insbesondere die folgenden aus dem Gesetz abgeleiteten Fragen[111] herangezogen werden:

- Bilden Einwilligungen der Betroffenen die Rechtsgrundlage der Verarbeitungstätigkeit?
- Ist die Verarbeitung für die Erfüllung eines Vertrags 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 der bzw. die Verantwortliche unterliegt?
- 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?

Die materiellrechtliche Bewertung beurteilt, inwieweit eine von den Verantwortlichen geplante und gegebenenfalls von der Aufsichtsbehörde zu prüfende Verarbeitungstätigkeit grundsätzlich zulässig ist. Darüber hinaus gibt sie Antworten insbesondere auf die folgenden Fragen, die die Anwendung des KDM vorbereiten:

- Welches kirchliche oder ggf. auch weltliche Datenschutzrecht ist auf die Verarbeitung anzuwenden?
- Welche legitimen Zwecke können mit der Verarbeitung verfolgt werden und welche Zweckänderungen sind im 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 beteiligten Stellen sowie von diesen an Dritte?

[110] Werden besondere Kategorien personenbezogener Daten verarbeitet, ist zudem Art. 9 DSGVO zu beachten.
[111] § 6 DSG-EKD / § 6 KDG

- Sind die erforderlichen Vereinbarungen getroffen, wenn mehrere Verantwortliche in die Verarbeitungstätigkeit involviert sind und gemeinsam verantwortlich[112] sind?
- Sind Auftragsverarbeiter[113] 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?

Ausführlichkeit und Detaillierungsgrad insbesondere der Feststellungen zu den sachlichen Verhältnissen werden von Verarbeitung zu Verarbeitung variieren, ebenso wie der Grad der Formalisierung des Vorgehens. Eine strukturierte Zusammenfassung der Ergebnisse ist unabhängig davon ebenso üblich wie für die weiteren Schritte unentbehrlich. Die Feststellungen zu den sachlichen Verhältnissen gehen in die Phase 1 „Planen/Spezifizieren“ des DSM-Zyklus ein.

D4.3 Spezifizieren und Prüfen

Grundlegende Voraussetzung für ein Spezifizieren (siehe Abschnitt D4.5.1) und ein späteres Prüfen (siehe Abschnitt D4.5.3) ist die Festlegung, wie die Gewährleistungsziele für die betrachtete Datenverarbeitung operationalisiert werden.

In Abhängigkeit vom festgestellten Risiko (siehe dazu auch Abschnitt D3) und unter Bezug auf die konkreten rechtlichen Anforderungen sind die aus den jeweiligen Gewährleistungszielen resultierenden Eigenschaften der Verarbeitungstätigkeit qualitativ näher zu bestimmen:

- **Verfügbarkeit** *Innerhalb von welchen Prozessen ist für wen die Verfügbarkeit von welchen Daten zu gewährleisten? Innerhalb welcher Zeiten müssen Daten für wen verfügbar und ggf. wiederherstellbar sein?* Der Einfluss der ordnungsgemäßen Verwendung der Daten auf die Interessen der Betroffenen ist der Maßstab für die Konkretisierung des Gewährleistungsziels der Verfügbarkeit.
- **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 gesetzten Zweck entsprechend korrekt geplant, betrieben und kontrolliert werden? Auch hier ist das Interesse der Betroffenen der Maßstab.
- **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 Geschäftsprozessen abzuleiten. Hiermit ist der Rahmen bestimmt, innerhalb dessen sich die Maßnahmen zum Vertraulichkeitsschutz gegenüber unbefugten Beschäftigten der Verantwortlichen zu bewegen haben. Der

[112] § 29 DSG-EKD / § 28 KDG
[113] § 30 DSG-EKD / § 29 KDG

Rahmen für die Kenntnisnahme Dritter ist durch die in der materiell-rechtlichen Analyse festgestellten Übermittlungsbefugnisse gegeben.

