Das Kirchliche Datenschutzgesetz (KDG)

DiAG-MAV im Erzbistum Hamburg

24./25. April 2018
Schwerin/Hamburg

Übersicht

A. Warum Datenschutz?

B. Rechtliche Grundlagen

C. Schlaglichter Datenschutzrecht

D. Datenschutzbehörde

E. Schlaglichter Datensicherheit und Technik

F. Grundlagen der rechtlichen Prüfung

G. Grundlagen der technischen Prüfung

A. Warum Datenschutz?

1. Datenschutz als Grundrecht

1.1. Entscheidungen des BVerfG

- Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die:
  - Befugnis des Einzelnen, „*grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.*“

    (BVerfG, Urteil vom 15.12.1983, Az. 1 BvR 209/83, Rn. 173 - Volkszählungsurteil)

- Das Grundrecht auf informationelle Selbstbestimmung dient als Abwehrrecht gegen staatliche Eingriffe
- Das Grundrecht ist eine Ausprägung des allgemeinen Persönlichkeitsrecht gem. Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG

1. Datenschutz als Grundrecht

1.2. Worum geht es im Datenschutz?

- Datenschutzrecht regelt, für welche Zwecke und in welchem Umfang personenbezogene Daten eines anderen verarbeitet werden dürfen (≙ **Spielregeln der Datenverarbeitung**).
- Geschützt sind Einzelangaben einer natürlichen Person (betroffene Person)
  - Mitarbeiter
  - Bewerber
  - Patienten
  - Bewohner
  - Nutzer Homepage

B. Rechtliche Grundlagen

1. Aktuelle Entwicklung des Datenschutzrechts

1.1. Europarecht

- seit 1995 gilt die EU -Datenschutzrichtlinie (95/46/EG)
- mit Datum vom **14.04.2016** hat die EU die Datenschutz-Grundverordnung beschlossen
- Die DS-GVO gilt ab dem **25.05.2018** unmittelbar (Übergangszeit)
- Es gibt keine weitere Übergangsfrist!

1. Aktuelle Entwicklung des Datenschutzrechts

1.1. Europarecht (Fortsetzung)

- DS-GVO gilt gem. Art 2 für jedweden Umgang mit personenbezogenen Daten (auch kirchlichen Daten)
- grds. auch Vorrang vor deutschem Verfassungsrecht
- auch Vorrang vor Art.140 GG i.V.m. Art 137 Abs.3 WRV (Staatskirchenrecht)

aber

Art. 17 Abs. 1 AEUV

„Die Union achtet den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, und beeinträchtigt ihn nicht.“

1. Aktuelle Entwicklung des Datenschutzrechts

1.1. Rechtsgrundlage DS-GVO

Artikel 91 Abs. 1 DS-GVO

„Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden."

1. Aktuelle Entwicklung des Datenschutzrechts

1.1. Rechtsgrundlage DS-GVO (Fortsetzung)

- Zwingende Voraussetzung somit die Anpassung der bisherigen KDO an die DS-GVO
  - Keine Unterschreitung des Schutzniveaus möglich!
- Art. 91 Abs. 2 DS-GVO regelt die Organisation der Aufsichtsbehörde (s.U.)

1. Aktuelle Entwicklung des Datenschutzrechts

1.2. Bundesrecht

- Ca. 50 Öffnungsklausel in der DS-GVO für nationale Regelungen
- BDSG – neu tritt ebenfalls am 25. Mai 2018 in Kraft
- Hier relevant: § 18 Abs. 1 – Kirchen –
- Die Aufsichtsbehörden des Bundes und der Länder beteiligen die nach Art. 91 Abs. 2 der EU-DSGVO in Angelegenheiten der EU eingerichteten spezifischen Aufsichtsbehörden, sofern diese von den Angelegenheiten betroffen sind (Kohärenzverfahren).
  - **Ziel**: einheitliche Anwendung der DS-GVO
- Zustimmung BT 27. April 2017; Zustimmung BR 12. Mai 2017
  - tritt am 25. Mai 2018 in Kraft

1. Aktuelle Entwicklung des Datenschutzrechts

1.3. Kirchliches Datenschutzrecht

- Kirchliches Datenschutzrecht betrifft u.a.:
  - Allgemeine Vorschriften
  - Kinder- und Jugendhilfe
  - Archivwesen
  - Krankenhäuser
  - Datensicherheit
  - Meldewesen
  - Friedhöfe
  - Schulen
  - Internet
  - u.v.a.

1. Aktuelle Entwicklung des Datenschutzrechts

1.4. Allgemeine Vorschriften (KDO/KDG)

- Aktuelle Version KDO (Anordnung über den Kirchlichen Datenschutz) seit November 2013
- Vollversammlung des VDD vom 20. November 2017 hat einstimmig einen Entwurf beschlossen

  (Gesetz über den Kirchlichen Datenschutz (KDG) in der Fassung des einstimmigen Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20. November 2017)
- Inkraftsetzung in allen Bistümern Beginn 2018

(Ziellinie: 24. Mai 2018)

2. Begriffe des Datenschutzrechts

2.1. Was sind personenbezogene Daten, § 4 Nr. 1 KDG?

- Personenbezogen Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen
- Somit sind auch Daten geschützt, die Rückschlüsse auf die Person zulassen
  - Kfz-Kennzeichen
  - IP-Adresse
  - Steuer-ID
- Die Identifizierung muss nicht zwingend unmittelbar durch den Verantwortlichen erfolgen können!

