

# Einführungshilfe für den betrieblichen Datenschutzbeauftragten nach § 36 KDG

Überarbeitungsstand 18.04.2020

**Soweit Sie neu anfangen: Vielen Dank für Ihre Bereitschaft zur Übernahme ihres neuen Amtes und herzlichen Glückwunsch zu Ihrer Bestellung als betrieblicher Datenschutzbeauftragter!  
Sonst: Vielen Dank für Ihre Mühe!**

Dieses Dokument ist für das Lesen am Bildschirm konzipiert, da die Links dann sofort aus dem Textprogramm aufgerufen werden können (Strg + Linksklick). Eine recht gute Informationsquelle ist auch der Wikipedia-Artikel zum Datenschutz (<http://de.wikipedia.org/wiki/Datenschutz>). Für alle betrieblichen Datenschutzbeauftragten – und noch einige Interessierte mehr - in Bayern gibt es auch die gemeinsame Downloadseite, die Sie mit

[www.erzbistum-muenchen.de/datenschutz/](http://www.erzbistum-muenchen.de/datenschutz/)

aufrufen können. Auf der linken Seite finden Sie das: Klicken Sie dort auf das Wort **Downloadbereich**. Es öffnet sich eine neue Seite.



ERZDIÖZESE MÜNCHEN  
UND FREISING

Kind

## Gemeinsame Datenschutzaufsicht der bayerischen (Erz-) Diözesen

### Datenschutzaufsicht

Konferenz der  
Diözesandatenschutz-  
beauftragten

Kirchliches Datenschutzgesetz,  
DurchführungsVO und  
Praxishilfen

Downloadbereich

Leitende betriebliche DSB

### Gemeinsame Datenschu



Jupp Joachimski,  
Datenschutzbeauftragter



Datenschutzstelle	Suche ...
<p><b>Datenschutzaufsicht</b></p> <p>Konferenz der Diözesandatenschutz- beauftragten</p> <p>Kirchliches Datenschutzgesetz, DurchführungsVO und Praxishilfen</p> <p>► <b>Downloadbereich</b></p> <p>Leitende betriebliche DSB</p>	<p>Downloads in einzelnen Ordnern:</p> <p>Hier finden Sie erst einmal Material, das für alle Bereiche bedeutsam <b>Allgemeines</b></p> <p>Vorformulierte Muster für verschiedene Erklärungen sollen die Arbei- Datenschutz erleichtern: <b>Muster für verschiedene Erklärungen</b></p> <p>In den Pfarrbüros fallen besonders viele Datenschutzprobleme an. <b>Material für Kirchenstiftungen</b></p>

Hier finden Sie nach dem Wort **Downloadseite** gleich die wichtigsten Dokumente und darunter Links zu weiteren Ordnern mit Dokumenten. Schauen Sie sich bitte alles an und öffnen Sie auch einmal die Ordner weiter unten! Grundsätzlich wäre nichts dagegen einzuwenden, wenn Sie sich alles einmal ausdrucken lassen und in einem Ordner sammeln. Besonders wichtiger Inhalt:

- Kirchliches Datenschutzrecht (Ordner „Allgemeines“)
- Merkblatt Kirchlicher Datenschutz in Bayern, z.B. für Belehrungen
- Informationen für Pfarrbüros; hier auch [unten](#) abgedruckt
- Informationen für Kindertageseinrichtungen
- Erklärungsmuster

Neben dieser offiziellen führe ich für viele Kollegen und Freunde noch eine private Webseite, auf der ein [Internetportal](#) mit stark rechtlichem Einschlag steht. Wenn Sie sich also einmal mit Rechtsfragen befassen und ggfs. Gesetze einsehen müssen, kann das hilfreich sein. Allerdings sind dort durchaus auch viele Links für das „normale“ Leben enthalten.

**Datenschutzbeauftragte an kirchlichen Schulen sollten sich zusätzlich die [Handreichung für Datenschutzbeauftragte an staatlichen Schulen](#) herunterladen, die weitere gute Anhaltspunkte bieten.**

## A. Die rechtlichen Grundlagen des Datenschutzrechts

behandle ich hier nicht mehr. Sie finden alles Wichtige im Dokument „Kirchliches Datenschutzrecht“, dessen Durcharbeitung ich hier voraussetze.

## B. Kirchliches Datenschutzrecht im Einzelnen

### Vorbemerkung:

Wer das KDG mit der EU-DS-GVO vergleicht, wird schnell feststellen, dass sich viele inhaltsgleiche Regelungen finden. Die Begriffe des KDG können also auch an Hand eines Kommentars zur EU-DS-GVO geklärt werden. Leider gibt es noch keinen Kommentar zum KDG.

Für Begriffsklärungen muss man daher z. B. auf die folgenden Kommentare zur EU-DS-GVO zurückgreifen:

- Gola/Schomerus, EU-DS-GVO und BDSG, Beck-Verlag

- Paal/Pauly, EU-DS-GVO, 2.Auflage 2018, Beck-Verlag

Die aktuelle Fassung des KDG können Sie auf der [Seite des EOM](#) herunterladen.

## 1. Was gehört zum Datenschutz?

Hierüber gingen früher die Meinungen auseinander. Vielfach wurde unter dem Begriff „Datenschutz“ vor allem der Schutz sensibler wissenschaftlicher Erkenntnisse vor Ausbeutung durch andere gesehen. Mittlerweile ist unter dem Begriff nur noch der Schutz personenbezogener Daten natürlicher lebender Personen zu verstehen.

Es müssen natürliche Personen betroffen sein, das heißt, dass Vereine oder Gesellschaften des Handelsrechts wie öffentlich-rechtliche Körperschaften keinen Datenschutz genießen. Da der Datenschutz lediglich für lebende Personen eingreift, genießen Verstorbene auch keinen Datenschutz.

Zum Datenschutz gehören drei Komponenten:

### a. Datensicherheit

Daten müssen so aufbewahrt werden, dass sie bei Bedarf zur Verfügung stehen. Sie müssen Vorkehrungen gegen eine zufällige Löschung oder ein sonstiges Abhandenkommen getroffen werden.

### b. Schutz gegen unbefugte Kenntnisnahme

Personenbezogene Daten sind nur für bestimmte Zwecke zu erheben, zu speichern und weiterzugeben. Nur die dazu Berechtigten dürfen von ihnen Kenntnis nehmen.

### c. Auskunftspflicht

Der Betroffene, dessen Daten erhoben, gespeichert oder weitergegeben werden, hat grundsätzlich ein Auskunftsrecht über all diese Vorgänge. Die Auskunftspflicht ist unmittelbar mit der Datenerhebung verbunden.

## 2. Woher kommt der Datenschutz?

Während das kirchliche Recht im [corpus iuris canonici](#) schon seit 1230 Datenschutzbestimmungen kennt, waren solche dem Grundgesetz bis 1980 fremd. Bei der Schaffung des Grundgesetzes spielte der Gedanke des Datenschutzes keine Rolle.

1970 verabschiedete Hessen das [weltweit erste Datenschutzgesetz](#); 1977 folgte das deutsche [Bundesdatenschutzgesetz](#) (BDSG), die Schwerpunkte lagen in der Bestimmung der Voraussetzung für die Einführung von [Datenschutzbeauftragten](#) und der Vorrangstellung des Schutzes personenbezogener Daten. Landesdatenschutzgesetze waren 1981 für alle Bundesländer beschlossen.

Erst das [Volkszählungsurteil des Bundesverfassungsgerichts](#) vom 15.12.1983 schuf das (Grund-) Recht des Einzelnen auf informationelle Selbstbestimmung (vgl. Arbeitshilfe 206, S.57). Seit 1980 existieren mit den OECD [Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data](#) international gültige Richtlinien, welche die Ziele haben, die mitgliedstaatlichen Datenschutzbestimmungen weitreichend zu harmonisieren, einen freien Informationsaustausch zu fördern, ungerechtfertigte Handelshemmnisse zu vermeiden und eine Kluft insbesondere zwischen den europäischen und US-amerikanischen Entwicklungen zu verhindern.

1981 verabschiedete der Europarat mit der [Europäischen Datenschutzkonvention](#) eines der ersten internationalen Abkommen zum Datenschutz. Die Europäische Datenschutzkonvention ist bis heute in Kraft, sie hat jedoch lediglich empfehlenden Charakter. Dagegen sind die Datenschutzrichtlinien der Europäischen Union für die Mitgliedstaaten verbindlich und in nationales Recht umzusetzen.

### 3. Der Geltungsbereich des Kirchlichen Datenschutzgesetzes

#### a. In räumlicher Hinsicht:

Das KDG wird vom jeweiligen Diözesanbischof für den Bereich seiner Diözese erlassen. Sie gilt im Prinzip auch nur in diesem Bereich; allerdings wird in anderen Diözesen ein wortgleiches KDG angewandt. Entsprechendes gilt für den Bereich der Orden päpstlichen Rechts. Sie erlassen ihre eigene Kirchliche Datenschutzregelung für Ordensgemeinschaften (KDR-OG) durch den Ordensoberen und ernennen einen eigenen Ordensdatenschutzbeauftragten. Orden bischöflichen Rechts unterstehen dagegen uneingeschränkt dem Diözesan-KDG.

