Der Diözesandatenschutzbeauftragte

des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Arbeitshilfe
AH 520

Datenschutz

in der kirchlichen Erwachsenenbildung

im Erzbistum Hamburg,
den Bistümern Hildesheim und Osnabrück
und dem Bischöflich Münsterschen Offizialat in Vechta i.O.

Stand: 03/2018

Herausgegeben vom

Diözesandatenschutzbeauftragten
des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

Unser Lieben Frauen Kirchhof 20
28195 Bremen

Tel.: 0421 / 16 30 19 25
Mobil: 0151 / 41 97 57 58
Mail: info@datenschutz-katholisch-nord.de

Diese Arbeitshilfe können Sie auch auf unserer Internetseite abrufen unter:
https://www.datenschutz-kirche.de/

Inhaltsverzeichnis

Der Schutz des Rechts auf informationelle Selbstbestimmung ist selbstverständlich auch im Bereich der Erwachsenenbildung zu gewährleisten. Dabei gilt für Einrichtungen in Trägerschaft der katholischen Kirche das „Gesetz über den kirchlichen Datenschutz – KDG. Die bisher geltende Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO) bleibt bis zu einer Neuregelung, längstens bis zum 30.06.2019, in Kraft. Die nachfolgenden Ausführungen sollen auf die wesentlichen Aspekte hierbei hinweisen und zum Nachdenken über die eigene Arbeit anregen. Für weitere Fragen steht der Diözesandatenschutzbeauftragte jederzeit zur Verfügung:

I. Datenverarbeitung

Im Gegensatz zur bisher geltenden Anordnung über den kirchlichen Datenschutz (KDO) kennt das KDG nunmehr nur noch die „Verarbeitung“ von Daten als zentralen Begriff, unter dem die bisherigen Begriffe wie erheben, übermitteln und speichern in § 4 Nr. 3 KDG zusammengefasst werden. Eine gesonderte Definition wie noch in der KDO üblich erfolgt nicht mehr. Die Verarbeitung meint somit jegliche Art von Vorgang im Zusammenhang mit Daten wie

- das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Zu beachten ist, dass diese Auflistung der Vorgänge im KDG nicht abschließend ist, sodass auch hier nicht benannte Vorgänge von der Datenverarbeitung umfasst sind.

„Betroffene Person“ im Sinne des KDG ist jede identifizierte oder identifizierbare natürliche Person.

Zur Durchführung von Kursen, Seminaren, Tagungen, etc. werden Daten der angemeldeten Teilnehmer benötigt.

Zum Schutz des Persönlichkeitsrechts der betroffenen Person ist nach § 6 Abs. 1 KDG eine solche Datenverarbeitung aber nur dann zulässig, wenn

- eine Rechtsvorschrift sie erlaubt oder anordnet,

- die betroffene Person eingewilligt hat oder
- die Datenverarbeitung erforderlich ist.

Im Einzelnen ergibt sich aus § 6 Abs. 1 lit. c) – g) KDG, wann eine Datenverarbeitung erforderlich ist.

1. Datenerhebung

Die Erforderlichkeit der Datenerhebung, d.h. das Beschaffen der Daten, im Bereich der Erwachsenenbildung kann sich bereits aus der Erfüllung der vertraglichen Verpflichtungen ergeben, § 6 Abs. 1 lit. c) KDG. Für die Erhebung von personenbezogenen Daten als Unterfall der Datenverarbeitung gelten dennoch folgende bestimmte Regeln:

