



TRI<sup>er</sup>QM<sup>elementar</sup>

## Arbeitshilfe Datenschutz in katholischen Tageseinrichtungen für Kinder



Abteilung  
Kindertageseinrichtungen im  
Caritasverband für die  
Diözese Trier e.V.



- 3 Einleitung
- 4 Grundsätzliches, Datenschutz als Qualitätsmerkmal, Um wessen Rechte geht es
- 5 Um welche Daten geht es, Was ist zu beachten, Grundsatz der Erforderlichkeit, Grundsatz der Zweckbindung, Grundsatz der Nichtdiskriminierung, Grundsatz der Transparenz
- 6 Bildungs- und Lerndokumentation, Kooperation mit der Grundschule
- 7 Zusammenarbeit mit anderen Stellen, Förderstellen und Gesundheitsdiensten, Jugendamt, Landesjugendamt
- 8 Fotos und andere Bildaufnahmen vom Kind, Wer hat ein Recht auf Auskunft und Akteneinsicht
- 9 Wie müssen personenbezogene Daten aufbewahrt werden, Wer kontrolliert den Datenschutz
  
- 10 Anordnung über den kirchlichen Datenschutz (KDO)
- 19 Muster als Kopiervorlagen

## Inhalt



## Einleitung

Die pädagogischen Fachkräfte in Kindertagesstätten werden immer häufiger mit Fragen des Datenschutzes konfrontiert. Eltern wollen wissen, ob die Träger der Einrichtung ihre Daten und die Daten ihrer Kinder in einem Computer speichern, wer darauf zugreifen darf, an wen sie weiter gegeben werden und wann sie gelöscht werden. Haben sie ein Recht, Ergebnisse von Beobachtung und Dokumentation einzusehen und dürfen Informationen über das Kind an Lehrkräfte der Grundschule weitergegeben werden. Verunsicherung herrscht, ob sich Erziehungskräfte private Notizen über den Entwicklungsfortschritt und das Verhalten einzelner Kinder machen dürfen und ob die Eltern einen Anspruch auf Einsicht in diese Unterlagen haben. Hinzu kommen Fragen des Umgangs mit Fotos und Videoaufnahmen und die Einhaltung von Datenschutzvorschriften bei der Sicherstellung des Kinder- und Jugendschutzes in der Einrichtung. Datenschutz in Kindertagesstätten ist ein Thema, zu dem es offenbar mehr Fragen als Antworten gibt.

Um hier eine Orientierung zu erhalten ist es notwendig, sich zunächst vor Augen zu führen, dass es beim Datenschutz im Kern um die Respektierung der Persönlichkeitsrechte des Kindes und seiner Eltern geht. Anknüpfungspunkt sind dabei Überlegungen, die das Bundesverfassungsgericht 1983 in seinem Volkszählungsurteil entwickelt hat. Das Gericht statuierte erstmalig ein Grundrecht auf informationelle Selbstbestimmung. Nach Auffassung des Gerichtes wird unter den Bedingungen der modernen Datenverarbeitung der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten im Grundgesetz von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 GG (Menschenwürde) umfasst. Das Grundrecht gewährleiste insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Diese Grundüberlegungen aus dem Volkszählungsurteil gelten im Prinzip unabhängig von der Verarbeitungsform, also auch für Daten und Informationen in Akten sowie aus Sammlungen von Texten und Bildern.

Während bei der Volkszählung die Gefahr einer missbräuchlichen Nutzung von Daten durch staatliche Stellen gesehen wurde, muss inzwischen davon ausgegangen werden, dass die Persönlichkeitsrechte in zunehmendem Maße auch durch Private bedroht werden. Wirtschaftliche Interessen haben den gläsernen Kunden geschaffen, soziale Netzwerke erlauben Einblicke in privateste Bereiche. Die Entwicklung von Speichermedien von nahezu unbegrenzter Kapazität und von Netzen mit unvorstellbaren Übertragungsraten erlauben es, die Datenverarbeitung in mehr oder weniger rechtsfreie Räume zu verlegen und der Kontrolle nationaler Behörden und Stellen zunehmend zu entziehen. Umso mehr gilt daher die Maxime, dass mit einem bewussten und respektvollen Umgang mit Persönlichkeitsrechten schon im Kindergarten angefangen werden muss.

### Verfasser

→ Hartmut Gerstein  
Ass. jur., Lehrbeauftragter, FH Koblenz

## Grundsätzliches

Für Kindertagesstätten in kirchlicher Trägerschaft gilt das Kirchenprivileg.