#### b. Sachlich:

Das KDG gilt nach seinem § 2 Abs.2 Nrn.1 und 2 uneingeschränkt für alle kirchlichen Dienststellen und die Dienststellen der Caritas. Bei den sonstigen kirchlichen Körperschaften, Stiftungen, Anstalten, Werken und Einrichtungen der Nummer 3 ist eine differenzierte Betrachtungsweise angebracht. Sie sind zwar dem KDG unterworfen, doch ist eine so genannte Kirchlichkeitsprüfung erforderlich: Diese Einrichtungen unterliegen dann dem KDG, wenn sie nach kirchlichen Selbstverständnis ihrem Zweck oder ihrer Aufgabe entsprechend zur Mitwirkung an der Erfüllung des kirchlichen Auftrags berufen sind. Reine Gewerbebetriebe scheiden demnach auch bei kirchlicher Trägerschaft aus dem Bereich des KDG aus.

### 4. Die Hauptprinzipien des Datenschutzes

- Datensparsamkeit oder Datenvermeidung: *Je weniger Daten erhoben werden, umso besser! Die Folge daraus: Der Datenschutzbeauftragte wird in der Regel nicht gerne angeben, wie lange Daten gespeichert werden müssen. Für den Datenschutz ist es immer besser, wenn die Daten gar nicht erst gespeichert werden oder schnell gelöscht werden. Es gibt allerdings Fristen, innerhalb derer in der Regel die Daten nicht gelöscht werden sollten. Für Sozialdaten gibt es eine recht gute Aufstellung unter <http://www.datenschutz-kirche.de/node/55>.*
- Erforderlichkeit - §§ 7 Abs. 1 b, c KDG: *Auch wenn eine gesetzliche Grundlage zur Datenerhebung und -speicherung vorliegt, dürfen nur solche Daten gespeichert werden, die zur Erreichung des Zwecks der speichernden Stelle nötig sind. Die Erforderlichkeit im Sinne des § 7 Abs. 1 bestimmt sich nach objektiven Kriterien. Erforderlich sind demnach alle Daten, die sinnvollerweise benötigt werden, um den Anforderungen der jeweiligen Stelle gerecht zu werden. Nicht notwendig ist es, dass im konkreten Fall wirklich auch alle erhobenen Daten unerlässlich sind. Auch ein Irrtum über die Erforderlichkeit ist unschädlich.*
- Zweckbindung *Daten dürfen nur zu den gesetzlich vorgesehenen Zwecken gespeichert werden. Dies ist aber nur eine Seite des Grundsatzes: Auf der anderen Seite gilt die Regel, dass die Daten auch nur für den vorgesehenen Zweck verwendet werden dürfen. Beispiel: Wurden Bankdaten für die Lohnbuchhaltung von den Beschäftigten erhoben, so dürfen diese Daten nicht ohne weiteres dazu verwendet werden, festzustellen, ob der Beschäftigte zum Beispiel Geld seiner Dienststelle auf sein eigenes Konto überweist.*

### 5. Schutzbereiche kirchlichen Datenschutzes

Sie müssen immer beachten, dass das Datenschutzrecht in zwei Richtungen wirkt: Zum einen bestimmt es das Verhältnis zwischen dem kirchlichen Dienstgeber und den Dienstnehmern, zum anderen das Verhältnis zwischen den Dienstnehmern und den Klienten, also zum Beispiel den Kirchen- und Gemeindegliedern, Schülern kirchlicher Schulen, Ministranten, usw.

Während der Datenschutz für die Klienten in des KDG recht detailliert geregelt ist, fehlen Aussagen zum Mitarbeiterdatenschutz weitgehend. Das liegt daran, dass auch im staatlichen Bereich der Mitarbeiterdatenschutz kaum gesetzlich geregelt ist und die vorhandene gesetzliche Regelung auf Gerichtsurteilen basiert.

#### a. Mitarbeiterdatenschutz

Gegenwärtig gibt es nur die Regelung in § 53 KDG. Sie entspricht dem § 26 BDSG, welcher allerdings die Worte „einschließlich der religiösen Überzeugung“ nicht enthält. Im Übrigen ist im Hinblick auf den Mitarbeiterdatenschutz das bisherige Richterrecht anzuwenden. Seine Grundsätze sind:

- *Alle Daten müssen grundsätzlich beim Mitarbeiter erhoben werden.*
- *Der Dienstgeber darf nur solche Daten erheben, die zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder gesetzlich vorgesehen sind.*
- *Der Grundsatz der Zweckbindung ist streng zu beachten.*
- *Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Mitarbeiters führen kann, ist unzulässig.*
- *Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.*
- *Dem Dienstgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung bekannt gegeben werden.*
- *Den Mitarbeitern sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen.*

Von besonderer Bedeutung für die Tätigkeit des betrieblichen Datenschutzbeauftragten in diesem Zusammenhang ist die Aufbewahrung von Personalakten in der Dienststelle. Der betriebliche Datenschutzbeauftragte muss deren Sicherheit prüfen und darauf hinwirken, dass Personalakten ordentlich verschlossen aufbewahrt werden. Den Maßstab hierfür liefert § 26 KDG.!

#### b. Klientendatenschutz

Klienten in diesem Sinne sind alle Personen, deren Daten von kirchlichen Stellen gehalten werden. Im Prinzip gehören die Beschäftigten ebenso dazu, doch gelten für diese Sonderregelungen.

Die größte Bedeutung hat der Schutz der Klientendaten beim so genannten Seelsorgegeheimnis. Das Kirchenrecht verpflichtet den Seelsorger zur Wahrung des Beicht- und Seelsorgegeheimnisses. Seelsorger in diesem Sinne ist jeder hauptamtlich mit Seelsorgeaufgaben Betreuer; auf eine Weihe kommt es nicht an. Der Klientendatenschutz beschränkt sich jedoch nicht auf die Seelsorge, sondern gilt unmittelbar für alle Vorgänge, bei denen kirchliche Dienststellen mit den Daten natürlicher Personen zu tun haben.

#### **Beispiele:**

*Die Kirchenstiftung hat Zugriff auf die Meldedaten, weil sie feststellen muss, wer zu ihrer Gemeinde gehört. Lehrer an kirchlichen Schulen haben Zugriff auf die Daten ihrer Schüler und deren Eltern.*

*Das Personal kirchlicher Krankenhäuser nutzt die Daten der Patienten.*

Die Arbeitshilfe 206 erläutert im Einzelnen in die Anforderungen an den Datenschutz, so dass hier auf weitere Ausführungen in diesem Zusammenhang verzichtet werden kann. Ein Punkt allerdings konnte der Arbeitshilfe zu kurz weg:

#### **Der Schutz des Seelsorgegeheimnisses im strafrechtlichen Verfahren:**

Aus dem Seelsorgegeheimnis resultiert für das Strafverfahren ein Zeugnisverweigerungsrecht des Geistlichen. Geistlicher in diesem Sinne ist nach der Rechtsprechung des Bundesgerichtshofes und des Bundesverfassungsgerichts aber auch der Laie, der hauptamtlich mit Seelsorgeaufgaben betraut ist (BGH NJW 2007, 307 und BVerfG NJW 2007, 1865). Allerdings ist das Zeugnisverweigerungsrecht teilbar: Es bezieht sich nur auf Vorgänge im Rahmen eines seelsorgerischen Gesprächs, nicht auf solche, die nur anlässlich eines solchen geschahen.

Daneben sind kirchliche Angestellte nur bei Vorliegen einer Aussagegenehmigung ihrer Dienststelle zur Aussage verpflichtet, weil § 54 StPO auch für sie gilt (OLG Köln StraFo 1999, 90, für Mitarbeiter in Beratungsstellen aber umstritten). Die Aussagegenehmigung ist durch das Strafgericht zu erholen.

#### **Verhältnis der neuen Kirchlichen Archivordnung zum KDG**

- Die KAO geht dem KDG insofern vor, als die Archivierung ein sog. Löschungssurrogat ist, d.h.:

- Statt zu löschen wird der Vorgang dem Archiv angeboten: Das erscheint auf den ersten Blick paradox, ist es aber nicht. Sogar die Strafprozessordnung erkennt die Archivierung nämlich als sog. Löschungssurrogat an.
- Auskunft darf nicht mehr erteilt werden, § 17 Abs.6 KDG

## 6. Andere für kirchliche Dienststellen bedeutsame gesetzliche Regelungen

**Bilder und Filme:** Sie enthalten keine personenbezogenen Daten im engeren Sinne; deswegen gibt es in [§ 22 Kunsturhebergesetz](#) entsprechende Regelungen. Im Prinzip bedarf jede Veröffentlichung von Bildern mit Personen deren Einwilligung. Die wichtigste Ausnahme hierfür enthält § 23 Abs. 1 Nr.3:

*Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;*

Beachten Sie aber, dass diese Voraussetzung nur dann gilt, wenn das Geschehen der Veranstaltung und nicht die Personen im Fokus stehen. Sicherheitshalber wenden wir die Vorschrift nur an, wenn

- mindestens 8 Personen auf dem Bild sind und
- das Bild nicht gestellt ist.

Für den Bereich von Schulen und Kindertageseinrichtungen gibt es in der Downloadseite Erklärungsvordrucke, die Sie den Einrichtungen überlassen sollten.

**Sozialdaten:** Hier gelten kraft bischöflicher Anordnung in der freien Jugendhilfe in kirchlicher Trägerschaft die staatlichen Vorschriften entsprechend. Sozialdaten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener), die von einer in § 35 des SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden. Beachten Sie dazu die Ausführungen in der Arbeitshilfe.