- **Transparenz** *Wie und in welcher Form ist die Datenverarbeitung gegenüber betroffenen Personen und Aufsichtsbehörden transparent zu halten?* Es sind Anforderungen an die Informations- und Auskunftspflichten[114], die Benachrichtigungspflicht[115], an die Dokumentation der Verarbeitung[116], an die interne Dokumentation der Verarbeitungsvorgänge und deren Auswertbarkeit sowie an die Revisionsfähigkeit der Verarbeitung festzuhalten.
- **Intervenierbarkeit** *In welcher Ausprägung sind Betroffenenrechte zu gewähren?* Es muss festgelegt werden, wie betroffene Personen ihre Rechte wahrnehmen können, wie sichergestellt wird, dass Anfragen berechtigt stattfinden, wie in die Verarbeitung personenbezogener Daten eingegriffen werden kann (z. B. durch Berichtigung, Löschung oder Einschränkung der Verarbeitung von personenbezogenen Daten) und in welche Form Daten von oder zu anderen Verantwortlichen übertragen werden können.
- **Nichtverkettung** *Welche Zweckänderungen sind zulässig? Welche Zwecke von Hilfsprozessen leiten sich aus den Kernprozessen legitim ab?* Benötigt werden lediglich Aussagen zu solchen Zwecken, welche die Verantwortlichen tatsächlich verfolgen bzw. zu verfolgen beabsichtigen. Maßnahmen zur Gewährleistung der Nichtverkettung sollen mit dem Ziel ergriffen werden, die Verarbeitung oder Nutzung der Daten für alle außer den festgelegten legitimen Zwecken auszuschließen.
- **Datenminimierung** *Auf welche Weise wird das Gebot der Datenminimierung umgesetzt?* Es ist zu klären, wie die Kenntnisnahme von und die Ausübung welcher Verfügungsgewalt über welche Daten der Betroffenen durch welche Personen und Stellen zu minimieren sind. Dazu gehört es auch Speicherfristen für personenbezogene Daten sowie Prozesse zur Sicherstellung ihrer Einhaltung festzulegen. Ausgangspunkt sind dabei erneut die Interessen der Betroffenen, auch innerhalb einer Verarbeitung zu legitimen Zwecken die Belastung auf das erforderliche Maß zu begrenzen.
- **Belastbarkeit** *Sind Systeme und Prozesse auf Ereignisse, welche Störungen der regulären Abläufe verursachen, hinreichend vorbereitet?* Es ist zu klären, welche Schadensereignisse, Störungen oder Angriffe negative Auswirkungen für Betroffene haben können und ob hierfür Gegenmaßnahmen zur Verfügung stehen und diese zielgerichtet und zeitnah angewandt werden können. Aufgrund des Querschnittscharakters des Ziels der Belastbarkeit kann davon ausgegangen werden, dass bei einem hohen Reifegrad der Umsetzung der übrigen Gewährleistungsziele ein hinreichender Grad an Belastbarkeit erreicht ist.

Nachdem die Gewährleistungsziele bzgl. der Verarbeitungstätigkeit qualitativ konkretisiert wurden, können technische und organisatorische Maßnahmen bestimmt werden. Zu diesem

[114] § 16 ff DSG-EKD / §§ 14 und 17 KDG
[115] § 33 DSG-EKD / §§ 15 und 16 KDG
[116] § 31 DSG-EKD / § 31 KDG

Zweck werden die Ergebnisse der Datenschutzfolgen-Abschätzung herangezogen, sofern eine durchgeführt wurde. Das im Rahmen der Risikobeurteilung (z.B. nach dem Vorgehensmodell der Anlage „Das Risikomodell des KDM“) festgestellte Risiko für die Rechte und Freiheiten der von der Verarbeitung Betroffenen ist maßgeblich für das weitere Vorgehen. Ihr Ergebnis fließt in dreierlei Form in die weiteren Betrachtungen ein.

Zum Ersten können die Gewährleistungsziele quantitativ näher bestimmt werden. Beispiele für Präzisierungen sind Antworten auf folgende Fragen: Für welchen Zeitraum ist der Verlust der Verfügbarkeit der Daten für die Betroffenen in welchem Grad tolerabel? Mit welcher Verzögerung soll die Aktualität der Daten garantiert werden? Mit welcher zeitlichen Präzision muss die Verarbeitung im Nachhinein nachvollzogen werden können? In welchem zeitlichen Rahmen muss der bzw. die Verantwortliche in der Lage sein, die jeweiligen Betroffenenrechte zu gewähren? Wie lange dürfen Daten zu welchen Zwecken verarbeitet werden, bevor diese von der Verarbeitung ausgeschlossen oder gelöscht werden?