2. Begriffe des Datenschutzrechts

2.2. Was heißt Verarbeitung, § 4 Nr. 3 KDG?

Der Begriff **Verarbeiten** umfasst **jede Handlung** im Zusammenhang mit personenbezogenen Daten, § 4 Nr. 3 KDG

erheben	speichern	verändern	verwenden
erfassen	einschränken	löschen	anpassen
organisieren	ordnen	auslesen	verknüpfen
verbreiten	abgleichen	abfragen	übermitteln

2. Begriffe des Datenschutzrechts

2.3. Auf welche Verarbeitungsvorgänge ist das KDG anwendbar, § 2 Nr. 1 KDG?

- ganz oder teilweise automatisierte Verarbeitung
  - U.a. Computer, Smartphones, Überwachungsanlagen, digitale Kopierer und Scanner, jede Benutzung von Computer, Internet, E-Mail führt somit zur Anwendbarkeit
- nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen
  - Jede manuelle Verarbeitung im analogen Bereich

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung, § 7 KDG

- Allgemeine Grundsätze der Verarbeitung sind einzuhalten
  a) Zulässigkeit
  b) Transparenz
  c) Zweckbindung
  d) Datenminimierung
  e) Richtigkeit der Datenverarbeitung
  f) Speicherbegrenzung
  g) Integrität und Vertraulichkeit (IT-Sicherheit)
- Rechenschaftspflicht durch Verantwortlichen

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung

a) Zulässigkeit

- der Datenverarbeitung, § 6 KDG
  - Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn
    1. sie wird von einer Rechtsvorschrift erlaubt oder angeordnet oder
    2. es liegt eine Einwilligung der betroffenen Person vor.

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung

a) Zulässigkeit

- durch Rechtsvorschrift
  - Vertragserfüllung, § 6 Abs. 1 lit. c) KDG
  - Rechtliche Verpflichtung, § 6 Abs. 1 lit. d) KDG
  - Kirchliches Interesse, § 6 Abs. 1 lit. f) KDG
    - Bsp. Kirchliche Aufgaben nach BMG
  - Aufgaben öffentlicher Gewalt, § 6 Abs. 1 lit. f) KDG
  - berechtigtes Interesse des Verarbeiters, § 6 Abs. 1 lit. g) KDG
    - Interessenabwägung erforderlich

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung

a) Zulässigkeit

- durch Einwilligung, § 6 Abs. 1 lit. b) i.V.m. § 8 KDG
  - Freiwillig = freie Entscheidung des Einwilligenden
  - Vorab = Einwilligung vor der DV einholen
  - Informiert = über Zweck und Umfang der DV aufklären
  - Beweisbar = Schriftform
  - Sichtbar = Einwilligung besonders hervorheben

  Einwilligung kann jederzeit widerrufen werden

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung

b) Transparenz

- Die Verarbeitung muss für den Betroffenen nachvollziehbar sein
- Konkrete Maßnahmen werden in §§ 14 ff. KDG benannt
- Betroffene Person soll über
  - Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung informiert werden

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung

c) Zweckbindung

- Verarbeitung personenbezogener Daten nur für den Zweck, für den die Daten erhoben worden sind
- Für spätere Zweckänderungen wird eine neue Erlaubnis benötigt (Verbot mit Erlaubnisvorbehalt!)
  - Ergänzende Voraussetzungen für die Zweckänderungen finden sich in § 7 Abs. 2 KDG
    - Hier u.a. Einwilligung, Rechtsgrundlage, Interessen-abwägung

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung

d) Datenminimierung

- Personenbezogene Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.
  - Faustregel: „So viel wie nötig und so wenig wie möglich!“

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung

e) Richtigkeit der Datenverarbeitung

- Daten sollen sachlich richtig und auf dem neusten Stand sein
- Dafür sind angemessenen Maßnahmen zu treffen.
  - „Karteileichen“ sind nicht erlaubt

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung

f) Speicherbegrenzung

- Daten sollen nur so lange gespeichert werden, wie es für die Erfüllung des Zwecks, für den Sie erhoben wurden, erforderlich ist
  - Löschfristen beachten
  - Nach Ablauf der Löschfristen ist eine Speicherung nicht mehr erforderlich!

2. Begriffe des Datenschutzrechts

2.4. Grundsätze der Verarbeitung

g) Integrität und Vertraulichkeit (IT-Sicherheit)

- Es sind technische und organisatorische Maßnahmen zu treffen, zum Schutz personenbezogener Daten vor:
  - Unbefugter/unrechtmäßiger Verarbeitung
  - Verlust
  - Zerstörung
  - Schädigung

3. Anpassungen und Veränderungen

3.1. Recht der betroffenen Person auf transparente Informationen, § 14 ff. KDG

- Betroffene sind künftig in
  - präziser,
  - transparenter,
  - verständlicher und
  - leicht zugänglicher Form
  - in einer klaren und einfachen Sprache,
  - ggf. auch mit standardisierten Bildsymbolen, zu informieren

3. Anpassungen und Veränderungen

3.1. Recht der betroffenen Person auf transparente Informationen, § 14 ff. KDG (Fortsetzung)

- Die betroffene Person ist zudem über ihre Rechte zu informieren
  - Auskunftsrecht der betroffenen Person nach § 17 KDG,
  - Recht auf Berichtigung nach § 18 KDG,
  - Recht auf Löschung nach § 19 KDG,
  - Recht auf Einschränkung der Verarbeitung nach § 20 KDG,
  - Recht auf Datenübertragbarkeit nach § 22 KDG,
  - Widerspruchsrecht nach § 23 KDG

3. Anpassungen und Veränderungen

3.1. Recht der betroffenen Person auf transparente Informationen, § 14 ff. KDG (Fortsetzung)

- Zu beachten sind ebenfalls bei
  - unmittelbarer Datenerhebung, § 15 KDG
  - mittelbarer Datenerhebung, § 16 KDG
- Informationen sind unentgeltlich zur Verfügung zu stellen