Die **beruflichen Geheimhaltungsvorschriften** des [§ 203 Strafgesetzbuch](#) sind zusätzlich zu beachten.

## C. Die Datenschutzbeauftragten der Kirche

### 1. Der Diözesandatenschutzbeauftragte

- ist der kirchliche, vom Bischof für seine Diözese oder von den zuständigen Bischöfen für ihre Diözesen bestellte Datenschutzbeauftragte
- wacht über die Einhaltung der kirchlichen Datenschutzanordnung sowie kirchlicher und staatlicher Vorschriften über den Datenschutz im Bereich der Katholischen Kirche....
- und zwar unabhängig davon, ob dieser
  - öffentlich-rechtlich (z. B. Kirchengemeinde als Körperschaft des öffentlichen Rechts) oder
  - „nicht öffentlich-rechtlich“ organisiert ist (z. B. eingetragene Vereine, Stiftungen, Anstalten oder Gesellschaften des privaten oder katholischen Rechts).

#### **Sonderfall: Orden päpstlichen Rechts**

Die Orden päpstlichen Rechts unterstehen nicht dem Diözesanbischof und damit auch im Datenschutz nicht dem Diözesandatenschutzbeauftragten. Ob ein Orden nach päpstlichem oder bischöflichem Recht gegründet wurde, lässt sich leicht auf der [Webseite der deutschen Ordensobernkongferenz](#) feststellen. Orden päpstlichen Rechts haben statt des Diözesandatenschutzbeauftragten einen eigenen Ordensdatenschutzbeauftragten; dieser sollte auf der Webseite des Ordens genannt sein. Daneben kann und soll es - wie in den Bistümern - betriebliche Datenschutzbeauftragte, z.B. für einzelne Häuser, geben.

### 2. Der betriebliche Datenschutzbeauftragte

wurde mit des KDG 2003 eingeführt.

#### **a. Notwendigkeit der Bestellung**

- § 36 KDG beschreibt, unter welchen Voraussetzungen ein betrieblicher Beauftragter für den Datenschutz bestellt werden soll und kann.
- Seine Berufung schmälert nicht die Aufgaben und Rechte des Diözesandatenschutzbeauftragten.
- Schon mit der Änderung 2011 wurde aus der ursprünglichen Kannvorschrift eine Sollvorschrift. Sie ist – wie alle Sollvorschriften - innerdienstlich bindend!

- Um nicht ständig auf Personalschwankungen reagieren zu müssen, wurde den Kirchenstiftungen geraten, sich dekanatsweise auf einen betrieblichen DSB zu einigen.
- Nach § 36 Abs. 1 KDG müssen Dienststellen der verfassten Kirche betriebliche Beauftragte für den Datenschutz bestellen.
- Verbände wie z.B. die Caritas und Orden müssen unter den Voraussetzungen des § 36 Abs. 2 a, b oder c einen betrieblichen Datenschutzbeauftragten bestellen.
- Die Nichtbestellung eines betrieblichen Datenschutzbeauftragten kann zur Beanstandung durch die Datenschutzaufsicht, im Extremfall sogar zur Verhängung einer Geldbuße gegen den Verantwortlichen führen.

### **b. Voraussetzungen der Bestellung**

Zum betrieblichen Beauftragten für den Datenschutz darf nur bestellt werden, wer die erforderliche „Fachkunde und Zuverlässigkeit“ besitzt. Der betriebliche Datenschutzbeauftragte muss also sowohl die technische als auch die rechtliche Seite seiner Aufgaben kennen und Kenntnisse in allen Bereichen haben, die für die Organisation, in der er arbeitet, von Bedeutung sind. Allerdings sollten diese Anforderungen nicht überspitzt werden: An technischen Kenntnissen genügen normale Anwenderkenntnisse; die rechtlichen Kenntnisse sollten den betrieblichen Datenschutzbeauftragten in den vom Ordinariat angebotenen Schulungen vermittelt werden, soweit er sie sich nicht selbst anhand der Arbeitshilfen aneignen kann.

Das sollte er am Schluss der Einarbeitung wissen:

#### A. Grundlagen der Arbeit

1. Struktur kirchlicher Entscheidungen
2. Kirchliche Gesetzgebung / verfassungsrechtliche Grundlagen
3. Subsidiaritätsprinzip (§ 2 Abs. 2 KDG) / Zusammenspiel mit staatlichen Gesetzen

#### B. Rechtliche Aspekte

1. KDG inkl. DVO und der KDSGO
2. Nebengesetze (KMAO, KAO, andere diözesane Regelungen)
3. Einschlägige Regelungen der nichtkirchlichen Gesetze (z.B. SGB, BMG, DSGVO, EU-DS-GVO)
4. Unterschiede zwischen KDG und DSGVO bzw. dem BDSG
5. Spezialfall: Auftragsverarbeitung / Funktionsübertragung

#### C. Technische Aspekte

1. Grundlagen der IT
2. Aspekte der IT-Sicherheit
3. Technisch-organisatorische Schutzmaßnahmen
4. Grundlegendes Verständnis von BSI-Grundschutz / ISO 2700x / ISIS 12

#### D. Organisation der Arbeit

##### 1. Rechte des bDSB

- 1.1. Kündigungsschutz
- 1.2. Direkter Berichtsweg zur Leitung der Einrichtung
- 1.3. Notwendigkeit der Einbindung in die Prozesse der Einrichtung / Beteiligung nach § 38 Satz 2 Buchst. a KDG)
- 1.4. Einsichtsrechte

##### 2. Pflichten des bDSB

- 2.1. Verschwiegenheitspflicht nach § 43 Abs. 9 KDG
- 2.2. Meldepflicht nach § 36 Abs. 4 KDG
- 2.3. Fortbildung / Erhalt der Fachkunde nach § 37 Abs. 2 KDG
- 2.4. Überwachung ordnungsgemäße Anwendung DV-Programme (§ 38 Satz 2 Buchst. a KDG)
- 2.5. „Vertraut machen“ der Mitarbeiter / Mitarbeiterinnen (Schulung) mit Regelungen (§ 38 Satz 2 Buchst. c KDG)

##### 3. Vernetzungsmöglichkeiten und -pflichten des bDSB

- 3.1. ... mit internen Stellen (z.B. MAV, Revision, Rechtsabteilung oder QM)
- 3.2. ... mit der Aufsicht (§ 38 Satz 1 und Satz 2 Buchst. e KDG)
- 3.3. ... mit anderen externen Stellen (z.B. Arbeitskreise, Erfahrungsaustauschkreise)

##### 4. Wichtige „Werkzeuge“

- 4.1. Bestandsaufnahme / Schwachstellenanalyse
- 4.2. Verfahrensverzeichnis
- 4.3. Datenschutzfolgenabschätzung
- 4.4. Dokumentation der Datenverarbeitung (Accountability) für die Arbeit des bDSB nutzen
- 5. Beherrschung des Handwerkszeuges
  - 5.1. Empfehlung zur risikoorientierten Herangehensweise an die Bewertung von Sachverhalten im Datenschutz / Erstellung + Umsetzung individueller Maßnahmenkatalog
  - Informationsquellen finden und nutzen

### **c. Vorgang der Bestellung des betrieblichen Datenschutzbeauftragten**

Bestellt wird der betriebliche Datenschutzbeauftragte vom jeweiligen Dienststellenleiter, also z.B. vom Direktor der kirchlichen Schule oder vom Geschäftsführer eines kirchlichen Verbandes. Etwas komplizierter ist die Bestellung des betrieblichen Datenschutzbeauftragten für mehrere Kirchenstiftungen innerhalb eines Dekanats. In diesem Fall müssen alle Kirchenverwaltungsvorstände die Bestellung vornehmen. Als Anhaltspunkt mag das folgende Muster gelten:

#### **Muster für die Bestellung zum/zur gemeinsamen betrieblichen Datenschutzbeauftragten für alle Kirchen- und Pfründestiftungen eines Dekanats und für den Dekanatssitz:**

Herrn/ Frau  
Vor- und Zuname  
Anschrift

#### **Bestellung zum/zur betrieblichen Datenschutzbeauftragten**

Sehr geehrte/r Frau / Herr .....

die Versammlung der Kirchenverwaltungsvorstände in ... vom ... hat Sie mit sofortiger Wirkung gemäß § 20 der Anordnung über den kirchlichen Datenschutz (KDG) zum/zur betrieblichen Datenschutzbeauftragten für alle im Katholischen Dekanat .....<sup>1</sup> gelegenen Kirchen- und Pfründestiftungen einschließlich deren etwaiger rechtlich unselbständiger Einrichtungen sowie für den Dekanatssitz bestellt. Die Bestellung gilt – vorbehaltlich der Möglichkeit der Verlängerung - für vier Jahre.

In Ihrer Funktion als betriebliche/r Datenschutzbeauftragte/r sind Sie dem Dekan des Dekanats ..... sowie den Kirchenverwaltungsvorständen und Pfründeinhabern der im Katholischen Dekanat ..... gelegenen Kirchen- und Pfründestiftungen unmittelbar unterstellt.

Ihre Aufgaben als betriebliche/r Datenschutzbeauftragte/r ergeben sich aus des KDG.

In Anwendung Ihrer Fachkunde auf dem Gebiet des Datenschutzes sind Sie weisungsfrei.

....., den .....  
(Ort, Datum)

<sup>2</sup>Für das Katholische Dekanat .....