Zum Zweiten bildet das Ergebnis der Risikoprüfung bzw. der Datenschutz-Folgenabschätzung die Grundlage für die Abwägung zwischen der Wahrung der Interessen der Betroffenen und dem hierfür erforderlichen Aufwand der Verantwortlichen. Für typische Verarbeitungskontexte ist das Ergebnis einer solchen Abwägung durch die Darstellung regelhaft zu ergreifender Maßnahmen in Kapitel D1 vorgezeichnet.

Zum Dritten fließt das Ergebnis der Datenschutz-Folgenabschätzung in die Bewertung der Restrisiken ein, die nach Umsetzung der Maßnahmen verbleiben, die mit einem Aufwand ergriffen werden können, der in angemessenem Verhältnis zum Zweck der Verarbeitung besteht. Diese Risiken können von dem Interesse Dritter oder Beteiligter abhängen, die Gewährleistungsziele zu verletzen, sei es, um Daten der Betroffenen unbefugt zur Kenntnis zu nehmen, um sie für illegitime Zwecke, über das erforderliche Maß hinaus oder in intransparenter Weise zu verarbeiten.

D4.4 Datenschutzmanagementprozess

Der DSM-Prozess (siehe Abbildung 1) wird in Anlehnung an den bewährten PDCA-Zyklus ausgestaltet. Der Datenschutz-PDCA-Zyklus (DSM-Zyklus) umfasst die folgenden vier Phasen:

- Plan: Planen und Spezifizieren / DSFA / Dokumentieren
- Do: Implementieren / Protokollieren
- Check: Kontrollieren / Prüfen / Beurteilen
- Act: Verbessern

Das KDM unterstützt die Verantwortlichen bei der Durchführung von Schwellwertanalyse (siehe auch Kapitel D3.1) und Datenschutz-Folgenabschätzung und der daraus resultierenden Auswahl eines Satzes von technischen und organisatorischen Maßnahmen (Soll-Werte), indem individuell gewählte Maßnahmen mit den im Referenzmaßnahmenkatalog vorgeschlagenen Maßnahmen abgeglichen werden (in **Phase 1** des DSM-Zyklus). Die ausgewählten Maßnahmen werden in **Phase 2** für den laufenden Betrieb umgesetzt. Die aus

der Planungsphase resultierenden funktionalen Soll-Werte werden mit den aus dem laufenden Betrieb resultierenden funktionalen Ist-Werten verglichen (**Phase 3a**). Anschließend erfolgt eine Beurteilung der Erfüllung der rechtlichen Vorgaben und der ggf. verbleibenden Restrisiken für die Rechte und Freiheiten der Betroffenen (**Phase 3b**). Ein zu geringes Schutzniveau bzw. als zu hoch beurteilte Restrisiken müssen dann durch entsprechende Verbesserungen etwa durch zusätzliche Maßnahmen auf ein akzeptables Maß gemindert werden (**Phase 4**).

Die zum Ende von Phase 3 getroffene Beurteilung kann in der Folge sowohl Grundlage für die Empfehlung bzw. die Aufforderung der Aufsichtsbehörde als auch der Anweisungen der Verantwortlichen bilden. (Phase 4 des DSM-Zyklus).

Die nachfolgende Grafik zeigt den gesamten DSM-Zyklus, in den das KDM eingebunden ist. Der Baustein 80 „Datenschutzmanagement“ des Referenzmaßnahmenkatalogs beschreibt das gesamte DSM-System ausführlich.