- Es dürfen nur die Daten erhoben werden, deren Kenntnis zur Aufgabenerfüllung notwendig sind – § 7 Abs. 1 lit. c) KDG. Hierzu gehören:
  - Name und Anschrift zur Identifikation des Teilnehmers
  - Kontoverbindungen, soweit sie für Zahlungsvorgänge benötigt werden.
  - Daten über die Voraussetzungen zur Kursteilnahme.
  - Daten über den Arbeitgeber, falls dieser die Kosten der Kursteilnahme trägt.
- Weitere Daten dürfen nur mit Einwilligung der betroffenen Person erhoben werden. Dabei ist auf die Freiwilligkeit besonders hinzuweisen. Die Erklärung hat in der Regel schriftlich zu erfolgen – § 8 Abs. 2 KDG
- Die Daten sind der betroffenen Person selbst zu erheben – § 9 Abs. 1 Satz 1 KDG. Dies geschieht in der Regel durch Anmeldeformulare, die von der betroffenen Person selbst auszufüllen und zu unterschreiben sind. Werden die Daten auf einer Website im Internet erhoben, sind auch die Anforderungen des Telemediengesetzes zu erfüllen. Siehe AH 701 „Das neue Telemediengesetz“.
- Die Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden – § 7 Abs. 1 lit. b) KDG.
- Die betroffene Person hat jederzeit Anspruch auf eine Auskunft, ob personenbezogene Daten verarbeitet worden sind. Sofern dies der Fall ist, hat die betroffene Person einen Anspruch auf Auskunft über die personenbezogenen Daten und auf weitere, in § 17 Abs. 1 KDG aufgelistete, Informationen. Die Erteilung der Auskunft ist für die betroffene Person unentgeltlich.
- Die Rechtmäßigkeit der Datenerhebung ist unabhängig vom Ort ihrer späteren Speicherung. Für Daten in Akten, Listen, etc. gelten die gleichen Grundsätze, wie für

EDV-mäßig erfasste Daten. § 1 KDG will das Persönlichkeitsrecht der betroffenen Person umfassend schützen.

Datenerhebung im Internet

Wer die Anmeldung zu Kursen durch Bereithalten eines entsprechenden Formulars auf seiner Website im Internet ermöglicht, hat zusätzlich zu den oben genannten Grundsätzen auch die Vorschriften des Telemediengesetzes zu beachten. Erforderlich ist in jedem Fall

- ein Impressum nach § 5 TMG und
- eine Datenschutzerklärung (Privacy Policy) nach § 13 TMG.

Dabei ist sicherzustellen, dass der Teilnehmer die Datenschutzerklärung gelesen und akzeptiert hat, bevor er auf das elektronische Anmeldeformular weitergeleitet wird. Genaue Hinweise und Muster zur Gestaltung von Impressum und Datenschutzerklärung finden Sie in der Broschüre „Das neue Telemediengesetz (TMG) - Pflichten für kirchliche Internetanbieter bei der Gestaltung von Webseiten“ auf der Homepage „Datenschutz in der katholischen Kirche“.

Besonders wichtig ist der Zahlungsvorgang. Sollen im Anmeldeformular Angaben zur Kontoverbindung oder Kreditkarte gemacht werden, so muss hierzu auf eine sichere Seite (https://....) mit Secure Socket Layer (SSL) weitergeleitet werden.

2. Offenlegung von Daten

Die Rechtmäßigkeit der Offenlegung von personenbezogenen Daten, also die Übermittlung, Verbreitung oder andere Form der Bereitstellung, an andere Stellen orientiert sich wie die Datenerhebung daran, ob eine Rechtsvorschrift sie erlaubt oder anordnet, die betroffene Person eingewilligt hat oder die Datenverarbeitung erforderlich ist, § 6 Abs. 1 KDG. Andere Stellen können sowohl kirchliche und öffentliche Stellen nach § 9 KDG als auch nicht kirchliche und nicht öffentliche Stellen nach § 10 KDG sein.

- Die Offenlegung von Daten an andere kirchliche oder öffentliche Stellen, die ebenfalls der KDO unterliegen (§ 3 KDG), ist nach § 9 Abs. 1 KDG zulässig, wenn,
  - sie zur Erfüllung der in der Zuständigkeit der offenlegenden oder der empfangenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und
  - die Voraussetzungen des § 6 KDG vorliegen.