.....  
(Vor- und Zuname)  
Dekan

Für die in der Pfarrei ..... gelegenen Kirchenstiftungen aufgrund Kirchenverwaltungsbeschlüssen vom .....<sup>3</sup> und Pfründestiftungen:

<sup>1</sup> Dekanat ergänzen.

<sup>2</sup> Die Bestellung muss vom jeweiligen Dekan sowie von allen Kirchenverwaltungsvorständen und Pfründeinhabern, der im jeweiligen Dekanat gelegenen Kirchen- und Pfründestiftungen, unterzeichnet werden.

<sup>3</sup> Bitte Datum der zugrunde liegenden Kirchenverwaltungsbeschlüsse einfügen.

.....  
 (Vor- und Zuname)  
 Kirchenverwaltungsvorstand und Pfründeinhaber

Für die in der Pfarrei ..... gelegenen Kirchenstiftungen aufgrund Kirchenverwaltungsbeschlüssen vom .....<sup>4</sup> und Pfründestiftungen:

.....  
 (Vor- und Zuname)  
 Kirchenverwaltungsvorstand und Pfründeinhaber

Der Dienststellenleiter (beziehungsweise der Dekan bei der Bestellung eines Dekanatsbeauftragten) setzt den neuen betrieblichen Datenschutzbeauftragten von der Bestellung in Kenntnis und teilt die Bestellung allen ggfs. vorhandenen Untergliederungen der Dienststelle - z.B. Kirchenstiftungen - mit. In kirchlichen Schulen setzt der alle Lehrer von der Bestellung in Kenntnis.

#### **d. Auswirkungen der Bestellung**

##### Verhältnis zur Dienststellenleitung

Der betriebliche Datenschutzbeauftragte ist dem Leiter der kirchlichen Stelle unmittelbar zu unterstellen. Um seine Unabhängigkeit in der Wahrnehmung seiner fachlichen Aufgaben zu gewährleisten, bestimmt das KDG, dass er in der Ausübung seiner Fachkunde weisungsfrei ist. Niemand, auch nicht der Leiter der Stelle, kann vorschreiben, wie er datenschutzrechtliche Fragen bewertet. Dazu kommt eine Auswirkung auf sein Arbeitsverhältnis: Kündigungsschutz wie bei Mitgliedern der MAV.

Auch der Leiter Ihrer Dienststelle – in Kirchenstiftungen der Pfarrer - wird sich in Zukunft mit den Fragen des Datenschutzes wohl oder übel auseinandersetzen müssen. Er sollte zusammen mit Ihnen ein Datenschutzkonzept für seinen Bereich erarbeiten. Näheres können Sie [weiter unten](#) nachlesen.

Wenn sich der Leiter der Dienststelle über das Votum des betrieblichen DSB hinwegsetzt, weil er in letzter Konsequenz die Verantwortung für die Daten verarbeitende Stelle trägt, kann sich der betriebliche Beauftragte für den Datenschutz an den Diözesandatenschutzbeauftragten wenden. Ganz generell ist der betriebliche DSB Auge und Ohr des diözesanen. Der diözesane DSB wird bei Beschwerden über eine Dienststelle immer erst den betrieblichen anhören und ggfs. um Ermittlungen bitten. Der Diözesandatenschutzbeauftragte wird den betrieblichen auch mit allen notwendigen rechtlichen Informationen im Einzelfall versorgen. Er ist für den betrieblichen DSB immer zu sprechen.

##### Verhältnis zu den betroffenen kirchlichen Stellen

Die kirchliche(n) Stelle(n), für die der betriebliche Datenschutzbeauftragte zuständig ist, müssen dem Datenschutzbeauftragten eine Übersicht über die in § 31 KDG genannten Angaben sowie zugriffsberechtigte Personen zur Verfügung stellen.

Er ist bei der Erfüllung seiner Aufgaben von allen Beschäftigten und der Dienststellenleitung zu unterstützen. Nach § 20 Abs. 8 KDG findet im Übrigen § 16 KDG Anwendung; das heißt:

- Bestellung für mehrere Dienststellen zulässig;
- Widerruf nur auf Antrag des Amtsinhabers oder bei schwerwiegenden Verfehlungen.

Zusätzlich gilt für den internen betrieblichen Datenschutzbeauftragten nach § 36 Abs. 5 S. 2

- Bestellung für mindestens vier, höchstens acht Jahre;
- Ende mit der Aufnahme der Amtsgeschäfte durch den Nachfolger
- Mehrmalige erneute Bestellung ist zulässig.
- Dienststellen- oder IT-Leiter sollten nicht benannt werden, § 36 Abs. 7 KDG.

<sup>4</sup> Bitte Datum der zugrunde liegenden Kirchenverwaltungsbeschlüsse einfügen.

## D. Vorschläge zum Vorgehen des betrieblichen Datenschutzbeauftragten

### 1. Eigenes Vorgehen planen

Die Tätigkeit als betrieblicher Datenschutzbeauftragter sollte sich schon von den Grundzügen her ganz erheblich von seiner sonstigen Tätigkeit unterscheiden. Es ist viel mehr Eigeninitiative notwendig und angebracht als sonst vielleicht üblich. Der betriebliche Datenschutzbeauftragte ist als Kontrollorgan ein vom bischöflichen Gesetz her notwendiger Bestandteil des Gesamtdatenschutzes der Kirche. Nur wenn er seine Aufgaben ernst nimmt und etwas aus seiner Stellung macht, erfüllt er die in ihn gesetzten Erwartungen und trägt dazu bei, dass die Kirche ihre Selbstständigkeit im Datenschutz wahrt. Er sollte sich also auch vorher überlegen, wann und wieviel er tätig werden kann, ohne dass dies seine sonstigen Aufgaben erheblich beeinträchtigt.

### 2. Absprache mit der Dienststellenleitung

Der betriebliche Datenschutzbeauftragte ist direkt dem Dienststellenleiter unterstellt, soweit diese Aufgaben betroffen sind. Er wird also zunächst den Kontakt zur Dienststellenleitung suchen und mit dem Dienststellenleiter das weitere Vorgehen besprechen. Dies ist besonders deswegen notwendig, weil der zeitliche Einsatz gerade am Anfang der Tätigkeit größer ist als nach der Anlaufphase.

### 3. Kontakt herstellen

Zunächst wird der betriebliche Datenschutzbeauftragte sich per E-Mail an die zugeordneten Dienststellen wenden, sich vorstellen und freundlich darum bitten, Angaben zur Datensicherheit in der Dienststelle zu machen. Er übersendet dazu die Dokumentvorlage „Erweitertes Verzeichnis“ mit dem zugehörigen Erläuterungsblatt (Falls Sie es noch nicht haben, finden Sie es an derselben Stelle wie dieses Dokument). Die Frist zur Ausfüllung des Verzeichnisses sollte nicht länger als einen Monat sein, weil sonst die ganze Bitte ins Vergessen gerät. Dienststellen, die nicht fristgerecht antworten, sollten besser telefonisch gemahnt werden als schriftlich, um eine persönlichere Vorstellung zu ermöglichen. Hat der betriebliche Datenschutzbeauftragte Visitenkarten, kann dies helfen und den Erinnerungseffekt steigern.

Es kommen natürlich zum Erweiterten Verzeichnis Fragen, die Sie beantworten müssen. Aus meiner Tätigkeit heraus sind mir die meisten Fragen geläufig; daher will ich Ihnen mit Kommentaren und Beispielen bzw. Weblinks helfen:

#### Erweitertes Verzeichnis:

**Dienststelle:** Kirchenstiftung XXX (oder Kindergarten YYY, Straße, Ort)

**Leiter:** Pfarrer Müller

**Mit der Dateneingabe befasste und/oder zugriffsberechtigte Personen:**

Hier sind alle zu nennen, die Zugang zu den Daten haben, auch Kleriker und Ehrenamtliche, nicht aber z.B. Reinigungskräfte usw.

Vorname	Familiename	Funktion	Angestellt (a), beamtet (b) oder ehrenamtlich (e)	Verpflichtungserkl.	Eigener PC?
Meier	Sabine	Pfarrsekr.	a	j	Desktop
Müller	Hans	Pfarrer	b	j	Laptop
Schulze	Siegfried	Diakon	b	j	keiner
Huber	Karl	PGR-V	e	j	Fremd-PC
Gruber	Anna	Aushilfs-S.	a	j	Laptop

#### Personenbezogene Daten (nicht Sachdaten) :

Welcher Personen?	Datensätze ca.	zu welchem Zweck?	an wen werden die Daten mitgeteilt?	Regellöschung vorgesehen j/n	Elektronisch (e) / Papier (p)	mit welcher Anwendung?
Gemeindemitglieder	6800	Mitgliederdokumentation	Vorstand, PGR	n	e	Meldewesen verfahren
Ministranten	20	Gottesdiensteinteilung	Pfarrer	j	e	Access
				j	e	

				j	e	
				j	e	
				j	e	

**Datenverarbeitung:**Zahl der PCs Gesamtzahl inkl. etwa genehmigter Privat-PC DSL-Anbindung (schnelles Internet) WLAN (Drahtlosnetzwerk)WLAN-Sicherung:  WPA  WEPLetzter Passwortwechsel: \_\_\_\_\_  keine SicherungEingesetzte Software:  Word  Excel  AccessSonstige Standardanwendungen: allgemein erhältliche Software, z.B. FTP-Programm Filezilla; Browser wie Internet-Explorer müssen nicht genannt werdenSpezialsoftware (Name und Ursprung): Das ist Software, die entweder nur für diese Dienststelle programmiert wurde oder solche, die allgemein für Dienststellen dieser Art Verwendung findet.**Zugangssicherung:**

Räume mit Aktenschranken/EDV-Geräten:

 einzeln verschließbar nur über Haustür gesichert Fenster: Gitter und/oder SicherheitsglasAktenschranke:  verschließbar  offen

Haben zu diesen Räumen weitere als die oben genannten Personen Zutritt?