3. Anpassungen und Veränderungen

3.2. Besonderer Schutz der Daten von Kindern und Jugendlichen, § 8 Abs. 8 KDG

- Das neue Recht schützt besonders Minderjährige vor den Risiken elektronischer Datenverarbeitung
- Grundsätzlich ist die Datenverarbeitung bei Anmeldungen oder Bestellungen im Internet nur mit der Einwilligungserklärung der Betroffenen erlaubt.
- Eine solche Erklärung kann künftig nur von Personen abgegeben werden, die das 16. Lebensjahr vollendet haben.
- Ausnahme: kostenfreies Beratungsangebot einer kirchlichen Stelle

  Hier: ab dem 13. Lebensjahr (z.B. Familienberatung)

3. Anpassungen und Veränderungen

3.3. Die eigene Dokumentation im Bereich der Datenverarbeitung

- Das KDG sieht an unterschiedlichen Stellen Dokumentations-pflichten vor:
  - Nachweis über die Einhaltung der Grundsätze der Datenverarbeitung
  - Nachweis des Vorliegens einer Einwilligungserklärung
  - Nachweis der Einhaltung der TOMs
  - Verzeichnis von Verarbeitungstätigkeiten ist zu führen
  - Informationspflicht der betroffenen Personen (s.o.)
  - Dokumentation von Datenschutzvorfällen

3. Anpassungen und Veränderungen

3.4. Bestellung eines betrieblichen Datenschutzbeauftragten

- für den verfasst-kirchlichen Bereich (Diözese, Kirchengemeinde, Kirchenstiftung und Kirchengemeindeverbände) unabhängig von der Zahl Ihrer Mitarbeiter, § 36 Abs. 1 KDG
- Nach § 36 Abs. 2 KDG andere kirchliche Stellen, wenn
  - mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind,
  - die Kerntätigkeit der Einrichtung in der Durchführung von Verarbeitungsvorgängen besteht, **oder**
  - die Kerntätigkeit der Einrichtung in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht.

3. Anpassungen und Veränderungen

3.5. Bestellung eines betrieblichen Datenschutzbeauftragten (Fortsetzung)

- Änderungen zur KDO:
  - mehr als 10 Personen ist durch mindestens 10 Personen ersetzt worden
  - Einschränkung auf die Verarbeitung in elektronische Medien ist entfallen
- Möglichkeit der Bestellung eines gemeinsamen bDSB
  - Organisationsstruktur und Größe müssen berücksichtigt werden

3. Anpassungen und Veränderungen

3.6. Bestandsaufnahme aller durchgeführten Verarbeitungsprozesse, § 31 KDG

- Bisher musste bereits ein Verfahrensverzeichnis für den Fall automatisierter Verarbeitung erstellt werden, § 3a KDO
- Neu:
  - Verzeichnis der Verarbeitungstätigkeit
  - Pflicht zur Erstellung gilt für Einrichtungen, die 250 oder mehr Beschäftigte haben
    oder

3. Anpassungen und Veränderungen

3.6. Bestandsaufnahme aller durchgeführten Verarbeitungsprozesse, § 31 KDG (Fortsetzung)

- für Einrichtungen mit weniger als 250 Beschäftigte, wenn
  - durch die Verarbeitung die Rechte und Freiheiten der betroffenen Personen gefährdet werden, oder
  - die Verarbeitung nicht nur gelegentlich erfolgt oder
  - die Verarbeitung besondere Datenkategorien beinhaltet.
- Übergangsfrist: 30.06.2019
- Beispiele:
  - Zeiterfassung, E-Mail und Telefonanalagen, Personaldatenverarbeitung, Lohnbuchhaltung

3. Anpassungen und Veränderungen

3.7. Bestehende Verträge mit Auftragsverarbeitern überprüfen und anpassen, § 29 KDG

- Bestehende Verträge zur Auftragsverarbeitung überprüfen und gegebenenfalls anpassen.
  - Der Auftragsverarbeiter darf die Daten **nur** innerhalb der Europäischen Union verarbeiten.
    - Ausnahme
      - Angemessenheitsbeschluss Kommission oder
      - wenn Datenschutzaufsicht festgestellt hat, dass dort ein angemessenes Datenschutzniveau besteht.
- Frist zur Anpassung bisheriger Regelungen: 31.12.2019

3. Anpassungen und Veränderungen

3.8. Datenschutz-Folgenabschätzung, § 35 KDG

- Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung durch den Verantwortlichen, wenn
  - die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, voraussichtlich
  - ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat
- Erforderlich ist eine Prognoseentscheidung

3. Anpassungen und Veränderungen

3.8. Datenschutz-Folgenabschätzung, § 35 KDG (Fortsetzung)

- Praxisbeispiele für hohes Risiko
  - Verarbeitung von Gesundheitsdaten
  - Intelligente Videoüberwachung des Straßenverkehrs
  - Neuartige Videoüberwachung
- Eine DSFA ist **immer** erforderlich, wenn biometrische Daten oder die Daten von Kindern verarbeitet werden.

3. Anpassungen und Veränderungen

3.9. Haftung und Schadensersatz, § 50 KDG

- Zivilrechtliche Haftung für das Entstehen materieller und immaterieller Schäden
  - betragsmäßige Haftungsbeschränkung ist nicht vorgesehen
- Feststellung der Aufsichtsbehörde, eine Datenschutzverletzung habe objektiv vorgelegen, ist im Prozess bindend (§ 47 Abs. 2 KDG).