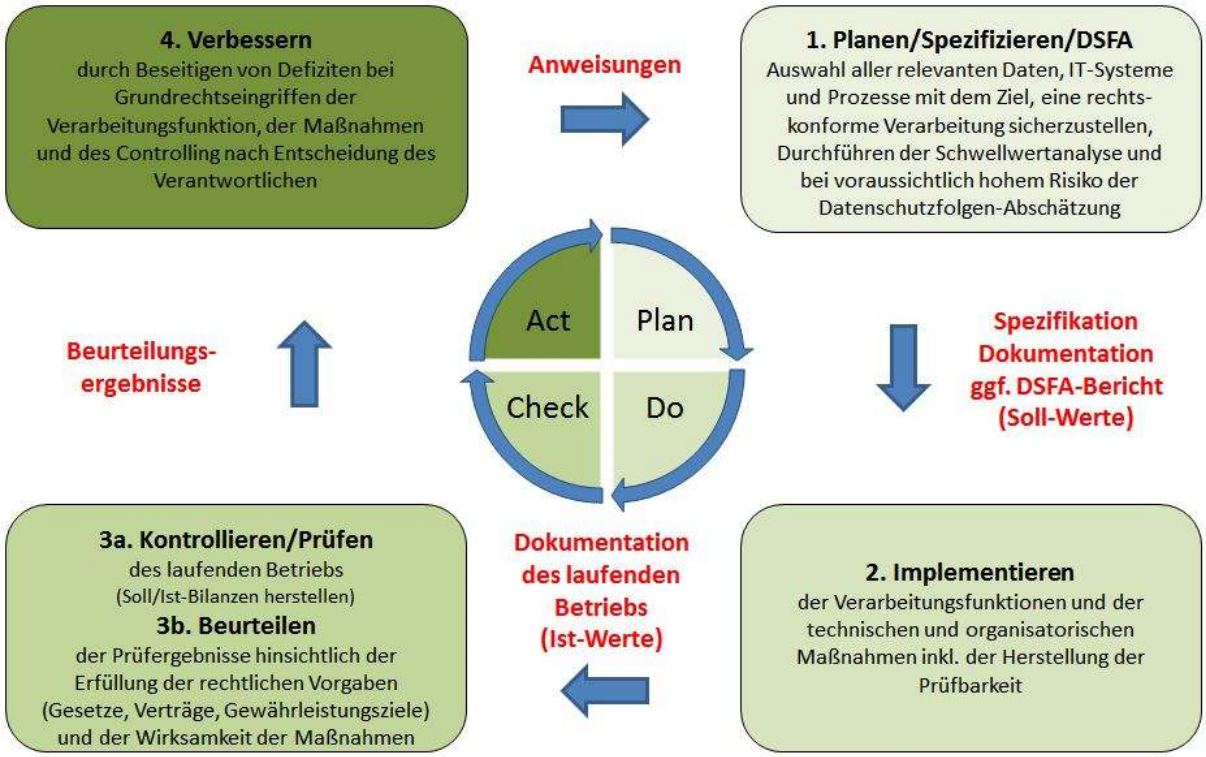


Abbildung 1: Der PDCA-Zyklus des Datenschutzmanagements (DSM-Zyklus) als Rahmen für die Anwendung des kirchlichen-Datenschutzmodells bei Planungs-, Beratungs- und Prüfvorgängen

Für jede Verarbeitungstätigkeit wird es in der Regel erforderlich sein, den DSM-Zyklus mehrfach zu durchlaufen. Das betrifft insbesondere die Verantwortlichen bei der Planung von Verarbeitungstätigkeiten. So könnte bei der Inbetriebnahme eines Fachverfahrens ein erster Zyklus dessen Testbetrieb betreffen, der zweite Zyklus den Pilotbetrieb und der dritte Zyklus den Wirkbetrieb. Die Häufigkeit der Durchläufe hängt davon ab, wie weit der Verarbeitungskontext an die Erfordernisse des Datenschutzes in der Planungsphase oder im Rahmen eines Prüfprozesses der Aufsichtsbehörde angepasst werden musste.

D4.4.1 Plan: Spezifizieren / DSFA / Dokumentieren

In Phase 1 zur Planung einer Verarbeitungstätigkeit mit Personenbezug werden angemessene Maßnahmen bestimmt, durch die die Risiken des Grundrechtseingriffs gemildert, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann. Um den Nachweis der Wirksamkeit der Maßnahmen erbringen zu können, müssen funktionale Anforderungen (Soll-Werte) festgelegt und dokumentiert werden. Diese werden aus den gesetzlichen Anforderungen (Soll) hergeleitet (siehe Teil B Anforderungen des kirchlichen Datenschutzrechtes). Erst dann wird festgelegt, welche Aktivitäten der Programme und Systeme und welche Ereignisse von Prozessen zu protokollieren sind.