 Reinigungspersonal innerhalb  außerhalb der allgemeinen Dienststunden;Personalien  erfasst  nicht erfasstSonstige  innerhalb  außerhalb der allgemeinen Dienststunden:**Videüberwachung: Hier geht es um die Einhaltung von § 52 KDG!** vorhanden Anlass nach § 52 Abs.1 KDG geprüft? Hinweis nach § 52 Abs.2 vorhanden Regellöschung eingerichtet § 52 Abs.5Erläuterungen dazu finden Sie auch im Ordner „Videoüberwachung“ der Downloadseite.**Internetauftritt vorhanden? für diese spezielle Dienststelle!**

www-Adresse:

 Verantwortlicher genannt siehe Arbeitshilfe 234 (Internetpräsenz) S. 43/44 Kontaktanschrift angegeben

Wie hat sich der Verantwortliche über Datenschutz im Internet informiert?

Der Verantwortliche sollte sich dem DSB gegenüber dazu erklären, ob er die wesentlichen Normen für den Internetauftritt kennt und woher diese Kenntnis stammt. An dieser Stelle bietet sich ein Hinweis auf die Arbeitshilfe 234 an.

Werten Sie die zurückkommenden Verfahrensverzeichnisse aus und machen Sie sich Notizen darüber, wo Mängel vorhanden sind.

In dem auf die Ernennung folgenden Jahr sollte dann jede der zugehörigen Dienststellen einmal aufgesucht werden, damit ein wirklich persönlicher Kontakt hergestellt wird. Bei dieser Gelegenheit sollte auch mit dem jeweiligen Dienststellenleiter besprochen werden, welche Probleme in seinem Bereich aufgetreten sind und wie sie am besten behoben werden können. Sofern für den Internetauftritt ein anderer zuständig ist als der Dienststellenleiter sollte auch dieser hinzugezogen werden.

- Planen Sie für jeden Monat einige Telefonate mit den Dienststellen in Ihrem Bereich ein, so dass Sie in etwa drei Monaten mit allen gesprochen haben.
- Lassen Sie sich über Änderungen berichten.
- Besuchen Sie jeden Monat eine Dienststelle zu einem etwas intensiveren Gespräch.

Auf Folgendes sollte bei diesem persönlichen Kontakt hingewirkt werden:

- Sensibilisierung der Mitarbeiter
- Weiterbildung aller Mitarbeiter, die mit personenbezogenen Daten umgehen, veranlassen
- Hinwirken auf die Einhaltung des Datenschutzes
- regelmäßige, (unangemeldete) Kontrollen
- schriftliche Niederlegung der Ergebnisse
- Umgang mit den Daten rechtmäßig?
- Datensicherheitsmaßnahmen eingehalten?
- Beachtung der Rechte Betroffener?
- Datenschutzerklärungen der Mitarbeiter abgegeben?

Die bei ihm eingetroffenen Verfahrensverzeichnisse überprüft der betriebliche Datenschutzbeauftragte und speichert sie auf seinem Rechner ab.

### **Kurzinformation für Pfarrämter**

Die Pfarrämter der ED München und Freising haben die folgende Kurzinformation bekommen, die ich natürlich Ihnen nicht vorenthalten will. Fragen Sie bei Ihren Kontakten mit den Pfarrämtern, ob die Kurzinformationen vorhanden und bekannt sind!

## **KURZINFORMATION ÜBER DEN KIRCHLICHEN DATENSCHUTZ FÜR PFARRÄMTER UND SONST. KIRCHLICHE EINRICHTUNGEN**

Für die Kirche gelten weder das Bundesdatenschutzgesetz (BDSG) noch die Landesdatenschutzgesetze. Damit jedoch die Kirche weiterhin ihre Datenschutzangelegenheiten selbst verwalten und z.B. kommunale Meldedaten erhalten kann, hatte sie 1978 in ihren Diözesen gleichlautende Anordnungen über den kirchlichen Datenschutz (KDG) erlassen. Diese wurden (für den Bereich der Erzdiözese München und Freising) zum 01.01.1994 und zum 01.12.2003 und 1.2.2011 novelliert.

Fundstelle:	KDG, Amtsblatt EOM XXXXXXXXX, Durchführungsverordnung zur KDG (DVO), Amtsblatt XXXXXX; im Internet unter <a href="http://www.erzbistum-muenchen.de/datenschutz/">www.erzbistum-muenchen.de/datenschutz/</a>
Schutzzweck:	Das KDG schützt personenbezogene Daten vor Missbrauch bei ihrer Erhebung, Verarbeitung (Datenverarbeitung = Speichern, Übermitteln, Verändern, Sperren und Löschen von Daten) und Nutzung.
Datenübermittlung:	Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an <u>Dritte</u> . Dieses Bekanntgeben kann mündlich oder schriftlich oder durch Gewährung von Einsicht in eine Datei geschehen. Unter <u>Dritten</u> versteht man alle Personen und Stellen, die nicht kraft ihrer Tätigkeit im Pfarramt mit der Führung der Personendateien befasst sind. Vorgesetzte sind in der Regel nicht als Dritte anzusehen. Übermitteln ist auch die Bekanntgabe von Daten an einen unbestimmt großen Personenkreis (z.B. Veröffentlichung im Pfarrbrief oder im Internet, Aushang oder Verkündigung im Gottesdienst).  Listenmäßige Auszüge aus Dateien (z.B. Alphanalisten, Wählerverzeichnisse usw.) unterliegen gleichfalls den Datenschutzbestimmungen. Geregelt ist die Datenübermittlung in den §§ 11 und 12 des KDG (bitte nachlesen).

### **Pflichten des Pfarrers bzw. des Leiters einer Einrichtung**

Datengeheimnis:	Sämtliche Personen, die Zugang zu personenbezogenen Daten haben, müssen über das Datengeheimnis belehrt und schriftlich verpflichtet werden. Die Verpflichtungserklärungen sind am Ende des Textes des KDG als Anhang abgedruckt. Vor der Unterzeichnung empfiehlt es sich, dem neuen Mitarbeiter einen Ausdruck des KDG zu überlassen und ihn auf die wichtigsten Punkte hinzuweisen (Schweigepflicht, Informationsmöglichkeiten, Bedeutung des eigenen Datenschutzes für die Kirche. <u>In der Pfarrei trägt der Pfarrer die Verantwortung für die Belehrung, Verpflichtung und korrekte Geschäftsführung. Er verwahrt die Verpflichtungsurkunden seiner Mitarbeiter. Als Leiter der Dienststelle „Pfarrbüro“ ist er auch gehalten, die Erstellung eines Datenschutzkonzeptes zu überwachen.</u>
Benennung eines betr. Datenschutzbeauftragten:	ist nunmehr für jede Kirchenstiftung notwendig, auch wenn die Zahl der mit der Dateneingabe befassten Personen nicht übersteigt. Um Komplikationen bei Personalschwankungen zu vermeiden, wird dringend empfohlen, dass die Kirchenstiftungen eines Dekanats immer einen gemeinsamen betrieblichen Datenschutzbeauftragten bestellen.
Datensicherung:	Dateien (vor allem automatische oder herkömmliche Pfarrkarteien) sind so zu verwahren, dass sie von Unbefugten nicht eingesehen werden können. Personalakten sind immer in verschlossenen Schränken aufzubewahren. Überholte Dateien, die nicht archiviert werden müssen, sind gewissenhaft zu vernichten (Reißwolf, Verbrennen oder Löschen).
Rechte des Betroffenen:	Er hat grundsätzlich ein Recht auf Auskunft über die zu seiner Person gespeicherten Daten (§ 17 KDG). Er hat ein Recht auf Berichtigung falscher sowie Löschung oder Sperrung unrechtmäßig gespeicherter Daten (§ 18f. KDG).