- Die Offenlegung personenbezogener Daten auf Ersuchen der empfangenden kirchlichen Stelle ist darüber hinaus nur zulässig, wenn
  - dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Person und der Aufgaben oder Geschäftszwecke der beteiligten kirchlichen Stellen angemessen ist, § 9 Abs. 2 KDG
- Für die Rechtmäßigkeit einer Offenlegung an kirchliche oder öffentliche Stellen trägt die offenlegende kirchliche Stelle die Verantwortung, es sei denn, dass die Offenlegung auf Ersuchen der empfangenden kirchlichen Stelle erfolgt. In diesem Fall ist nur zu prüfen, ob das Ersuchen im Rahmen der Aufgaben der empfangenden kirchlichen Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Offenlegung besteht – § 9 Abs. 3 KDG.
- Die Offenlegung von Daten an die Arbeitsagenturen ist durch Gesetz geregelt. Rechtsgrundlage ist hier z.B. § 83 Abs. 2 SGB III (Weiterbildungskosten)
- Die Offenlegung personenbezogener Daten gegenüber nicht kirchlichen und nicht öffentlichen Stellen ist ebenfalls möglich, wenn
  - sie zur Erfüllung der in der Zuständigkeit der offenlegenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 6 zulassen würden, oder
  - der Empfänger ein berechtigtes Interesse an der Kenntnis der offenzulegenden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Offenlegung hat, es sei denn, dass Grund zu der Annahme besteht, dass durch die Offenlegung die Wahrnehmung des Auftrags der Kirche gefährdet würde.
  - Die Verantwortung für die Zulässigkeit einer Offenlegung an kirchliche und nicht öffentliche Stellen trägt nach § 10 Abs. 2 KDG immer die übermittelnde Stelle.

Auf die Art und Weise der Offenlegung kommt es nicht an. Umfasst ist somit jede Art der Offenlegung, sei es mündlich, schriftlich per E-Mail oder Brief oder im Internet auf der Webseite.

Einzelfälle:

Die Weitergabe von Daten zu Werbezwecken oder an die Presse liegt nicht im Aufgabenbereich der Bildungseinrichtungen. Ein berechtigtes, also rechtlich schützenswertes Interesse des Empfängers an der Kenntnis dieser Daten besteht ebenfalls nicht. Eine Übermittlung kann daher nur mit ausdrücklicher und schriftlicher Zustimmung der betroffenen Person erfolgen.

Öffentliche Stellen, Arbeitgeber, etc. haben ihre Daten ebenfalls direkt bei den Teilnehmern zu erheben. Die Bildungseinrichtungen haben insoweit keine Auskünfte zu erteilen. Dabei ist besondere Wachsamkeit angezeigt. Fälle, in denen Arbeitgeber nur nachgefragt haben, weil der Teilnehmer zur gleichen Zeit am Arbeitsplatz krank gemeldet war, machen deutlich, dass hier die Rechte der betroffenen Person massiv beeinträchtigt werden können. Anderes kann allerdings dann gelten, wenn die Teilnahme auf Veranlassung dieser Stelle erfolgt und von dieser auch finanziert wird.

Die Veröffentlichung personenbezogener Daten der Referenten im Internet ist vorher mit diesen abzusprechen. In vielen Fällen macht es Sinn, den Referenten kurz mit seiner derzeitigen Position und beruflichen Qualifikationen vorzustellen. Diese Daten sind aber über Suchmaschinen wie Google weltweit verfügbar. Deshalb bedarf ihre Veröffentlichung der Zustimmung der betroffenen Person.

3. Datenspeicherung

Datenspeicherung meint das Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke der weiteren Verarbeitung. Mit Datenträgern sind nicht nur elektronische Speichermedien gemeint, sondern auch Akten und Karteikarten. Hierfür gilt:

- Es dürfen nur solche Daten gespeichert werden, deren dauerhafte Aufbewahrung zur Aufgabenerfüllung notwendig ist, § 7 Abs. 1 lit. c) KDG.
- Die gespeicherten Daten dürfen nur für die Zwecke verarbeitet werden, für die sie erhoben worden sind, § 7 Abs. 1 lit. b) KDG. Eine dem Zweck entsprechende Verarbeitung liegt auch dann vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Revision, der Durchführung von Organisationsuntersuchungen für den Verantwortlichen, im kirchlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken dient, § 6 Abs. 3 KDG.

Besondere Kategorien personenbezogener Daten, § 4 Ziffer 2 KDG

Hierzu gehören Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Sie sind in besondere Weise geschützt. Der Grundsatz lautet auch hier, dass eine Verarbeitung besonderer Kategorien personenbezogener Daten untersagt ist.

Neben einer ausdrücklichen Einwilligung der betroffenen Person über die Verarbeitung vorgenannter besonderer Kategorien personenbezogener Daten ist ein Verarbeitung nach § 11 Abs. 2 KDG u.a. dann erlaubt, wenn

- die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der kirchlichen Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist;
- die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist.