Eine wesentliche Komponente der Phase 1 ist die Durchführung einer Schwellwertanalyse und eine daraus ggfs. resultierende Datenschutz-Folgenabschätzung (DSFA).

Ein Ergebnis dieser DSFA ist der DSFA-Bericht, in dem die Risiken aufgezeigt und die Gegenmaßnahmen zur Verringerung von Risiken bestimmt werden. Häufig werden den Verantwortlichen in diesem Bericht zusätzlich Empfehlungen zur weiteren Vorgehensweise bei der Implementierung der zu ergreifenden Maßnahmen[117] gegeben, weil das kirchliche Recht die Implementierung von solchen Abhilfemaßnahmen fordert.

Die Verantwortlichen müssen während der Phase 1 über die DSFA entscheiden. Am Ende der Phase 1 entscheiden sie über die geplante Implementierung der Gegenmaßnahmen.

Die Durchführung einer DSFA ist dabei kein einmaliger Vorgang. Sollten sich wesentliche Änderungen im Verfahren oder bei den Umständen der Verarbeitung, die die Bewertung bereits erkannter Risiken ändern, oder neue Risiken bekannt werden, so ist die DSFA zu überprüfen und anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung von Funktionen empfohlen. Dieser iterative Prozess der DSFA ist in den DSM-Prozess eingebunden.

Die Implementierung der empfohlenen Funktionen und der technischen und organisatorischen Maßnahmen geschieht in Phase 2 des DSM.

D4.4.2 Do: Implementieren / Protokollieren

In Phase 2 werden die aus den Ergebnissen der Phase 1 empfohlenen Maßnahmen entsprechend den Anweisungen der Verantwortlichen umgesetzt. Beim Vorliegen eines DSFA-Berichts muss der bzw. die Verantwortliche dessen Ergebnisse bei der Implementierung von Verarbeitungstätigkeiten berücksichtigen.

Bei der Implementierung von Systemen und Programmen ist darauf zu achten, dass anhand von Systemdokumenten und Protokollen die Funktionen der Fachapplikationen und der Schutzvorkehrungen von IT-Systemen und Diensten auf den verschiedenen Ebenen (Client,

[117] § 34 DSG-EKD / § 35 KDG

Server) überprüft werden können. Das Vorliegen dieser Dokumente und Protokolle (Ist-Werte) ist die Voraussetzung zur Durchführung der Phase 3 des DSM.

D4.4.3 Check: Kontrollieren, Prüfen Beurteilen

Der Kern der Anwendung des KDM im DSM-Zyklus besteht darin, die in der Planungsphase bestimmten funktionalen Soll-Werte mit den festgestellten Ist-Werten in Beziehung zu setzen (Phase 3a). Zudem werden die relevanten Referenzmaßnahmen mit den tatsächlich umgesetzten technischen und organisatorischen Maßnahmen verglichen. Abweichungen vom Soll sind danach zu beurteilen, inwieweit sie die Umsetzung der Grundsätze aus § 5 DSG-EKD/ § 7 KDG bzw. das Erreichen der Gewährleistungsziele gefährden. In einem Prüfvorgang der Aufsichtsbehörde erlaubt die bis zu diesem Punkt geführte Analyse aus einem Verfehlen der Gewährleistungsziele auf (ggf. sanktionierbare) datenschutzrechtliche Mängel zu schließen.