### Einige praktische Hinweise zur Anwendung des KDG

- Namen und Adressen von Erstkommunikanten und Firmlingen dürfen nur dann an Sparkassen und sonstige Firmen gegeben werden, wenn das schriftliche Einverständnis von den Erziehungsberechtigten der jeweiligen Kinder vorliegt.
- Die Nennung von Name (nicht Anschrift) und Datum im Zusammenhang mit kirchlichen Amtshandlungen (Taufe, Erstkommunion, Firmung, Trauung, Sterbefall) im Pfarrblatt oder durch Aushang in der Kirche ist grundsätzlich zulässig, soweit ein entgegenstehender Wille der Betroffenen nicht erkennbar ist und dies nicht zu einer Gefährdung berechtigter Interessen des Betroffenen führen kann. Die Anschrift Verstorbener oder der von einem Todesfall betroffenen Angehörigen darf ohne Zustimmung der Betroffenen nicht in Anzeigen oder in Aushängen enthalten sein (Einbruchgefahr! vgl. Amtsblatt 1991, S. 162).
- Veröffentlichungen von Jubiläen (Geburtstagen, Ehejubiläen) sind datenschutzrechtlich nicht ohne weiteres unbedenklich. Hier liegt keine kirchliche Amtshandlung vor. Im Pfarrblatt oder in sonst geeigneter Weise muss einmal jährlich auf die Widerspruchsmöglichkeit eines Betroffenen hingewiesen werden.
- Die Weitergabe von Namen und Adressen an Gemeindeglieder, die beispielsweise neu zugezogene oder ältere Gemeindeglieder besuchen oder Haussammlungen für kirchliche (einschließlich karitative) Zwecke durchführen, ist zulässig. Der Helfer darf jedoch nur diejenigen Namen und Anschriften erhalten, die er für seine Aufgabe benötigt (evtl. Auskunftssperre beachten). Außerdem muss er auf das Datengeheimnis schriftlich verpflichtet werden.
- Die Weitergabe von Namen und Adressen an das jeweilige Bistumsblatt zur Werbung neuer Abonnenten ist zulässig. Dies gilt jedoch nicht für andere Zeitungen und Zeitschriften, auch wenn sie der Kirche nahestehen.
- Die Weitergabe von Daten an Privatpersonen, Firmen oder nichtkirchliche Vereine (z.B. für Werbungen, Einladungen usw.) ist ohne vorherige Zustimmung der jeweiligen Betroffenen nicht zulässig. Ausnahmen bilden Notfälle, wie das Ermitteln von Angehörigen bei Verkehrsunfällen durch Polizei oder Krankenhaus.
- Wenn Daten an Dritte weitergegeben werden, so darf dies **keinesfalls so geschehen, dass die empfangende Person oder Stelle selbst Einsicht nimmt in die Kartei, oder dass die Kartei komplett an die empfangende Person oder Stelle weitergegeben wird**. Die für die jeweilige Aktion benötigten Angaben sind am Aufbewahrungsort der Kartei vom Pfarrer oder von einer auf den Datenschutz schriftlich verpflichteten, von ihm benannten Person abzuschreiben oder zu diktieren. Es muss stets gewährleistet sein, dass die zur Verfügung gestellten Daten nur in dem zur Erfüllung der jeweiligen Aktion oder Aufgabe erforderlichen Umfang verwendet werden. Nach Abschluss der Aktion müssen die Daten ausnahmslos an das Pfarramt zurückgegeben werden.
- Gesperrte Daten dürfen ohne Einwilligung des Betroffenen in der Regel nicht übermittelt werden.

Besonders vertrauliche Daten: Im Interesse des Schutzes besonders empfindlicher Daten werden Aufzeichnungen über rein seelsorgerische Fakten (besondere familiäre Verhältnisse, Werturteile), zweckmäßig vom Seelsorger selbst, getrennt von den Karteien, geführt, sie dienen dann ausschließlich dem Seelsorger.

Kirchenaustritte: Die Veröffentlichung von Namen aus der Kirche ausgetretener Pfarrmitglieder ist grundsätzlich nicht zulässig.

Aufgebote sind in der kirchenrechtlich vorgeschriebenen Form durchzuführen.

Bei Haussammlungen muss durch geeignete Maßnahmen dafür Sorge getragen werden, dass die Sammler den Inhalt der Spendenlisten nicht den Angesprochenen zur Kenntnis bringen. Dies kann z.B. durch Abdeckung der früheren Einträge erfolgen.

Bilder von Personen dürfen grundsätzlich nur mit deren Einwilligung, bei Minderjährigen mit der Einwilligung beider Sorgeberechtigter veröffentlicht werden.

**In Zweifelsfällen empfiehlt es sich, beim Datenschutzbeauftragten der bayerischen (Erz) Diözesen Auskunft und Rat einzuholen (Tel.: 089/2137-1796, Bürozeit i. d. R. Dienstag und Mittwoch von 09:00 - 12:00 Uhr).**

#### 4. Übersicht: Die Aufgaben des betrieblichen Datenschutzbeauftragten

Die Aufgaben des Datenschutzbeauftragten sind in § 38 KDG zusammengefasst: Er hat

- auf die Einhaltung des KDG und anderer Vorschriften über den Datenschutz hinwirken,
- die ordnungsgemäße Programmanwendung überwachen,
- die bei der Verarbeitung personenbezogener Daten eingesetzten Beschäftigten mit den Anforderungen des Datenschutzes vertraut machen,
- die öffentlich zugänglichen Angaben des Verzeichnisses nach § 3a KDG in geeigneter Weise auf Antrag jedermann verfügbar machen. Einer besonderen Berechtigung oder Begründung bedarf es für denjenigen, der von diesem Recht Gebrauch machen möchte, nicht.

und

- Er soll mit dem Diözesan- beziehungsweise dem Ordensdatenschutzbeauftragten zusammenarbeiten.
- In Bezug auf seine Arbeit unterliegt er der Verschwiegenheitspflicht wie der Diözesandatenschutzbeauftragte (§ 37 Abs. 4 S.2 in Verbindung mit § 43 Abs. 9 und 10 KDG). Über die Identität des Betroffenen (Beschwerdeführers) oder Umstände, die Rückschlüsse hierüber erlauben, darf er keine Auskünfte geben. Eine Ausnahme gilt nur, wenn die betroffene Person ihn von seiner Verschwiegenheitsverpflichtung befreit.
- Überwachung der Datenverarbeitung
  - Alle Programme, die mit personenbezogenen Daten arbeiten
  - alle Phasen (Planung, Entwicklung, Lizenzierung, Eingabe, etc.)
- Materielle Vereinbarkeit mit dem Datenschutzrecht
- Datensicherheit
- Sicherstellung der eigenen organisatorischen Einbindung

Einen ganz wichtigen Teil des Aufgabenbereichs stellen die

**KONTROLLEN** dar:

##### ❖ ZUTRITTSKONTROLLE

- Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit bzw. auf denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

##### ❖ ZUGANGSKONTROLLE

- Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

##### ❖ ZUGRIFFSKONTROLLE

- Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

##### ❖ WEITERGABEKONTROLLE

- Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist bzw. stattgefunden hat.

##### ❖ EINGABEKONTROLLE

- Nachträglich muss festgestellt werden können, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.

##### ❖ AUFTRAGSKONTROLLE

- Es muss gewährleistet werden, dass personenbezogene Daten nur im Zuge der Auftragsdatenverarbeitung verarbeitet werden.
- ❖ **VERFÜGBARKEITSKONTROLLE**
  - Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
- ❖ **VERARBEITUNGSKONTROLLE**
  - Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Der ganz überwiegende Teil dieser Kontrollen ist von den Dienststellen selbst zu leisten. Sie können als betrieblicher Datenschutzbeauftragter nicht mehr als gelegentlich zu prüfen, ob die Dienststellen ihren Verpflichtungen in dieser Hinsicht nachkommen. Eine Hilfe dazu ist das "Erweiterte Verfahrensverzeichnis". Es erlaubt Ihnen, mit nur wenigen Blicken festzustellen, ob die wichtigsten Kontrollen greifen.

**Delegierbare Aufgaben** sind insbesondere auch

- die Verpflichtung auf das Datengeheimnis: Verpflichtungserklärungen sollten alle abgeben, die Zugang zu Daten haben, auch Kleriker und Ehrenamtliche (verkürzte Erklärung), Jugendliche ab 16 Jahren. Stellt der betriebliche Datenschutzbeauftragte fest, dass Verpflichtungserklärungen fehlen, fordert er sie von dem Betreffenden ein. Weigert sich dieser, so gibt der betriebliche Datenschutzbeauftragte dies dem Dienststellenleiter zur Kenntnis. Nur dieser kann weitere Reaktionen auslösen.
- Berichte
- Erstellung interner Datenschutz-Vorschriften (z. B. Datenschutz-Flyer)
- Berichterstattung an die Dienststellenleitung
- Gespräche
- Vermittlung zwischen Dienststelle und Betroffenen

Auch einen Teil der nötigen **Dokumentationen** können Sie von den Dienststellen machen lassen:

- Standorte (Computer, Server, Telefonanlagen usw. - wo steht was?)
- Berechtigungsvorgaben (wer darf was?)
- sonstige technische und organisatorische Maßnahmen
- Datenstromanalyse (wo gehen die Daten hin?)
- Betriebsvereinbarungen, falls vorhanden.

Das **Verzeichnis der Verarbeitungstätigkeiten** im Sinne des § 31 KDG ersetzt das frühere Verfahrensverzeichnis, enthält aber dieselben Elemente wie dieses. Es bedarf daher keiner großen Änderung im Ablauf. Der betriebliche DSB des Dekanats leitet das vorhandene Formblatt („Erweitertes Verfahrensverzeichnis“) jeder Dienststelle per Email zu und setzt eine kurze Frist (ca. 4 Wo.) zur Ausfüllung. Damit ist er in der Lage, das Verzeichnis nach § 31 bei Bedarf sofort zu produzieren.

#### **Datenschutzkonzept:**

Dieses sollte der betriebliche Datenschutzbeauftragte zusammen mit dem Dienststellenleiter – in Kirchenstiftungen der Pfarrer - entwerfen. Fehlt ein betrieblicher Datenschutzbeauftragter, muss der Pfarrer in eigener Person dafür sorgen. Allerdings ist die Entwicklung eines Datenschutzkonzeptes erheblich einfacher als es klingt: In der Regel genügt die Anpassung eines in der Downloadseite vorhandenen Musters an die tatsächlichen Gegebenheiten.