Religionsgemeinschaften und kirchliche Organisationen können nach Art. 140 Grundgesetz in Verbindung mit Art. 137 Abs. 3 Weimarer Reichsverfassung ihre inneren Angelegenheiten selbst regeln und sind insoweit nicht dem staatlichen Recht unterworfen. Dies gilt auch für privatrechtlich verfasste Organisationen, die in ihrem Wesen dem Kernbereich der Kirche zuzuordnen sind, z.B. für die Caritas und die von ihnen betriebenen Einrichtungen sowie für sonstige kirchliche Kindergärten.

Die katholische Kirche hat sich mit der Anordnung über den kirchlichen Datenschutz (KDO) (Den vollständigen Text finden Sie ab Seite 10) eigene Datenschutzvorschriften gegeben, die in ihren Grundzügen den staatlichen Vorschriften entsprechen. Die KDO in der seit 2003 geltenden Fassung orientiert sich an dem Bundesdatenschutzgesetz<sup>1</sup>. Sie ist von den deutschen Bischöfen gleichlautend in den jeweiligen Bistümern beschlossen und in Kraft gesetzt worden.

Beim Datenschutz geht es primär um die Beachtung der Persönlichkeitsrechte des Kindes. Diese werden von den Eltern treuhänderisch wahrgenommen. Eltern können stellvertretend für ihr Kind gegen Datenschutzverstöße vorgehen aber auch unter Beachtung des Kindeswohls für das Kind Einverständniserklärungen abgeben und Entscheidungen über die Verwendung personenbezogener Daten treffen. Neben dem Kind sind aber auch die Eltern selbst „Betroffene“ im Sinne des Datenschutzes .

Neben den Regelungen der KDO gelten für Kindertageseinrichtungen in katholischer Trägerschaft die Vorschriften des Sozialdatenschutzes in § 35 Abs. 1, 3 und 4 SGB I und §§ 67-80 §§ 83 und 84 SGB VIII<sup>2</sup>. Dies betrifft alle Daten, die im Rahmen der Arbeit in der Kindertagesstätte über Kinder und deren Familien bekannt werden, zum Beispiel Familienverhältnisse, Vermögensverhältnisse, Gesundheitszustand etc. Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden<sup>3</sup>. Zu den besonderen Dienstpflichten gehört das Gebot der Verschwiegenheit in allen dienstlichen Angelegenheiten. Die Verschwiegenheitspflicht des Kita-Personals besteht nicht nur während des Dienstverhältnisses, sondern auch nach dessen Beendigung<sup>4</sup>. Die Mitarbeiterinnen und Mitarbeiter werden in ihren Arbeitsverträgen zur Verschwiegenheit und zur Einhaltung des Datenschutzes verpflichtet (s. Verpflichtungserklärung auf Seite 18). Auf Verstöße kann der Arbeitgeber dann mit arbeitsrechtlichen Maßnahmen (Abmahnung, bei wiederholten Verstößen verhaltensbedingte Kündigung) reagieren.

## Datenschutz als Qualitätsmerkmal

Datenschutz in Kindertageseinrichtungen ist nicht einfach nur ein Rechtsproblem. Vielmehr geht es um den Respekt vor der Persönlichkeit des Kindes und damit um ein pädagogisches Grundverständnis der Fachkräfte bei der Unterstützung von Entwicklungs- und Lernprozessen in einem hochsensiblen Lebensabschnitt. Im Mittelpunkt steht das Kind als Subjekt. Hieraus folgt die Orientierung am Kindeswohl, der Schutz der Persönlichkeitsrechte, die Berücksichtigung des Kindeswillens und die Beteiligung des Kindes an Entscheidungen sowie die Einbeziehung der Eltern in diesen Prozess. Der Schutz personenbezogener Daten ist dabei Ausdruck einer pädagogischen Grundhaltung, die sich in Konzeptionen und Leitbildern wiederfindet und als wichtiges Qualitätsmerkmal für gute Arbeit in Kindertagesstätten verstanden werden muss. Dies zu verwirklichen ist Aufgabe und Herausforderung für jede gute Tageseinrichtung für Kinder.

## Um wessen Rechte geht es?

Beim Datenschutz in Kindertagesstätten geht es also primär um die Beachtung der Persönlichkeitsrechte des Kindes. Diese werden von den Eltern treuhänderisch wahrgenommen. Eltern können stellvertretend für ihr Kind gegen Datenschutzverstöße vorgehen aber auch unter Beachtung des Kindeswohls für das Kind Einverständniserklärungen abgeben und Entscheidungen über die Verwendung personenbezogener Daten treffen. Neben dem Kind sind aber auch die Eltern selbst „Betroffene“ im Sinne des Datenschutzes. Dies ist beispielsweise der Fall, wenn vom Träger der Kindertagesstätte zur Berechnung der Elternbeiträge Einkommensdaten erhoben werden oder zum Bedarfsnachweis für einen Krippenplatz oder einer Ganztagsbetreuung Arbeitgeberbescheinigungen verlangt werden.