C. Datenschutzbehörde

1. Grundlagen

1.1. Rechtsgrundlage DS-GVO

Artikel 91 Abs. 2 DS-GVO

„Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Aufsicht durch eine unabhängige Aufsichtsbehörde, […] sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt.“

– Zwingende Voraussetzung somit die Einrichtung von unabhängigen Aufsichtsbehörden

1. Grundlagen

1.2. Regelungen des Kapitel VI DS-GVO

- Kapitel VI der DS-GVO enthält die Bestimmungen zu den unabhängigen Aufsichtsbehörden
- Umsetzung dieser Bestimmungen in Kapitel 6 des KDG, u.a. Vorschriften zu
  - Rechtsstellung
  - Aufgaben
  - Zuständigkeit
  - Beanstandungen

1. Grundlagen

1.2. Regelungen des Kapitel VI DS-GVO (Fortsetzung)

- **Ziel der Datenschutzaufsicht:**
  - Schutz des Einzelnen vor Beeinträchtigungen in seinem Persönlichkeitsrecht bei der Verarbeitung personenbezogener Daten
  - Förderung des freien Verkehrs personenbezogener Daten durch Schaffung einheitlicher Standards

2. Neuerungen

2.1. Rechtsstellung, § 43 KDG

- In Ausübung der Tätigkeit ist der Diözesandatenschutzbeauftragte
  - an Weisungen nicht gebunden
  - nur dem kirchlichen Recht und dem verbindlichen staatlichen Recht unterworfen
- Ausübung geschieht in
  - organisatorischer und
  - sachlicher Unabhängigkeit

2. Neuerungen

2.2. Aufgaben, § 44 Abs. 1 und 3 KDG

- Überwachung der Anwendung der Vorschriften des KDG und weiterer Vorschriften über den Datenschutz
- Ferner u.a.:
  - Bearbeitung und Untersuchung von Beschwerden von Betroffenen, Stellen oder Organisationen
  - Unterstützung der betrieblichen Datenschutzbeauftragten
  - Öffentlichkeitsarbeit

2. Neuerungen

2.3. Befugnisse, § 44 Abs. 2 KDG

- Die Datenschutzbehörde hat im Zusammenhang mit der Verarbeitung personenbezogener Daten ein uneingeschränktes
  - Auskunftsrecht
  - Einsichtsrecht
  - Zutrittsrecht zu allen Diensträumen während der Dienstzeit, die der Verarbeitung und Aufbewahrung automatisierter Dateien dienen
- Durchführung von Datenschutzüberprüfungen

2. Neuerungen

2.4. Beanstandungen, § 47 KDG

- Sofern ein Verstoß festgestellt wird, kann die Aufsichtsbehörde den Verstoß
  - beanstanden und
  - eine Frist zur Behebung des Verstoßes setzen
- Bei Nichtbehebung der Mängel ist die Aufsicht führende Stelle zu verständigen und sie zu einer Stellungnahme aufzufordern

2. Neuerungen

2.4. Beanstandungen, § 47 KDG (Fortsetzung)

- Zudem können Anordnungen getroffen werden, z.B.
  - Pflicht zur Benachrichtigung des Betroffenen über den Verstoß
  - Ggf. korrigieren oder löschen von Daten
  - vorübergehende oder endgültige Beschränkung sowie der Ausspruch eines Verbot der Verarbeitung
- Anordnungen müssen geeignet sein, einen rechtmäßigen Zustand wiederherzustellen oder Gefahren für die Betroffenen abzuwehren

2. Neuerungen

2.5. Geldbuße, § 51 KDG

- Neben oder anstelle der vorgenannten Anordnungen kann ein Geldbuße verhängt werden, vgl. § 47 Abs. 6 KDG
- Eine Geldbuße kann bis zu 500.000 EUR betragen
- Eine Geldbuße soll im Einzelfall wirksam, verhältnismäßig und abschreckend sein
- Liegen mehrere Verstöße durch gleiche oder miteinander verbundene Verarbeitungsvorgänge vor, so wird ein Gesamtbetrag der Geldbuße festgesetzt
- Ausnahmen von der Geldbuße gelten im verfasst-kirchlichen Bereich (Diözese, Kirchengemeinde, Kirchenstiftung und Kirchengemeindeverbände)

2. Neuerungen

2.6. Gerichtliche Überprüfung, 49 Abs. 3 KDG

- Zuständigkeit liegt beim kirchlichen Gericht in Datenschutzangelegenheiten
- Ein Entwurf der Vollversammlung des VDD mit Beschluss vom 20.11.2017 einstimmig beschlossen worden

  (Kirchliche Datenschutzgerichtsordnung (KDSGO) in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20. November 2017)

3. Rechte der betroffenen Person

3.1. Beschwerde, § 48 KDG

- Jede Betroffene Person hat das Recht auf eine Beschwerde bei der Datenschutzaufsicht
- Die gilt unbeschadet anderweitiger Rechte (z.B. zivilrechtliche Ansprüche)
- Datenschutzaufsicht prüft den Sachverhalt und fordert den Verantwortlichen, Empfänger oder Dritten zu einer Stellungnahme auf

3. Rechte der betroffenen Person

3.2. Gerichtlicher Rechtsbehelf, § 49 Abs. 2 KDG

- Recht auf einen gerichtlichen Rechtsbehelf
- Recht gilt auch für den Fall, dass die Datenschutzaufsicht sich nicht
  - mit der Beschwerde befasst oder
  - innerhalb von drei Monaten die betroffene Person über den Stand oder das Ergebnis der Beschwerde in Kenntnis setzt

4. Rechte des Verantwortlichen

4.1. Gerichtlicher Rechtsbehelf, § 49 Abs. 1 KDG

- Auch der Verantwortliche hat das Recht auf einen gerichtlichen Rechtsbehelf gegen einen ihn belastenden Bescheid der Datenschutzaufsicht
- Ferner steht dieses auch anderen natürlichen oder juristischen Personen zu
  - Z.B. im Fall, dass der Beschwerde nicht abgeholfen wird