#### **Datenschutz-Folgeabschätzung**

Vor dem Inkrafttreten des KDG war die Einführung neuer Software in einer Dienststelle stets mit größeren Komplikationen verbunden. Zuständig war der betriebliche Datenschutzbeauftragte; er war in aller Regel aber auch mit dieser Aufgabe überfordert. Gab es dann eine Entscheidung, so bildete diese in aller Regel deswegen keine Arbeitserleichterung, weil die Autorität eines betrieblichen Datenschutzbeauftragten der Kirchenstiftung X Y kaum ausreichte, um andere von der Richtigkeit der Entscheidung zu überzeugen. Das alles hat sich mit Inkrafttreten des KDG geändert:

- geblieben ist die Voraussetzung, dass durch eine neue Verfahren Software ein besonderes Risiko für die Betroffenen entsteht.
- Statt ihn mit der Durchführung der Folgenabschätzung zu belasten wird der betriebliche Datenschutzbeauftragte nur noch vom Verantwortlichen angehört.

## Einzelfragen in alphabetischer Reihenfolge

### Arbeitsverhältnis

#### Einstellung:

Der Arbeitgeber darf fragen nach

- der Religionszugehörigkeit
- dem Familienstand
- kirchlicher Trauung bzw. Taufe der Kinder
- der privaten Anschrift und Telefonnummer

Der Arbeitgeber darf nicht fragen nach

- Schwangerschaft
- Eigenschaft „Raucher“

#### Personalakten:

- Personalakten sollen und dürfen alle Informationen über einen Arbeitnehmer enthalten, die eine *unmittelbare Beziehung* zu der vom Arbeitnehmer ausgeübten Tätigkeit haben und an denen der Arbeitgeber ein *berechtigtes sachliches Interesse* hat.
- *Bestandteil von Personalakten* können insofern Angaben zur Person des Arbeitnehmers, zu seiner beruflichen Entwicklung, zu seinen Leistungen und Fähigkeiten, sowie Zeugnisse, Personalfragebögen, ärztliche Beurteilungen, der Arbeitsvertrag inklusive späterer Änderungen, Beurteilungen, Zeugnisse, Lohn- und Gehaltsänderungen, Arbeitsunfälle, Abmahnungen, Darlehen und Pfändungen sein.
- Einen bestimmten Aufbau muss der Dienstgeber nicht einhalten.
- Auch Protokolle von Mitarbeitergesprächen können Inhalt sein.
- Der Arbeitgeber ist verpflichtet, Personalakten des Arbeitnehmers sorgfältig aufzubewahren.
- Der Kreis der mit den Personalakten der Mitarbeiter befassten Arbeitnehmer ist möglichst eng zu halten.
- Eine Weitergabe der Unterlagen an *Betriebsfremde*, insbesondere an andere Arbeitgeber, ist ohne Einverständnis des Arbeitnehmers unzulässig.
- Der Arbeitgeber hat Vorgänge aus der Personalakte zu entfernen, wenn sie sich wegen Zeitablaufs erledigt haben, der Arbeitnehmer aus dem Betrieb ausgeschieden ist oder eine Betriebsvereinbarung eine Entfernung vorsieht.
- Der Arbeitnehmer hat das Recht, in die über ihn geführten Personalakten Einsicht zu nehmen. Verlangt der Arbeitnehmer eine Einsichtnahme, so ist ihm die *gesamte Personalakte* inklusive aller Sonder- und Nebenakten vorzulegen.
- Eine Kennzeichnung von Unterlagen durch den Arbeitgeber als „*vertraulich*“ hindert die Einsichtnahme nicht.
- Mitteilungen über ergangene **Strafurteile** dürfen nicht zur Personalakte genommen werden, wenn
  - a) das strafbare Verhalten im außerdienstlichen Bereich lag,
  - b) die Verurteilung nicht in das vom Bundeszentralregister auszustellende Führungszeugnis aufzunehmen ist und
  - c) der AN den der Verurteilung zugrunde liegenden Sachverhalt nach § 51 Abs. 2 BZRG nicht zu offenbaren braucht

### Auftragsdatenverarbeitung:

In dem [entsprechender Ordner](#) der Downloadseite sind schon einige Vertragsmuster vorhanden. Mit der Zeit sollten es mehr werden.

Zur Erwähnung der KDG in diesen Verträgen gibt es eine [Entschließung der Konferenz der Diözesandatenschutzbeauftragten](#).

Wenn auf Anordnung des Ordensobers in einem Orden eine Dienststelle für andere Dienststellen Auftragsdatenverarbeitung durchführt, bedarf es keines Vertrags, weil ein „anderes Rechtsinstrument“ nach kirchlichem Recht (§ 29 Abs. 3 S. 1 KDG) vorliegt. Werden dagegen Dienststellen anderer Orden oder der verfassten Kirche eingebunden, muss ein Vertrag über Auftragsdatenverarbeitung geschlossen werden.

### **Bilder und Filme**

Die Thematik wird dort besprochen, wo sie im meisten Staub aufwirbelt, nämlich bei den Arbeitshilfen, die sich zum Thema Kinder- und Jugendarbeit äußern, also dem [Material für Kindertageseinrichtungen](#) und dem entsprechenden [Beschluss der Diözesandatenschutzbeauftragtenkonferenz](#).

### **Daten in der „Cloud“ - gibt es eine sichere Lösung?**

- Weitere Informationen: Ordner „webbasierte Anwendungen“ im Downloadbereich
- Verwenden Sie einen deutschen Anbieter, z.B. T-Online-Mediacenter (25 GB kostenlos) oder 1&1 Smartdrive (bei DSL-Vertrag 100 GB kostenlos). Übersicht: <http://www.computerwoche.de/a/cloud-services-aus-deutschland,2359614>
- Oder: Verschlüsseln Sie die Inhalte, z.B. mit BoxCryptor (<https://www.boxcryptor.com/>) oder TrueCrypt (<http://www.truecrypt.org/>).
- Oder: Verwenden Sie eine NAS (netzwerkverbundene Festplatte) mit eigenem passwortgeschütztem Zugang, z.B. Myfriz von AVM (Fritzbox); Anleitung <http://service.avm.de/support/de/SKB/FRITZ-Box-7390/116:Online-Speicher-in-FRITZ-Box-einrichten>
- Literatur: [http://www.tecchannel.de/server/cloud\\_computing/2040524/acht\\_tipps\\_fuer\\_die\\_sichere\\_cloud/](http://www.tecchannel.de/server/cloud_computing/2040524/acht_tipps_fuer_die_sichere_cloud/)  
<http://www.computerwoche.de/a/sicheres-cloud-computing,2527898>

### **Datenpanne**

oder – wie es in der Fachsprache der KDG heißt – **Datenschutzverletzung**. Man versteht darunter eine Zuwiderhandlung gegen datenschutzrechtliche Vorschriften, die dazu führt, dass schuldhaft (vorsätzlich oder fahrlässig) Datenschutzrechte anderer Personen verletzt wurden und diesen Personen deswegen ein nicht zwingend materieller Schaden droht. Ist in einer Dienststelle so etwas passiert, kommt es auf schnelles Handeln an: Innerhalb von 72 Stunden nach Kenntniserlangung muss nämlich der Verantwortliche der Dienststelle den Vorfall an den Diözesandatenschutzbeauftragten gemeldet haben. Er kann natürlich diese Meldepflicht an den betrieblichen Datenschutzbeauftragten delegieren.

Die Meldung können Sie von meiner Webseite aus abgeben oder [hier](#). Der Diözesandatenschutzbeauftragte prüft Ihre Meldung und überlegt, was man tun kann, um Schaden zu vermeiden oder wenigstens zu verringern. Das Ergebnis meiner Überlegungen erhalten Sie ein paar Tage später.

### **Datenschutzklassen:**

- Neu eingeführt mit des KDG-DVO 2015.
- Der Grundgedanke ist, dass nicht alle Arbeitsplatz-PC gleich stark gesichert werden müssen, sondern dass z.B. der PC des Hausmeisters weniger Sicherung braucht.

- In Kirchenstiftungen ist allerdings wegen der Verwendung von *Meldewesen Plus* bzw. Adebis Kita meine Sondersituation gegeben; Alle Rechner, auf denen diese Programme laufen, sind der Datenschutzklasse 3 zuzuordnen.

### Emailverkehr – Was ist zu beachten?

- Teilnehmer im Diözesennetz untereinander: Insoweit wird von einem *Virtuellen Privaten Netzwerk (VPN)* Gebrauch gemacht. Der Emailverkehr ist sicher.
- Alle Übrigen: Emails können ohne weiteres abgegriffen werden.
- Das ist nur unschädlich, soweit alle Zwischenstationen über öffentliche oder kirchliche Server laufen.
- Genaueres: Skriptum „[Elektronische Kommunikation und externe Datenspeicherung](#)“
- Die neue [KDG-DVO](#) sieht in § 25 vor, dass besondere personenbezogene Daten und Sozialdaten nicht per E-Mail über „unsichere Server“ (alle außer staatlichen und kirchlichen) übertragen werden dürfen.

### Email-Versand: CC oder BC?

- Grundsatz: Bei einer Mehrheit von Emailempfängern gibt es prinzipiell keine Rechtsgrundlage dafür, dass einer oder mehrere von ihnen die Emailanschriften der anderen erfahren.
- Deswegen: Emailversand **im Zweifel**
  - An eigene Adresse
  - CC leer
  - BCC die Empfänger
- Wenn Sie in Outlook Word als E-Mail-Editor verwenden, klicken Sie in einer neuen Nachricht auf den Pfeil rechts neben der Schaltfläche **Optionen**, und klicken Sie dann auf **Bcc**. Wenn Sie den Outlook-E-Mail-Editor verwenden, klicken Sie in einer neuen Nachricht im Menü **An-sicht** auf **"Bcc"-Feld**.