II. Technische und organisatorische Maßnahmen

Gemäß § 26 KDG hat der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. Hierdurch soll die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden.

Jeder Verantwortliche hat ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, zu führen. Die Angaben, welche in diesem Verzeichnis aufzuführen sind, sind im § 31 Abs. 1 KDG aufgelistet. Hierzu gehören

- der Name und die Kontaktdaten des Verantwortlichen
- die Zwecke der Verarbeitung

- eine Beschreibung der Kategorien betroffene Personen und der Kategorien personenbezogener Daten
- gegebenenfalls die Verwendung von Profiling;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt werden;
- gegebenenfalls Angaben dazu, ob eine Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation erfolgt;
- möglichst auch vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien;
- möglichst auch eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Ferner müssen folgende Maßnahmen ergriffen werden:

- Verpflichtung der Mitarbeiter auf das Datengeheimnis, § 6 KDG
  - Das Datengeheimnis verpflichtet die Mitarbeiter nicht nur, über das, was ihnen im Rahmen ihrer dienstlichen Tätigkeit bekannt geworden ist, zu schweigen, sondern auch Daten nicht unbefugt zu erheben, zu verarbeiten oder zu nutzen.
- Belehrung der Mitarbeiter über ihre Pflichten
- den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung sicherstellen
- Maßnahmen zum Schutz der Daten vor nicht autorisierter Einsichtnahme. Beachtung des Trennungsgebotes. Jedem Mitarbeiter darf nur der Teil des Gesamtdatenbestandes zur Verfügung gestellt werden, den er zur Erfüllung seiner Aufgaben benötigt;
- Unter Umständen Durchführung einer Datenschutz-Folgenabschätzung, insbesondere bei Verwendung neuer Technologien, gegebenenfalls unter Hinzuziehung der Datenschutzaufsicht;
  - Ein Beratungsgremium der europäischen Kommission in Fragen des Datenschutzes, auch als Art.-29-Datenschutzgruppe bezeichnet, hat zehn Kriterien zur Risikobeurteilung veröffentlicht. Je mehr Kriterien zutreffen, desto wahrscheinlicher ist das Vorliegen eines hohen Risikos. Einer Datenschutzfolgenabschätzung ist allerdings auf jeden Fall erforderlich, wenn biometrische Daten oder die Daten von Kindern verarbeitet werden. Die Kriterien lauten wie folgt:
    - Scoring, Profiling, Evaluation, z. B. Einschätzung der Kreditwürdigkeit, Behavioral Marketing etc.
    - automatisierte Einzelfallentscheidungen

  - systematische Überwachung,
  - Verarbeitung sensibler Daten
  - umfangreiche Datenverarbeitungen (bezogen auf die Anzahl betroffener Personen und Datenkategorien, die Dauer der Verarbeitung, die geographische Ausdehnung)
  - das Zusammenführen oder Abgleichen von Datenbeständen, wenn betroffene Personen nicht damit rechnen können
  - die Verarbeitung von Daten besonders schutzbedürftiger Personen
  - Neuartigkeit von Verarbeitungsvorgängen, Verwendung neuer Technologien (bspw. Fingerabdrucksensoren oder Gesichtserkennung)
  - Übermittlung von personenbezogenen Daten an Empfänger außerhalb der EU
  - Verarbeitungen, die es betroffenen Personen erschweren, ihre Rechte auszuüben oder eine Leistung in Anspruch zu nehmen, z.B. die Beurteilung der Kreditwürdigkeit durch eine Bank vor der Vergabe eines Darlehens
- Gegebenenfalls Bestellung eines betrieblichen Datenschutzbeauftragten, § 36 KDG

Beim Einsatz von EDV zur personenbezogenen Datenverarbeitung sind besondere Sicherheitsmaßnahmen zu beachten. Auch hier können in diesem Rahmen nur Mindestanforderungen aufgeführt werden:

- Strikte Trennung der Verwaltungsrechner von den zur Schulung eingesetzten PCs.
- Rechteverwaltung bei Netzwerkbetrieb oder gemeinschaftlicher Nutzung eines Arbeitsplatzrechners.
- Zugriffsschutz durch Passwortvergabe, möglichst in Verbindung mit Chipkarte oder biometrischen Verfahren.
- Bei mobilen Datenverarbeitungsgeräten (Notebooks, Subnotebooks, Netbooks): Verschlüsselung der Festplatte. Mobile Geräte sind in besonderer Weise gefährdet, wenn es um Verlust oder Diebstahl geht. Daher muss verhindert werden, dass ein unrechtmäßiger Besitzer imstande ist, die Daten auszulesen.
- Regelmäßige, möglichst automatisierte Datensicherung. Einsatz von RAID-Systemen.
- Einsatz von Firewall und Virenschutzprogrammen bei Internetzugang.
- Übermittlung personenbezogener Daten über ungeschützte Internetzugänge oder E-Mail nur bei Verschlüsselung des Inhalts.