In der Prüf- und Beurteilungspraxis lässt sich häufig mit nur geringem Aufwand feststellen, ob Anforderungen nicht erfüllt werden, weil die entsprechend zugeordneten Maßnahmen fehlen, Maßnahmen falsch oder unzureichend umgesetzt sind oder die Referenzmaßnahmen nicht korrekt angewendet wurden. Komplizierter ist der Fall, wenn die zu prüfende Stelle andere als die Maßnahmen des Referenzmaßnahmenkatalogs gewählt hat. Auch wenn diese als grundsätzlich geeignet beurteilt werden können, muss separat geprüft werden, ob sie in ihrer konkreten Ausgestaltung tatsächlich dem festgestellten Risiko entsprechen. An dieser Stelle hilft das KDM, die Erörterung auf den Nachweis dessen zu fokussieren, dass (oder inwieweit) die getroffene technische oder organisatorische Maßnahme funktional äquivalent bzw. wirkungsgleich zur Referenzmaßnahme ist.

Ausgangspunkt für die datenschutzrechtliche Beurteilung einer Verarbeitungstätigkeit ist die Feststellung der funktionalen Soll-Ist-Differenzen. Diese Differenzen werden in der Beurteilungsphase (Phase 3b) wieder ins Rechtliche übersetzt und mit den datenschutzrechtlichen Anforderungen (Soll) verglichen. Im Rahmen einer datenschutzrechtlichen Beurteilung werden aus den festgestellten Abweichungen ggfs. „normative Mängel“. Je gravierender ein Mangel ist, umso wirksamer muss er durch entsprechende Änderungsanweisungen in Phase 4 des DSM-Prozesses für ein erneutes Durchlaufen aller Phasen des DSM-Zyklus abgestellt werden. Das Ergebnis der Phase 3b besteht in Beurteilungen, die geeignet sind, um rechtliche und funktionale Verbesserungen herbeizuführen.

D4.4.4 Act: Verbessern und Entscheiden

Die in Phase 3b festgestellten Mängel müssen so formuliert sein, dass anschließend konkrete funktionale Maßnahmen getroffen werden können. Diese Beurteilungen als Ergebnisse aus Phase 3 sind von den Verantwortlichen in Phase 4 zu sichten, zu beraten und zu priorisieren. In Phase 4 müssen festgestellte Mängel zu Entscheidungen der Verantwortlichen und daraus resultierenden Anweisungen zu Änderungen von Maßnahmen oder zu neuen Maßnahmen führen, die dann in einem neuen Zyklus zu planen, zu implementieren und zu prüfen sind.

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

Teil E: Organisatorische Rahmenbedingungen

E1 Zusammenwirken von KDM und BSI-Grundschutz

Das KDM steht in einer engen Beziehung zur Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Der vom BSI entwickelte IT-Grundschutz ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium und die darin enthaltenen Bausteine konkrete (Maßnahmen-)Anforderungen. Bei der Auswahl von Maßnahmen orientiert sich der Grundschutz vorrangig an den aus der IT-Sicherheit bekannten Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit.

Um die Anwendung des KDM zu erleichtern, nutzt die KDM-Methodik vergleichbare Modellierungsmechanismen wie die Grundschutzmethodik. BSI-Grundschutz und KDM basieren auf einer vergleichbaren Analyse von Verarbeitungstätigkeiten (bzw. Geschäftsprozessen). Das KDM beschreibt die Verarbeitungstätigkeit mit ihren Daten, Systemen und Diensten sowie (Teil)-Prozessen (s. Abschnitt D2.3) und betrachtet umfassend das Element der personenbezogenen Daten. Die zu treffenden technischen und organisatorischen Maßnahmen sind abhängig vom Risiko, das von der Verarbeitungstätigkeit und deren Eingriffsintensität ausgeht (Vgl. **Anlage „Richtlinie zur Risikoanalyse und Risikobehandlung“**).

Die Umsetzung der im Referenzmaßnahmenkatalog sowie in den Bausteinen genannten Sicherheitsmaßnahmen ist für den Datenschutz essentiell. Das KDM nimmt dabei exklusiv die Perspektive des Betroffenen und dessen Grundrechtsausübung ein und unterscheidet sich daher von der Sicht des IT-Grundschutzes, der das Schadenszenario „Beeinträchtigung des informationellen Selbstbestimmungsrechts“ als eines unter mehreren bei der Bestimmung des Schutzbedarfs betrachtet. Ziel des Vorgehens gemäß IT-Grundschutz ist dabei der Aufbau eines Informations-Sicherheits-Management-Systems (ISMS). Vor diesem Hintergrund ist zwischen der Auswahl von Maßnahmen zur Gewährleistung der Informationssicherheit für Institutionen durch verantwortliche Stellen und der von Maßnahmen zur Gewährleistung der Betroffenenrechte zu unterscheiden.