### Heime

#### Heimbewohner - Welche Informationen müssen vorhanden sein?

- Von Seiten des Datenschützers aus gar keine.
- Aus Praxissicht: § 6 Abs.1 f KDG
- Alles, was zur Erfüllung der kirchlichen Aufgabe erforderlich ist, darf gespeichert werden. Die Datenübermittlung unterliegt der Einschränkung nach §§ 9, 10 KDG und SGB

#### In welche Teile ihrer Personalakte haben Bewohner Einblick?

In alle Teile, ausgenommen sind nur die Fälle des

- § 17 Abs. 6b KDG (Löschungsverbot)
- § 17 Abs. 6a KDG iVm § 15 Abs. 4/5
  - Aufwand
  - Gefährdung des kirchlichen Wohls
  - Gefährdung der öffentlichen Sicherheit und Ordnung
  - Geheimhaltungspflicht

### Schulen und Kinderbetreuung

**Private Lehrer-PC** sind zulässig. Näheres finden Sie in den weiterführenden Hinweisen des Bay. StMin für Unterricht im Ordner „Schulen“ der Downloadseite. Bei der elektronischen Datenverarbei-

tung von Lehrern ist das eigentliche Problem darin zu sehen, dass sie keinen häuslichen Dienst-PC haben und ihren privaten eigentlich nutzen müssten wie einen dienstlichen.

**Staatliches Prüfungsrecht bei Akten von Kinderbetreuungsstätten:** Deswegen wird das entsprechende Merkblatt in der Downloadseite verwiesen. Nach Auskunft des Bayerischen Sozialministeriums erstreckt sich die Einsichtnahme der Landratsämter und kreisfreien Städte

- auf die Kindergartenakten Teil A
- und auf den Umstand, dass Teil B angelegt ist, nicht aber auf den Inhalt von Teil B (Beobachtungsbögen).

Die Landratsämter sind gehalten, die Akten in der Betreuungsstätte einzusehen. Aus Gründen der Praktikabilität kann aber vereinbart werden, dass an einem Tag eine zentrale Einsicht durchgeführt wird.

### **Auskunft aus Schüler- oder Kindergartenakten**

Es wird immer wieder gefragt, was Eltern aus den Schülerakten oder den Akten der Kinderbetreuungsstätte erfahren dürfen. Die Antwort ist sehr einfach: **Alles!** Es gibt keinen vernünftigen Grund für Beschränkungen.

### **Social Media**

- Datenschutzbeauftragte mögen sie gar nicht! Man muss sich wirklich einmal klarmachen, dass die sozialen Netzwerke nicht aus Menschenfreundlichkeit betrieben werden. Es kommt vielmehr darauf an, möglichst viel über die Vorlieben eines Nutzers zu erfahren. Wer also bei Facebook seinen „Freunden“ im Vertrauen mitteilt, dass er eine bestimmte Musikgruppe mag, wird in der Folgezeit mit Werbung für entsprechende Lieder überschwemmt. Jeder, der dies nicht mag, sollte sozialen Netzwerken fernbleiben.
- Manchmal aber sind sie nicht zu vermeiden. Dann sollten Sie auf Folgendes dringen:
  - Einstellungen möglichst datenschutzgerecht.
  - Nicht einfach auf Zustimmung klicken, sondern vorher durchlesen!
  - Als Webseitenanbieter keinesfalls den Facebook-Like-Button einbauen, wenn überhaupt, dann nur mit der Heise-Sicherung. Der Facebook-Like-Button überträgt schon dann die Nutzerdaten an Facebook, wenn nur die Webseite aufgerufen wird. Dies kann zu Schadensersatzansprüchen des Nutzers gegen den Webseitenbetreiber führen!
- Literatur:
  - <http://www.pcwelt.de/ratgeber/Facebook-Sicherheitstipps-fuer-2012-4386079.html>
  - <http://www.sophos.com/de-de/security-news-trends/best-practices/facebook.aspx>
- Hessischer Rundfunk:  
[http://www.hr-online.de/website/rubriken/ratgeber/index.jsp?rubrik=55911&key=standard\\_document\\_40606745](http://www.hr-online.de/website/rubriken/ratgeber/index.jsp?rubrik=55911&key=standard_document_40606745)
- Tutorial Gulli-Board:  
<http://www.gulli.com/security/facebook>
- Facebook-Anleiter:  
<http://facebook.anleiter.de/was-sind-die-wichtigsten-facebook-sicherheitstipps>

Das neueste Material der Arbeitsgruppe „Datenschutz und Melderecht“ zu Facebook, Twitter und Google+ mache ich Ihnen immer auf der Downloadseite in einem eigenen Ordner zugänglich.

## Was tun bei Softwareänderungen?

Unterscheiden Sie:

- Standardsoftware (z.B. Office) oder
- Spezialsoftware (z.B. Domea)

Bei Standardsoftware wird nur der Eintrag im internen Verzeichnisse korrigiert, sofern nicht nur eine bloße Versionsänderung vorliegt. Bei Spezialsoftware ist zu prüfen, ob § 3 Abs. 5 KDG eingreift:

**Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheit der Betroffenen aufweisen, unterliegen der Vorabkontrolle, die nach Abs. 6 der Vorschrift grundsätzlich dem Verantwortlichen obliegt. Er muss aber nach Abs. 2 den Rat des betrieblichen Datenschutzbeauftragten einholen.**

Das KDG hat massive Änderungen gegenüber dem früheren Rechtszustand mit sich gebracht. War früher ausschließlich der betriebliche Datenschutzbeauftragte zuständig für die Freigabe eines neuen Verfahrens, so ist nunmehr klargestellt, dass er allein eine beratende Funktion ausübt. Dafür ist in § 35 Abs. 3 Vorsorge dafür getroffen, dass frühzeitig die Datenschutzaufsicht in die Folgeabschätzung einbezogen werden kann. Der Gedanke dahinter ist, dass durch die Freigabe eines Verfahrens seitens der Datenschutzaufsicht mehr an Außenwirkungen erzielt werden kann als durch die Freigabe seitens eines betrieblichen Datenschutzbeauftragten. Die Datenschutzaufsicht kann nämlich das freigegebene Verfahren in eine Liste gemäß § 35 Abs. 5 Satz 2 KDG aufnehmen und damit sicherstellen, dass weitere Freigaben nicht mehr erforderlich sind.

Die Liste mit den bisher freigegebenen Verfahren finden Sie in meinen Berichten über die vergangenen Jahre. In Zukunft – voraussichtlich ab 30.9.2020 – wird eine einheitliche Liste der freigegebenen Verfahren im Downloadbereich zu finden sein.

Angestrebt wird, sämtliche im kirchlichen Bereich vorhandenen Verfahren zentral zu erfassen und zu nennen. Darüber hinaus wird es Abgleichungen mit den Datenschutzbeauftragten der EKD und den staatlichen Datenschutzbeauftragten geben.

## Videüberwachung

Sog. Haustürvideoanlagen, die ohne Speicherung lediglich ein Bild des vor der Tür Stehenden übermitteln, fallen nicht unter § 52 KDG, ebenso wenig Videoatrapen.

Zu den Voraussetzungen der Videoüberwachung gibt es in der Downloadseite eine Zusammenstellung.

## Telefon- und Videokonferenzen

S. Downloadbereich – „[Webbasierte Anwendungen](#)“

## Webseiten:

**Verantwortlich:** Derjenige, der im Impressum als Verantwortlicher genannt ist; falls niemand genannt ist: Derjenige, der die Internetveröffentlichung tatsächlich veranlasst hat.

### **Insbesondere: Die eigene Homepage der Ministranten**

- Voraussetzung: Volljähriger Verantwortlicher
- Der Verantwortliche ist aufzuklären:
  - Veröffentlichung der Ministrantenliste = Übermittlung personenbezogener Daten an Dritte; Zustimmung aller Beteiligten erforderlich
  - Vorgaben des § 5 TMG zu beachten (☞ Arbeitshilfe Internetpräsenz)
  - Maßgaben der §§ 22ff. KunstUrhG

**Einige Worte zum Schluss:**

Dieses Dokument will ich allen betrieblichen Datenschutzbeauftragten zugänglich machen. Ich habe mich bemüht, die wichtigsten Fragestellungen, die ich bisher erhielt, einzuarbeiten. Was künftig aufnehmenswert erscheint, möchte ich - wie hier schon geschehen - in den Stichworten als Anhang behandeln, um die Übersichtlichkeit nicht zu gefährden.

Alles, was hier über Ihre Pflichten gesagt wurde, ist eine Maximalforderung, die Sie nicht von heute auf morgen erfüllen können. Weder Ihre Vorgesetzten noch ich erwarten das von Ihnen. Sie müssen aber in diese Aufgaben ebenso hineinwachsen wie in Ihre sonstigen Tätigkeitsfelder. Zunächst erwarten alle von Ihnen nur den guten Willen und den Vorsatz, das Beste zu geben.

Ich wünsche Ihnen viel Erfolg und Freude in Ihrer Tätigkeit!

Jupp Joachimski