- Schriftliche Benutzerordnung für den Umgang mit EDV, Internet und E-Mail. Regelung insbesondere der Privatnutzung von Internet und E-Mail durch Mitarbeiter.

Augmented Reality

Durch den Einsatz von Augmented Realtiy, z. B. durch Smartphone-Apps, ist es bereits heute möglich, dem Nutzer ergänzende Informationen zu seiner unmittelbaren Umwelt auf dem Endgerät anzeigen zu lassen. Großflächig bekannt wurde diese noch in den Kinderschuhen steckende Technologie durch das Spiel „Pokemon Go“. Das Spiel nimmt die unmittelbare Umwelt des Spielers über die Kamera auf, ermittelt den Standort über GPS und projiziert virtuelle Fantasiewesen dazu, welche es dann zu fangen, trainieren oder zu entwickeln gilt.

Im Herbst 2017 startete der US-Internet-Konzern Google die testweise Einführung der Lernsoftware „Google Expeditions“ in Schulen. Die Smartphone-App wird auf dem jeweiligen Endgerät installiert. Die Schüler sind in einer virtuellen Gruppe gemeinsam mit der Lehrkraft verbunden. Die Lehrkraft wird in dieser Gruppe zum „Guide“, die Schüler zu „Entdeckern“. Der „Guide“ führt die virtuelle Gruppe und kann Sehenswürdigkeiten weltweit zeigen. Ungeklärt sind jedoch noch die datenschutzrechtlichen Fragen zu dieser Lernsoftware. So ist im Moment nicht auszuschließen, dass die Schüler angehalten werden, ihr eigenes Smartphone zu nutzen, worüber dann auch personenbezogene Daten ausgetauscht werden könnten. Hierdurch verschwimmt die Grenze zwischen schulischen und privaten Daten. Die Gewährleistung der Datensicherheit durch die Schule kann nicht sichergestellt werden, da die Kontrolle von privaten Smartphones nicht bzw. nicht vollkommen überwacht werden können. Ungeklärt ist zudem die Frage, ob die Schüler, welche kein Smartphone besitzen, faktisch vom Unterricht ausgeschlossen werden.

Die Veröffentlichung personenbezogener Daten im Internet bedarf besonderer Sorgfalt. Ohne Zustimmung des Mitarbeiters ist sie nur gestattet, wenn dies zur Aufgabenerfüllung zwingend erforderlich ist. Etwa dann, wenn eine Tätigkeit ohne Außenkontakt nicht möglich ist. Besondere Regelungen gelten bei der Veröffentlichung von Bildern im Internet. Die gesonderten Informationen hierzu finden Sie auf unserer Homepage.

III. Besondere Verfahren

1. Auftragsdatenverarbeitung, § 29 KDG

„Outsourcing“ erfreut sich, meist durch den Zwang zu Einsparungen, großer Beliebtheit. In § 29 KDG wurde daher eine spezielle Rechtsgrundlage hierfür geschaffen. Dabei sind folgende Punkte zu beachten:

- Auftragsverarbeiter kann eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle sein, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
- Der Auftragsverarbeiter arbeitet ausschließlich auf Weisung des Verantwortlichen, § 30 KDG
- Der Auftragsverarbeiter ist nur dann Verantwortlicher in Bezug auf die Verarbeitung personenbezogener Daten, wenn dieser unter Verstoß gegen das KDG die Zwecke und Mittel der Verarbeitung bestimmt, § 29 Abs. 10 KDG. Im Übrigen bleibt der Verantwortliche auch verantwortlich. Die Verantwortung kann also nicht delegiert werden!
- Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen, in § 29 Abs. 3 KDG näher bestimmten Rechtsinstruments. Der Inhalt des Vertrages bzw. des anderen Rechtsinstruments ist in § 29 Abs. 4 KDG näher beschrieben. Die Auflistung ist jedoch nicht abschließend und soll einen Mindestinhalt gewährleisten.
- Der Auftragsverarbeiter darf die Daten nur innerhalb der Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeiten. Abweichend von hiervon ist die Verarbeitung in Drittstaaten zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission gemäß § 40 Abs. 1 KDG vorliegt oder wenn die Datenschutzaufsicht selbst oder eine andere Datenschutzaufsicht festgestellt hat, dass dort ein angemessenes Datenschutzniveau besteht.
- Die vorgenannten Grundsätze gelten auch dann, wenn es sich „nur“ um Wartungsarbeiten handelt, bei denen der Auftragnehmer die Möglichkeit hat, personenbezogene Daten einzusehen.

2. Videoüberwachung, § 52 KDG

Eine Rechtsgrundlage für die Durchführung von Überwachungsmaßnahmen mit optisch-elektronischen Einrichtungen ist nur für öffentlich zugängliche Räume vorhanden. Öffentlich

sind Räume dann, wenn sie von einer unbestimmten Zahl von Personen betreten werden können. Das Betreten von Seminarräumen ist in der Regel nur den Teilnehmern, Referenten und Servicepersonal gestattet. Sie sind daher nicht öffentlich. Anders sieht es aus, wenn es sich um den Eingangsbereich oder das Grundstück selbst (z.B. Parkplatz) handelt. Auch solch ein öffentlicher Bereich darf nur dann videoüberwacht werden, wenn folgende Voraussetzungen vorliegen:

- Es muss ein Anordnungsgrund vorliegen, der die Einrichtung der Videoüberwachung erforderlich macht. Solche Gründe können sein:
  - Eingangskontrolle. Hier sind sowohl solche Systeme gemeint, die den gesamten Eingangsbereich erfassen, wie auch Kameras, die eine Gesichtskontrolle nach Betätigung der Türglocke ermöglichen.
  - Schutz vor Diebstahl.
  - Schutz vor Vandalismus
  - Wahrnehmung des Hausrechts
  - Mitarbeiterüberwachung. Hierfür ist jedoch in jedem Fall eine Betriebsvereinbarung erforderlich. Eine generelle „Rund-um-die-Uhr-Überwachung“ verletzt jedoch in schwerwiegender Weise das Persönlichkeitsrecht der betroffenen Person und ist daher generell unzulässig.
- Der Anordnungsgrund muss konkret festgelegt werden. Die erhobenen personenbezogenen Daten dürfen nur zum Erreichen des festgelegten Zieles genutzt werden. Auch hier gilt die strenge Zweckbindung.
- Auf den Umstand der Beobachtung muss deutlich erkennbar hingewiesen werden. Es muss zudem erkennbar sein, wer die Videoüberwachung angeordnet hat.
- Beispiel: „Unsere Einrichtung wird videoüberwacht. Der Verwaltungsleiter.“
- Eine verdeckte Videoüberwachung ist nur in schwerwiegenden Fällen zulässig, in denen der Anordnungszweck auf andere nicht Weise erreicht werden kann.
- Bei Aufzeichnung dürfen die Daten nur solange aufbewahrt werden, wie sie zur Erreichung des Zwecks erforderlich sind. In der Regel sind das nicht mehr als 72 Stunden. Innerhalb dieses Zeitraums sollten sich Aufzeichnungsgeräte (Bänder, Festplatten) selbst überschreiben.
- Der Zugang zu den Aufzeichnungsgeräten und die Möglichkeit ihrer Auswertung und Verwendung müssen personell klar geregelt sein.
- Die Videoüberwachung ist im Verzeichnis von Verarbeitungstätigkeiten nach § 31 KDG aufzuführen.

Wann ist eine Videoüberwachung sinnvoll?