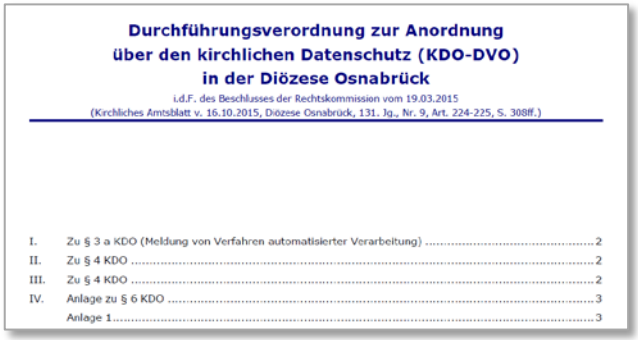
D. Schlaglichter Datensicherheit und Technik „TOMs & Co.“

1. Aktueller Stand: TOMs in der KDO/KDO-DVO

Anordnung über den kirchlichen Datenschutz (KDO)
in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 18.11.2013

Kirchliches Amtsblatt für die Diözese Osnabrück vom 19.02.2014, Band 60, Nr. 2, Art. 19, Seite 20 ff.

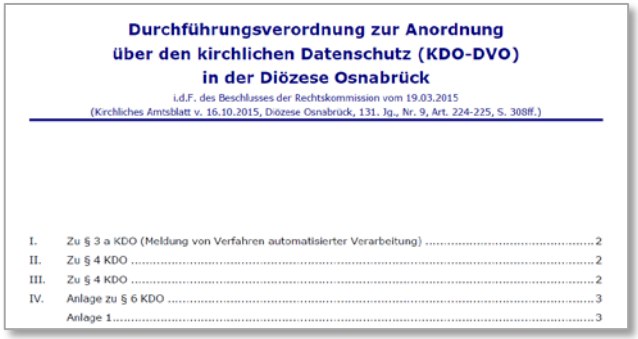
Inhaltsübersicht



Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO) in der Diözese Osnabrück

i.d.F. des Beschlusses der Rechtskommission vom 19.03.2015
(Kirchliches Amtsblatt v. 16.10.2015, Diözese Osnabrück, 131. Jg., Nr. 9, Art. 224-225, S. 308ff.)

Anlage 1 zu § 6 KDO („8 Gebote“)



Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO) in der Diözese Osnabrück

i.d.F. des Beschlusses der Rechtskommission vom 19.03.2015
(Kirchliches Amtsblatt v. 16.10.2015, Diözese Osnabrück, 131. Jg., Nr. 9, Art. 224-225, S. 308ff.)

Anlage 2 zu § 6 KDO (Einsatz von APC)

Anlagen

Zu Abschnitt IV. KDO-DVO (Anlage 2 zu § 6 KDO): IT-Richtlinien

IT-Richtlinien zur Umsetzung von IV. Anlage 2 zu § 6 KDO der Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO)

i.d.F. des Beschlusses der Rechtskommission vom 19.03.2015

Anlage zu Anlage 2 zu § 6 KDO (IT-Richtlinien, „Mindeststandard für kirchlichen Datenschutz“)

KDO-DVO

2. TOMs und Technik in der KDG

2.1. Grundsätze

- Datenschutz:
  - Schutz des Menschen vor Missbrauch ihrer personenbezogenen Daten
- Datensicherheit:
  - Schutz der Daten und ihrer Verarbeitung vor unberechtigten Zugriffen und/oder Zerstörung oder anderen Beeinträchtigungen
    - *„Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (IT-Grundrecht)*

(BVerfG, Urteil vom 27.02.2008, - 1 BvR 370/07)

2. TOMs und Technik in der KDG

2.1. Grundsätze (Fortsetzung)

§ 7 KDG

Abs. 1. lit. f.): *„Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich* ***Schutz vor unbefugter oder unrechtmäßiger Verarbeitung*** *und vor* ***unbeabsichtigtem Verlust****,* ***unbeabsichtigter Zerstörung*** *oder* ***unbeabsichtigter Schädigung*** *durch geeignete technische und organisatorische Maßnahmen.“*

Abs. 2: *„Der Verantwortliche ist für die Einhaltung der Grundsätze des Absatz 1 verantwortlich und muss dies nachweisen können.“*

2. TOMs und Technik in der KDG

§ 26 KDG: Gewährleistung eines **dem Risiko angemessenen Schutzniveaus**

Erforderliche TOMs:	Gegen folgende **Gefährdungen**:
Stand der Technik	Vernichtung
Implementierungskosten/ Unternehmensgröße	Verlust
Art, Umfang, Umstand, Zweck der Verarbeitung	Veränderung
Eintrittswahrscheinlichkeit	Weitergabe/unbefugter Zugang
Schwere des Risikos für die Rechte & Freiheiten	Unbefugte Offenlegung

2. TOMs und Technik in der KDG

2.2. Technische Schutzziele, § 26 Abs. 1 S. 2 lit. b) KDG

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit

2. TOMs und Technik in der KDG

2.2. Technische Schutzziele (Fortsetzung)

- **Vertraulichkeit**
  - Informationen dürfen nur Berechtigten bekannt sein
  - Maßnahmen zur Sicherung der Vertraulichkeit können sein
    - Verschlüsselung (Kryptographie, PGP)
    - Verhindern des Zugriffs auf Daten
    - Sicheres Löschen/Entsorgungskonzept

Frage: Wer darf welche Daten lesen und von ihnen Kenntnis erlangen und unter welchen Voraussetzungen?

2. TOMs und Technik in der KDG

2.2. Technische Schutzziele (Fortsetzung)

- **Integrität**
  - Informationen sind richtig und vollständig
  - Maßnahmen zur Sicherung der Integrität können sein
    - Digitale Signaturen
    - Hashwertbildung
    - Protokollierung

Frage: Wer darf welche Daten bzw. IT Systeme ändern und unter welchen Bedingungen?