<sup>1</sup>In der Fassung der Bekanntmachung vom 14.01.2003, BGBl. I S. 66 <sup>2</sup>Vgl. Anordnung des Diözesanbischofs über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft, Kirchliches Amtsblatt Bistum Trier vom 1. Juni 2004, Nr. 150-151. <sup>3</sup>Vgl. § 35 Abs. 1 S. 2 SGB I <sup>4</sup>Vgl. § 1 Abs.1 Richtlinien für Arbeitsverträge in den Einrichtungen des Deutschen Caritasverbandes (AVR), Allgemeiner Teil

Aber es geht auch um die Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter und die Fürsorgepflicht des Trägers als Arbeitgeber. Die Regelungen der KDO gelten in gleichem Maße auch für die Beschäftigten in der Kindertagesstätte.

## Um welche Daten geht es?

Beim Datenschutz geht es um den Schutz personenbezogener Daten. Dies sind Angaben über persönliche und sachliche Verhältnisse eines Menschen (Vgl. § 2 Abs. 1 KDO, abgedruckt auf Seite 11). Der Persönlichkeitsschutz umfasst daneben auch Tondokumente sowie Fotos und Filmaufnahmen. Hierbei sind neben datenschutzrechtlichen Vorschriften auch Verwertungsrechte (Urheberrechte und das „Recht am eigenen Bild“) zu beachten. Beim Schutz personenbezogener Daten kommt es nicht primär darauf an, ob es sich um besonders brisante Angaben handelt. Aus dem Zusammenhang gerissen können auch scheinbar harmlose Daten ein Persönlichkeitsbild verfälschen. Personenbezogene Daten sind nicht nur Angaben, die den Namen der Person enthalten. Es genügt, wenn ohne größere Schwierigkeiten der Bezug auf eine bestimmte Person (Vater von Max) oder bestimmte Personen (Eltern von Laura) hergestellt werden kann. Man spricht dann von personenbeziehbaren Daten. Datenschutzrechtlich irrelevant sind lediglich anonymisierte Daten, z.B. in Statistiken (Vgl. § 2 Abs. 6 KDO) oder pseudonymisierte Daten (Vgl. § 2 Abs. 7 KDO), d.h. Personendaten, bei denen die Namen geändert wurden. Diese unterliegen nicht dem Datenschutz, sondern allenfalls dem Schutz von Betriebs- und Geschäftsgeheimnissen.

## Was ist zu beachten?

Die Erhebung, Speicherung und Nutzung personenbezogener Daten ist in der Kindertagesstättenarbeit nicht grundsätzlich verboten und in vielen Fällen sogar unabdingbar (Führen von Anwesenheitslisten, Informationen über Allergien und Unverträglichkeiten, Liste der Abholberechtigten, Telefonverzeichnisse etc.). Wichtig ist, dass in der Einrichtung im Sinne des Persönlichkeitsschutzes eine Kultur des Umgangs mit personenbezogenen Daten herrscht, die einen Missbrauch ausschließt. Dazu gehört die Beachtung folgender Grundsätze:

### Grundsatz der Erforderlichkeit:

Personenbezogenen Daten dürfen nur erhoben werden, wenn sie zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich sind (Vgl. § 10 Abs. 1 KDO). Das Prinzip der Erforderlichkeit ist auch bei der Verarbeitung, Nutzung und Weitergabe zu beachten. In der Kindertagesstätte ist die Erhebung und Nutzung personenbezogener Daten der Kinder nur zulässig, wenn sie für die Erziehung, Bildung und Betreuung des Kindes oder die dafür notwendigen Verwaltungsvorgänge, erforderlich ist (Vgl. § 9 Abs. 1 KDO). Bei der Gestaltung und Auswahl von Datenverarbeitungssystemen ist das Prinzip der Datenvermeidung und Datensparsamkeit zu beachten (Vgl. § 2a KDO).

### Grundsatz der Zweckbindung:

Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden. Daher ist es immer notwendig, bei der Datenerhebung den Zweck festzulegen.