Das KDM erweitert die o. g. aus der IT-Sicherheit bekannten Schutzziele, was in der Terminologie des KDM zu den Gewährleistungszielen führt, aus denen, wie im Bereich der IT-Sicherheit, technische und organisatorische Maßnahmen abgeleitet werden. Die Gewährleistungsziele des Datenschutzes bieten in diesem Sinne im Vergleich zu den Schutzzielen der IT-Sicherheit eine feinere Granularität zur Beschreibung der Schutzziele für personenbezogene Daten. In den Fokus rücken dabei auch die Risiken, die von den Verarbeitungstätigkeiten der verantwortlichen Stelle selbst innerhalb und außerhalb ihrer Geschäftsprozesse für die Rechte und Freiheiten natürlicher Personen ausgehen.

BSI IT-Grundschutz und KDM ergänzen sich somit in idealer Weise und liefern gemeinsam die Informationen, die erforderlich sind, um die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen zu können.

Anwendungsbereich

Das KDM kann sowohl von kirchlichen Aufsichtsbehörden im Rahmen ihrer gesetzlichen Beratungs-, Prüf- und Sanktionstätigkeiten (Anwendergruppe 1) 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 (Anwendergruppe 2) angewendet werden. Eine Verpflichtung zur Nutzung des KDM ist nicht vorgesehen.

E2 Versionspflege des KDM

Das KDM wird vorerst in einer einmaligen Ausgabe für die katholische und die Evangelische Kirchen in Deutschland herausgegeben. Eine kontinuierliche Überarbeitung ist zum jetzigen Zeitpunkt nicht vorgesehen, wird aber nicht gänzlich ausgeschlossen.

E2.1 Änderungshistorie

20.10.2021: Korrektur eines Vertauschungsfehlers in der Tabelle C2 in den Zeilen B1.22 und B1.23 und Anpassung aller Verweise auf diese Zeilen
Aufnahme dieser Änderungshistorie

E3 Stichwortverzeichnis

E4 Abkürzungsverzeichnis

Abs.	Absatz
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der DSK

Art.	Artikel
Art.-29-Gruppe	Artikel-29-Datenschutzgruppe
BSI	Bundesamt für Sicherheit der Informationstechnik
bzgl.	bezüglich
bzw.	beziehungsweise
CON	Konzeption und Vorgehen (Bausteinbezeichnung im BSI-Kompendium)
CPU	Central Processing Unit (zentrale Verarbeitungseinheit)
CR	Change Request (Änderungsantrag)
d. h.	das heißt
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Datenschutzkonferenz
DSM	Datenschutzmanagement
ErwGr.	Erwägungsgrund
EuGH	Europäischer Gerichtshof
ggf.	gegebenenfalls
i. V. m.	in Verbindung mit
IKT	Informations- und Kommunikationstechnik
IT	Informationstechnik
Kap.	Kapitel
KDM	Kirchliches Datenschutzmodell
LAN	Local Area Network (lokales oder örtliches Netzwerk)
lit.	Buchstabe
NAS	Network Attached Storage (netzgebundener Speicher)
NEGS	Nationale E-Government-Strategie

Nr.	Nummer
PDCA	Plan Do Check Act (Phasen des Deming-Zyklus)
SAN	Storage Area Network (Datenspeicher-Netzwerk)
SDM	Standard-Datenschutzmodell
SPoC	Single Point of Contact (singulärer Kontaktpunkt, zentrale Anlaufstelle)
u. a.	unter anderem
vgl.	vergleiche
WP	Working Paper (der Art.-29-Gruppe)
z. B.	zum Beispiel

E5 Anhang Referenzmaßnahmenkatalog

Der Referenzmaßnahmenkatalog der DSK wird nach vorheriger Begutachtung durch die ökumenische Projektgruppe KDM Bestandteil des KDM.