- Eine Verhinderung von Straftaten wie Diebstahl und Sachbeschädigung ist in der Regel nur bei dauerhafter Beobachtung und kurzfristiger Reaktionsmöglichkeit zu erreichen.
- Die Aufzeichnung der Videoaufnahmen kann im günstigsten Fall Hinweise zur Ermittlung des Täters liefern. Dies ist aber abhängig von den Rahmenbedingungen, wie der Qualität der Kameras, ihrer Anbringung, des jeweils optisch erfassten Bereichs sowie ausreichender Beleuchtung.
- Meist sind weitere „flankierende“ Maßnahmen, wie ordnungsgemäße Raum- und Objektsicherung, Einsatz einer Warnanlage, Bewegungsmelder, etc. erforderlich. Hier sollten zuvor auch polizeiliche Beratungsstellen in Anspruch genommen werden.
- Untersuchungen zeigen, dass die Einrichtung einer Videoüberwachung üblicherweise spontan begangene Taten nicht verhindern kann. Solche Täter lassen sich im Moment von ihrem Impuls leiten und denken nicht darüber nach, ob sie sich im Erfassungsbereich einer Videokamera befinden. Beispiel: Der jüngste Fall in der Münchner U-Bahn, in der ein Helfer von alkoholisierten Jugendlichen zu Tode geprügelt wurde.
- Untersuchungen zeigen aber auch, dass geplante Straftaten in bestimmten Fällen signifikant zurückgehen. Täter scheuen das Risiko. Der Tatort wird meist vorher „ausbaldowert“. Dabei wird die Videoüberwachung als deutliche Risikoerhöhung wahrgenommen.
- Das Anbringen einer Kamera-Attrappe ist aus datenschutzrechtlicher Sicht als unkritisch einzustufen, da keine Datenverarbeitung i.S.d. § 4 Nr. 3 KDG vorliegt. Das Anbringen eine Kamera-Attrappe kann jedoch in besonderen Fällen zu einem Anspruch auf Entfernung der Kamera-Attrappe und Unterlassung der Anbringung führen. Unter gewissen Umständen kann eine Kamera-Attrappe sogar zu einem Schadensersatzanspruch der betroffenen Person führen.

IV. Rechte der betroffenen Person

Mit jeder Änderung der Datenschutzvorschriften wurden die Rechte der betroffenen Person gestärkt. Nach dem derzeitigen Rechtsstand sind folgende Rechte zu gewähren:

1. § 17 KDG – Anspruch auf Auskunft

Die betroffene Person hat zunächst das Recht, von dem Verantwortlichen eine Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat die betroffene Person ein Recht auf Auskunft über die personenbezogenen Daten sowie auf folgende Informationen:

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei der Datenschutzaufsicht;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß § 24 Abs. 1 und 4 KDG und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Unter bestimmten Umständen hat die betroffene Person jedoch kein Recht aus Auskunft. Dies gilt auch dann für den Fall, wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, § 17 Abs. 6 KDG.

2. § 18 KDG – Anspruch auf Berichtigung

Die betroffene Person hat ebenfalls einen Anspruch darauf, dass unrichtige oder unvollständige personenbezogene Daten zu berichtigen sind. Eine Ausnahme für unrichtige personenbezogene Daten gilt für den Fall, dass diese zu Archivzwecken im kirchlichen Interesse verarbeitet werden. Der betroffenen Person ist dann eine Gelegenheit zur Gegendarstellung einzuräumen, welche dann zu den Unterlagen zu nehmen ist.

3. § 19 KDG – Recht auf Löschung

Auch haben die betroffenen Personen das Recht aus Löschung nach § 19 KDG. Das Recht auf Löschung besteht dann, wenn folgende Gründe zutreffen:

- die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig;
- die betroffene Person widerruft ihre Einwilligung und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung;
- die betroffene Person legt nach § 23 KDG Widerspruch ein (s.u.);
- die personenbezogenen Daten wurden unrechtmäßig verarbeitet;
- die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem staatlichen oder dem kirchlichen Recht erforderlich, dem der Verantwortliche unterliegt.

Wenn der Verantwortliche die personenbezogenen Daten öffentlich bekannt gemacht hat und nach § 19 Abs. 1 KDG zur Löschung verpflichtet ist, so ist dieser nach § 19 Abs. 2 KDG ebenfalls dazu verpflichtet, andere Verantwortliche mit angemessenen Maßnahmen hierüber zu informieren.