Bei der Übermittlung der Daten an Dritte ist sicherzustellen, dass die Daten nur zu dem im Aufgabenbereich des Datenempfängers liegenden Zweck verarbeitet oder genutzt werden, zu dessen Erfüllung sie übermittelt wurden (Vgl. §§ 10 Abs. 1, 11 Abs. 3, 12 Abs. 1 Nr. 1 KDO).

### Grundsatz der Nichtdiskriminierung:

Personenbezogene Daten mit besonders sensiblem Inhalt, die für die Betroffenen zu einer Diskriminierung führen können, dürfen nicht oder nur unter sehr beschränkten Voraussetzungen erhoben, gespeichert oder an Dritte weiter gegeben werden (Vgl. § 3 Abs. 4 in Verbindung mit § 2 Abs. 10 KDO). Hierzu können z.B. Krankheitsdaten sowie Leistungs- und Verhaltensdaten gehören. Bei sensiblen Daten muss außerdem besonders auf die Sicherheit und den Schutz vor unbefugtem Zugriff geachtet werden.

### Grundsatz der Transparenz:

Wo immer dies möglich ist, muss ein Bürger die Chance haben, über die Verarbeitung seiner Daten mitzubestimmen. Insofern ist es nicht nur Ausdruck effizienter Erziehungs- und Bildungspartnerschaft, sondern auch datenschutzrechtlich geboten, dass Eltern umfassend darüber informiert werden, welche personenbezogenen Daten zu welchem Zweck im Rahmen der pädagogischen Arbeit oder im Rahmen der Verwaltung erhoben und gegebenenfalls auch an Dritte weitergegeben werden. Betroffene haben ein Recht auf Auskunft (Vgl. § 13 KDO). Wenn Daten ohne ihre Kenntnis erhoben und/oder weitergegeben werden, sind die Betroffenen in der Regel zu benachrichtigen (Vgl. § 13a KDO).

## Bildungs- und Lerndokumentation

Personenbezogene Daten von Kindern dürfen in Kindertageseinrichtungen nur erhoben werden, wenn und soweit sie für die Aufgabenerfüllung erforderlich sind. Sie sind daher zu löschen, wenn der Zweck entfallen ist (Vgl. § 14 Abs. 2 Nr. 2 KDO). Zum Beispiel geht es bei der Beobachtung und Dokumentation vorrangig um den Entwicklungsstand, das Verhalten und die Engagiertheit des Kindes in der Kindertagesstätte. Dabei wird oft mit strukturierten Erfassungs- und Einschätzbögen gearbeitet, mit denen die Beobachtungen fachlich geleitet werden und die dazu beitragen sollen, dass es bei der Auswertung zu vergleichbaren und gesicherten Ergebnissen kommt. Hinzu kommen als ergänzende Instrumente standardisierte Erhebungsbögen. Die von den Erzieherinnen dokumentierten Beobachtungen sind immer nur Momentaufnahmen. Sie werden gemacht, um den derzeitigen individuellen Förderungsbedarf zu erkennen oder Entwicklungsprobleme festzustellen, um Eltern z.B. zum Übergang in die Grundschule gezielte Rückmeldungen über ihr Kind zu geben, oder auch um Hinweise darüber zu gewinnen, welche Angebote in der Kita weiterentwickelt werden sollten. Wichtig ist, dass dieser Kontext erhalten bleibt und die gewonnenen Informationen über das Kind nicht in späteren Zusammenhängen genutzt werden und wie ein Etikett an ihm „kleben“ bleiben. Beobachtungsbögen dürfen daher in der Regel nur so lange aufbewahrt und verwendet werden, wie das Kind in der Einrichtung betreut wird. Eine Weitergabe an Dritte ist ohne Einverständnis der Personensorgeberechtigten nicht zulässig. Beobachtungsbögen sind zu vernichten oder den Eltern auszuhändigen, wenn das Kind die Einrichtung verlässt.

Die Beobachtung und Dokumentation der individuellen Bildungs- und Lernentwicklung des Kindes gehört inzwischen zu den fachlichen Standards der Arbeit in Kindertagesstätten. In den Bildungsplänen und -empfehlungen der Länder werden Bildungs- und Lerndokumentationen ausdrücklich gefordert. In Rheinland-Pfalz gibt es hierfür sogar einen gesetzlichen Auftrag. Gemäß § 2 Abs.1 Satz 2 Kindertagesstättengesetz ist für die Förderung der Gesamtentwicklung des Kindes „die Beobachtung und Dokumentation der kindlichen Entwicklungsprozesse unter Beachtung der trägerspezifischen Konzeption und des Datenschutzes erforderlich“. Im Saarland finden wir in der Ausführungs-VO SKBBG in § 3 „... eine systematische Dokumentation dieser Beobachtungen ist unerlässlich.“ Beobachtung und Dokumentation sind daher vom Erziehungs- und Bildungsauftrag des Kindergartens gedeckt und grundsätzlich zulässig. Es bedarf hierfür keiner ausdrücklichen Genehmigung durch die Eltern.