2. TOMs und Technik in der KDG

2.2. Technische Schutzziele (Fortsetzung)

- **Verfügbarkeit**
  - Informationen sind zugänglich, wann und wo sie von Berechtigten gebraucht werden
  - Maßnahmen zur Sicherung der Verfügbarkeit können sein
    - Redundanz
    - Backups
    - Vermeiden von „Single Points of Failure“ (durch Redundanz oder Diversität)

2. TOMs und Technik in der KDG

2.2. Technische Schutzziele (Fortsetzung)

- **Belastbarkeit**
  - Systeme sind selbst bei starkem Zugriff und bei internen und externen, bekannten oder unbekannten Störungen funktionsfähig
  - Maßnahmen zur Sicherung der Belastbarkeit können sein
    - Redundanz
    - Backups
    - Entflechtung (Reduktion der Komplexität)

2. TOMs und Technik in der KDG

2.3. Weitere Pflichten

- Sicherstellung der raschen Wiederherstellung nach physischen und technischen Zwischenfall (§ 26 Abs. 1 S. 2 lit. c) KDG)
- Sicherstellung der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs (§ 26 Abs. 1 S. 2 lit. c) KDG)

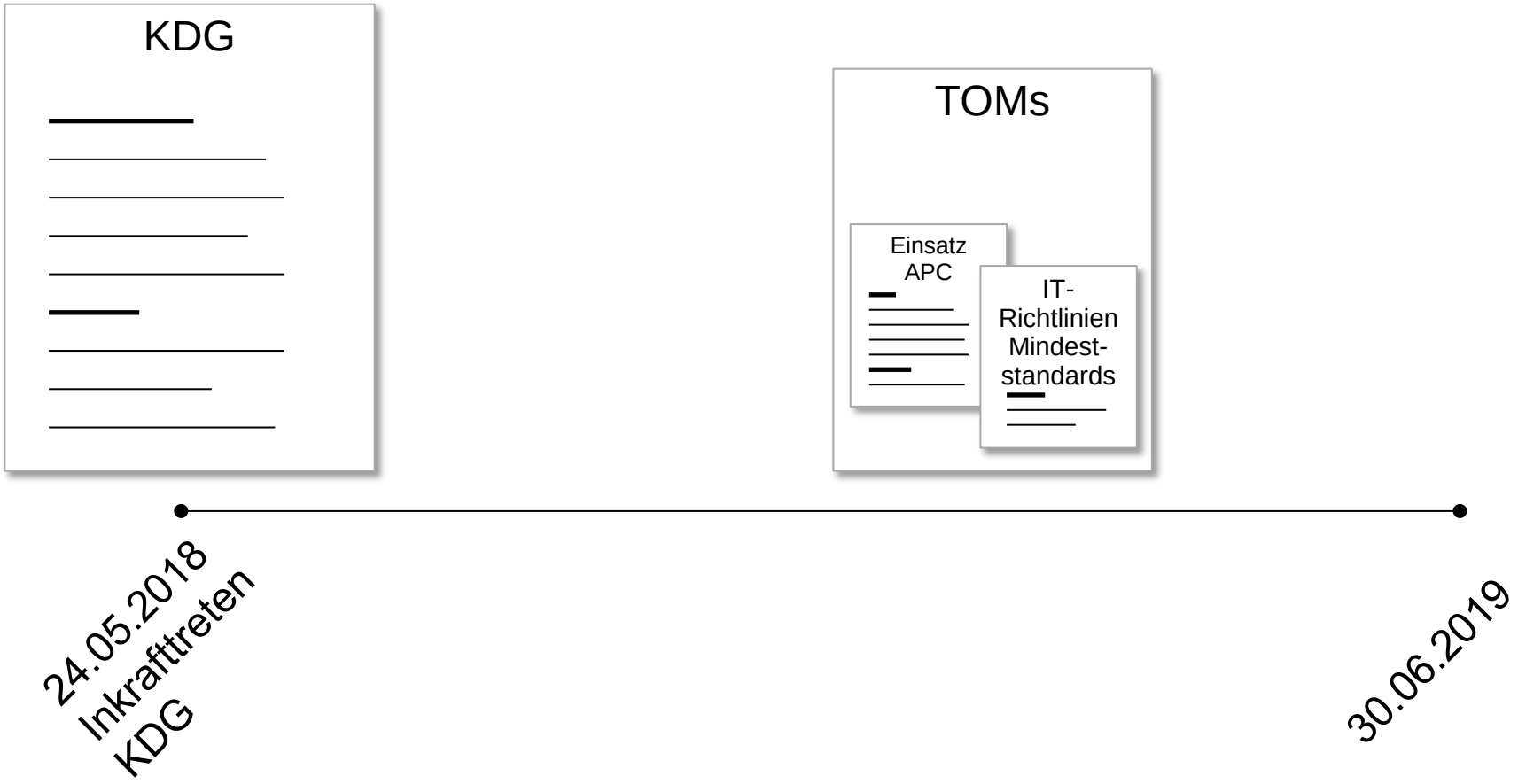
2. TOMs und Technik in der KDG

2.4. Anforderungen zu Umsetzung

- KDG gibt keine konkreten Anforderungen zur Umsetzung der TOMs vor
- Nur abstrakte allgemeine Anforderungen
  - Pseudonymisierung, Anonymisierung und Verschlüsselung (§ 26 Abs. 1 S. 2 lit. a) KDG)
  - Privacy by Design/Privacy by Default (§ 27 KDG)
  - “8 Gebote” in Anlage 1 zu § 6 KDO (KDO-DVO)
    - KDO-DVO bleibt längstens bis zum 30.06.2019 in Kraft, soweit sie den Regelungen des KDG nicht entgegenstehen