Das Recht auf Löschung kann von der betroffenen Person in einem formlosen Schreiben geltend gemacht werden. Wenn eine Löschung der personenbezogenen Daten nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, tritt an die Stelle des Rechts auf Löschung das Recht auf Einschränkung der Verarbeitung (s.u.). In dem Fall, dass die personenbezogenen Daten unrechtmäßig verarbeitet wurden, sind diese ohne Rücksicht auf den Aufwand zu löschen.

4. § 20 KDG – Recht auf Einschränkung der Verarbeitung

Die Einschränkung der Verarbeitung meint nach § 4 Nr. 4 KDG „die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken." Eine Einschränkung der Verarbeitung kommt nach § 20 Abs. 1 KDG in Betracht wenn

- die Richtigkeit bestritten wird;
- die Verarbeitung unrechtmäßig ist die betroffene Person die Löschung verlangt;
- die betroffene Person die Daten zur Geltendmachung von Rechtsansprüchen benötigt und der Verantwortliche diese nicht mehr benötigt oder
- die betroffene Person einen Widerspruch gegen die Verarbeitung eingelegt hat und über diesen noch nicht entschieden ist.

Nicht ausreichend ist es, den entsprechenden Datensatz mit einem Einschränkungsvermerk zu versehen.

Die Einschränkung der Verarbeitung wird vielmehr dadurch umgesetzt, dass personenbezogene Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für die Nutzer gesperrt oder dass veröffentliche Daten vorübergehend von einer Webseite entfernt werden. Die Weiterverarbeitung oder Änderung der Daten ist durch technische Maßnahmen effektiv zu unterbinden.

5. § 22 KDG – Recht auf Datenübertragbarkeit

Das Recht auf Datenübertragbarkeit soll gewährleisten, dass Daten von einem Verantwortlichen zu einem anderen Verantwortlichen „mitgenommen" werden können. Dieses Recht gilt jedoch nur dann, wenn die Verarbeitung der personenbezogenen Daten entweder auf einer Einwilligung oder auf einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt. Die Daten müssen in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden, wobei jedoch ein bestimmtes Format nicht vorgegeben wird.

Die betroffene Person kann ebenfalls verlangen, dass Daten unmittelbar von einem Verantwortlichen zu einem anderen Verantwortlichen übertragen werden, § 22 Abs. 2 KDG. Die unmittelbare Übertragung von personenbezogenen Daten zwischen den Verantwortlichen kann jedoch mit der Begründung abgelehnt werden, dass die technisch nicht machbar sei, z.B. aufgrund verschiedenartiger Software.

6. § 23 KDG – Widerspruchsrecht

Grundsätzlich kann die betroffene Person auch Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten einzulegen. Ein Widerspruch kann in den Fällen erfolgen, wenn

- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im kirchlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (§ 6 Abs. 1 lit. f) KDG) oder
- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um einen Minderjährigen handelt. Dies gilt nicht für die von öffentlich-rechtlich organisierten kirchlichen Stellen in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung (§ 6 Abs. 1 lit. g) KDG).

Werden personenbezogene Daten verarbeitet, um Direktwerbung oder Fundraising zu betreiben, hat die betroffene Person nach § 23 Abs. 2 KDG jederzeit das Recht, Widerspruch einzulegen.

7. § 25 KDG – Unabdingbare Rechte der betroffenen Person

Die Rechte der betroffenen Person auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

8. § 48 KDG – Beschwerde bei der Datenschutzaufsicht

Jede betroffene Person hat jederzeit das Recht, sich mit einer Beschwerde an die zuständige Datenschutzaufsicht, den Diözesandatenschutzbeauftragten, zu wenden.

Hinweis in eigener Sache
Der Inhalt dieser Arbeitshilfe wurde mit größter Sorgfalt erstellt und erhebt keinen Anspruch auf Vollständigkeit.

Diese Arbeitshilfe dient in erster Linie dazu, Ihnen bei der täglichen Arbeit die Einbindung der datenschutzrechtlichen Bestimmungen zu erleichtern. Sie berücksichtigt die Vorschriften des KDG durch den Diözesandatenschutzbeauftragten zum derzeitigen Zeitpunkt.

Sollten sich Unklarheiten oder offensichtliche Fehler aus dieser Arbeitshilfe ergeben, so bitten wir um einen entsprechenden Hinweis unmittelbar an den Diözesandatenschutzbeauftragten. Die Kontaktinformationen können Sie dieser Arbeitshilfe entnehmen.