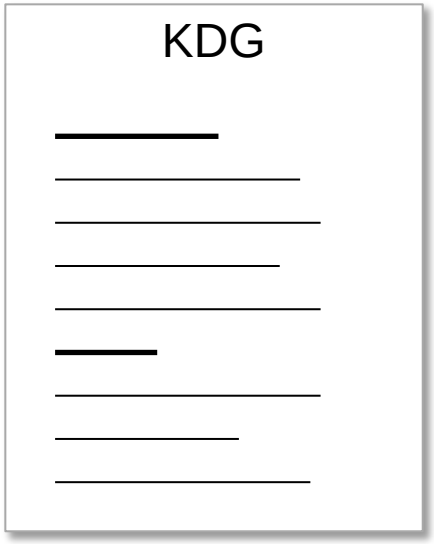
2. TOMs und Technik in der KDG

2.6. Zeitplan

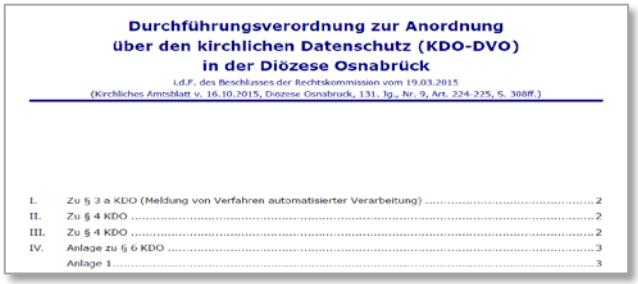


2. TOMs und Technik in der KDG

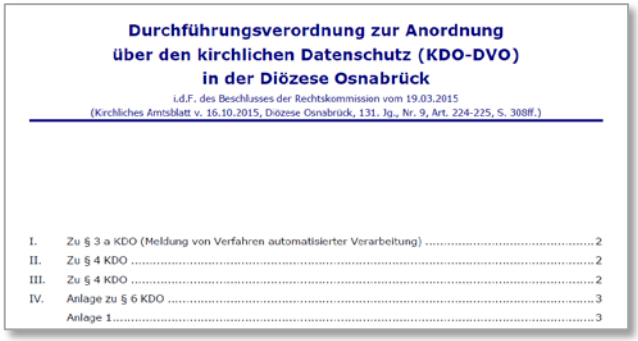
2.7 „Zustand“ ab 24.05.2018



KDG



Anlage 1 zu § 6 KDO („8 Gebote“)



Anlage 2 zu § 6 KDO (Einsatz von APC)

Anlage zu Anlage 2 zu § 6 KDO (IT-Richtlinien, „Mindeststandard für kirchlichen Datenschutz“)

KDO-DVO

E. Grundlagen der rechtlichen Prüfung

1. Prüfungsmaßstab

1.1. Datenschutzkonzept

- Anforderung des Datenschutzkonzepts
- Pflicht zur Erstellung eines Datenschutzkonzeptes ergibt sich aus Anlage 2 zu § 6 KDO-DVO (Punkt 3.2)
  - „Der Dienststellenleiter stellt sicher, dass ein Konzept zur datenschutzrechtlichen Ausgestaltung der Datenverarbeitungsanlagen erstellt wird.“
- Prüfung u.a. auf Vollständigkeit sowie Einhaltung der Mindestanforderungen
- Beispiel für die Gliederung eines Datenschutzkonzeptes:

1. Prüfungsmaßstab

Inhaltsverzeichnis

1. Prüfungsmaßstab

1. Prüfungsmaßstab

1. Prüfungsmaßstab

1.2. Verfahrensverzeichnis

- Angefordert wird ebenfalls das Verfahrensverzeichnis nach § 3a Abs. 2 KDO bzw. Verzeichnis von Verarbeitungstätigkeiten nach § 31 KDG
- Prüfung auf Vollständigkeit, Richtigkeit und Einhaltung/Umsetzung der dort beschriebenen Verfahren

F. Grundlagen der technischen Prüfung

1. Prüfungsmaßstab

1.1. Gesetzliche Vorgaben

- Gesetzliche Vorgaben finden sich in
  - § 6 KDO bzw. § 26 KDG sowie
  - IT-Richtlinien zur Umsetzung von IV. Anlage 2 zu § 6 KDO der KDO-DVO
  - Anlage 1 zu § 6 KDO der KDO-DVO („8-Gebote“)

1. Prüfungsmaßstab

1.2. Allgemeine Grundsätze

- Wer ist der Dienststellenleiter?
- Welche schutzwürdigen Daten werden verarbeitet und welchen Schutzklassen sind diese zugeordnet? (1, 2 oder 3)
- Wurde ein Datenschutzkonzept und ein Verfahrensverzeichnis erstellt?

2. „8-Gebote“

2.1. Zutrittskontrolle

- Umfasst Sicherungsvorkehrungen, die den ungehinderten Zutritt zu den physischen Räumlichkeiten der Datenverarbeitungs-vorgänge beschränken
- **Serverseitig getroffene Zutrittskontrollmaßnahmen:**
  - Werden personenbezogene Daten auf Ihren oder in Ihrem Auftrag betriebenen Server gespeichert?
  - Ist der der Serverraum Fensterlos?
  - Wer hat Zutritt zu dem Server bzw. zu den EDV-Anlagen?
  - Wie ist die Zutrittskontrolle bzw. Berechtigung geregelt?
  - In welchen Etage steht der Server bzw. die NW-Räume?

2. „8-Gebote“

2.1. Zutrittskontrolle

- **Clientseitig getroffene Zutrittskontrollmaßnahmen:**
  - Ist das Bürogebäude vollständig umfriedet?
  - Existiert ein Pförtnerdienst?
  - Welche Zutrittsregelung gibt es für Betriebsfremde?
  - Wird ein Besucherbuch geführt?
  - Existieren mechanische oder elektr. Schließsysteme?
  - Sind Zutrittsberechtigungen vergeben und wenn ja welche?

2. „8-Gebote“

2.2. Zugangskontrolle

- Umfasst Sicherungsvorkehrungen, die den Zugang zu den Datenverarbeitungssystemen verhindert, wenn die Zutrittskontroll-maßnahmen überwunden wurden
  - Existiert ein persönliches Passwort?
  - Wie lauten die Passwort Vorgaben? (Länge, Sonderzeichen)
  - Gibt es eine Begrenzung der Anmeldeversuche?
  - Besteht ein eigenständiger Admin-Account?
  - Wie sind Fernzugänge externer DL gesichert?
  - Gibt es einen Auftragsdatenverarbeitungsvertrag mit DL?

2. „8-Gebote“

2.3. Zugriffskontrolle

- Umfasst Sicherungsvorkehrungen, die den Zugriff berechtigter bzw. unberechtigter Nutzer auf oder die Löschung von bestimmten, fest definierten Daten regeln
  - Existiert ein Berechtigungskonzept für den Zugriff?
  - Wie werden die Zugriffsberechtigungen vergeben?
  - Wie werden Datenträger bzw. Unterlagen entsorgt?
  - Kommt ein externer DL zum Einsatz?
  - Wenn ja, besteht ein Auftragsdatenverarbeitungsvertrag?
  - Dürfen Ihre MA eigene Speichermedien verwenden?

2. „8-Gebote“

2.4. Weitergabekontrolle

- Umfasst Sicherungsvorkehrungen zum Schutz vor unbefugtem Lesen, Kopieren, Ändern oder Entfernen eines Datenträgers sowie beim Transfer von Daten an interne wie an externe Empfänger
  - Werden elektronisch übertragende Daten verschlüsselt?
  - Werden die Übertragungsvorgänge protokolliert?
  - Werden Daten auf mobile Geräte verarbeitet?
  - Dürfen Daten an private E-Mail-Adressen geleitet werden?
  - Verarbeiten MA Daten auf eigenen privaten Geräten?
  - Sind Nutzer schriftlich auf die IT-Richtlinien verpflichtet?

2. „8-Gebote“

2.5. Eingabekontrolle

- Die Eingabekontrolle ermöglicht eine nachträgliche Überprüfung, welche personenbezogenen Daten zu welcher Zeit, von wem in den Datenverarbeitungssytemen eingegeben oder verändert wurden
  - Werden Zugriffe (Lesen, Ändern, Löschen) protokolliert?
  - Wie lange werden diese Protokolldaten aufbewahrt?
  - Werden die Protokolle ausgewertet?
  - Ist der letzte Zugriff auf die Daten feststellbar? (Uhrzeit/Datum/Änderung)

2. „8-Gebote“

2.6. Auftragskontrolle

- Die Auftragskontrolle dient der Sicherung das personenbezogene Daten von Mitarbeitern und externen Dienstleistern vertraulich und entsprechend den gesetzlichen Vorgaben verarbeitet werden
  - Werden MA nachweislich im Datenschutzrecht geschult?
  - Werden MA schriftlich auf das Datengeheimnis verpflichtet?
  - Werden externe Dienstleister für Verarbeitungen eingesetzt?
  - Sind mit diesen Verträge abgeschlossen worden?
  - Wird die Einhaltung dieser Maßnahmen in regelmäßigen Abständen geprüft und das Ergebnis dokumentiert

2. „8-Gebote“

2.7. Verfügbarkeitskontrolle

- Die Verfügbarkeitskontrolle betrifft Maßnahmen, die den Verlust oder die Zerstörung von erhobenen Daten schützen
- **Serverseitig getroffene Verfügbarkeitskontrollmaßnahmen**
  - Verfügt der Serverraum über eine feuerfeste Zugangstür?
  - Ist der Serverraum mit Rauchmeldern ausgestattet?
  - Ist der Serverraum mit Löschsystemen ausgestattet?
  - Ist der Serverraum Klimatisiert?
  - Verfügt der Serverraum über eine Stromunterbrechungsfreie Stromversorgung (USV)?

2. „8-Gebote“

2.7. Verfügbarkeitskontrolle

- **Backup Konzepte**
  - Existiert ein dokumentiertes Backup Konzept?
  - In welchem Rhythmus werden Backups angefertigt?
  - Welche Sicherungsmedien werden für die Backups genutzt?
  - Wo werden die Backups aufbewahrt?
  - Sind die Daten der Sicherung / Backups verschlüsselt?
  - Wird die Funktion der Wiederherstellung getestet?

2. „8-Gebote“

2.7. Verfügbarkeitskontrolle

- **Allgemeine Verfügbarkeitskontrollmaßnahmen**
  - Wie sind Ausdrucke von Datenbeständen vor gleichzeitigen Vernichtung mit den Originaldaten geschützt?
  - Sind die IT Systeme vor Datenverlust geschützt? (Virenschutz, Anti-Spyware, Firewall)
  - Existiert ein dokumentiertes Notfallkonzept? Bspw. Notfallmaßnahmen bei Brand, Totalverlust der Daten, Hardwaredefekt etc.?

2. „8-Gebote“

2.8. Trennungsgebot

- Das Trennungsgebot enthält die Verpflichtung, zu unterschiedlichen Zweck erhobene personenbezogene Daten getrennt von einander verarbeiten zu können
  - Wie sind die zu verschiedenen Zwecken erhobenen Daten voneinander getrennt?
  - Durch logische oder physische Datentrennung?

    Z.B. eine Datenbank mit Mandanten-Zugriffsberechtigungen oder mit mehreren Datenbankensystemen.

Vielen Dank für die Aufmerksamkeit!

Kontakt:

https://www.datenschutz-kirche.de/

Telefon: 0421 - 16301925

a.bloms@datenschutz-katholisch-nord.de

d.friedemann@datenschutz-katholisch-nord.de

Referenten:

Andreas Bloms

Daniel Friedemann