Dennoch sollten die Personensorgeberechtigten aus Gründen der Transparenz darüber informiert werden, dass Bildungs- und Lerndokumentationen über das Kind angelegt und fortgeschrieben werden. Ein geeigneter Ort hierfür ist der Betreuungsvertrag. Die Eltern können mit ihrer Unterschrift ihr ausdrückliches Einverständnis zum Führen von Bildungsdokumentationen geben, wobei gleichzeitig die Verpflichtung der Kindertagesstätte festgelegt werden kann, dass dabei die Regeln des Datenschutzes eingehalten werden und die Eltern die Möglichkeit erhalten, die Dokumentationsmappen für ihre Kinder einzusehen (Akten-einsichtsrecht). Wenn für die Beobachtung standardisierte Erhebungsbögen verwendet werden, wäre es sinnvoll, die Elternvertretung in die Entscheidungsfindung mit einzubeziehen und alle Eltern über den Inhalt der Bögen zu informieren.

## Kooperation mit der Grundschule

Bei der Übermittlung von Daten sind auch die Datenschutzvorschriften der Stellen zu berücksichtigen, die personenbezogene Daten empfangen und verwenden wollen, etwa die für die Schulen geltenden Regelungen<sup>5</sup>. Die Verantwortung liegt allerdings bei der empfangenden Stelle. Bei der notwendigen Zusammenarbeit zwischen Kindertagesstätte und der Grundschule ist ein Austausch von Informationen und Erfahrungen dann datenschutzrechtlich unproblematisch, wenn dabei die Namen der Kinder nicht genannt werden.

Wenn Unterlagen und personenbezogenen Informationen ohne Zustimmung des Betroffenen an Dritte weitergegeben werden, liegt darin ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung. Dies gilt auch für den Informationsaustausch mit der Grundschule. Zwar ist die Zusammenarbeit zwischen Kindergarten und Grundschule heute wichtiger denn je und im Kindertagesstättengesetz für Rheinland-Pfalz wird sie sogar ausdrücklich gefordert. Im Saarland finden wir dazu Aussagen in der Ausführungs-VO SKBBG in § 5. Das Zusammenarbeitsgebot bezieht sich jedoch nur auf die Information und Abstimmung der jeweiligen Bildungskonzepte und somit nicht auf den Informationsaustausch über einzelne Kinder. Die datenschutzrechtlich gebotenen Schranken des Informationsaustauschs sind also nicht aufgehoben. Unproblematisch sind aber zunächst die Fälle, bei denen die Eltern über Art und Inhalt

der an die Schule weitergegebenen Informationen informiert wurden und diese vorab ihr Einverständnis bekundet haben. Wenn aber seitens der Grundschule vom Kindergarten ohne Wissen und Zustimmung der Eltern Einblick in die Unterlagen oder Informationen über die Leistung und das Verhalten von Kindern fordern, wäre die naheliegende Frage, aus welchem Grund dies ohne das Wissen der Eltern von statten gehen soll. Hierfür gibt es kaum triftige Gründe. Daher ist in solchen Fällen grundsätzlich das Einverständnis der Eltern einzuholen. Dies sollte zur Sicherheit schriftlich geschehen. Unter dem Gesichtspunkt der Erziehungspartnerschaft wäre es allerdings noch besser, wenn die Eltern an den Gesprächen beteiligt werden oder Unterlagen den Eltern ausgehändigt werden, damit diese frei entscheiden können, ob, und wenn ja, welche Informationen sie an die Grundschule weitergeben wollen. Wenn seitens der Grundschule vom Kindergarten Einblick in die Unterlagen oder Informationen über die Leistung und das Verhalten von Kindern anfordern muss das Einverständnis der Eltern vorliegen. Auch bei einer Entbindung von der Schweigepflicht besteht kein Auskunftsanspruch der Schule. Die Kindertagesstätte kann nach eigener Einschätzung darüber entscheiden, welche Informationen sie an die Schule weitergibt.

## Zusammenarbeit mit anderen Stellen

Im Grundsatz gilt, dass die Weitergabe von Sozialdaten an Dritte nur mit wirksamer Einwilligung zulässig ist.

### Förderstellen und Gesundheitsdiensten

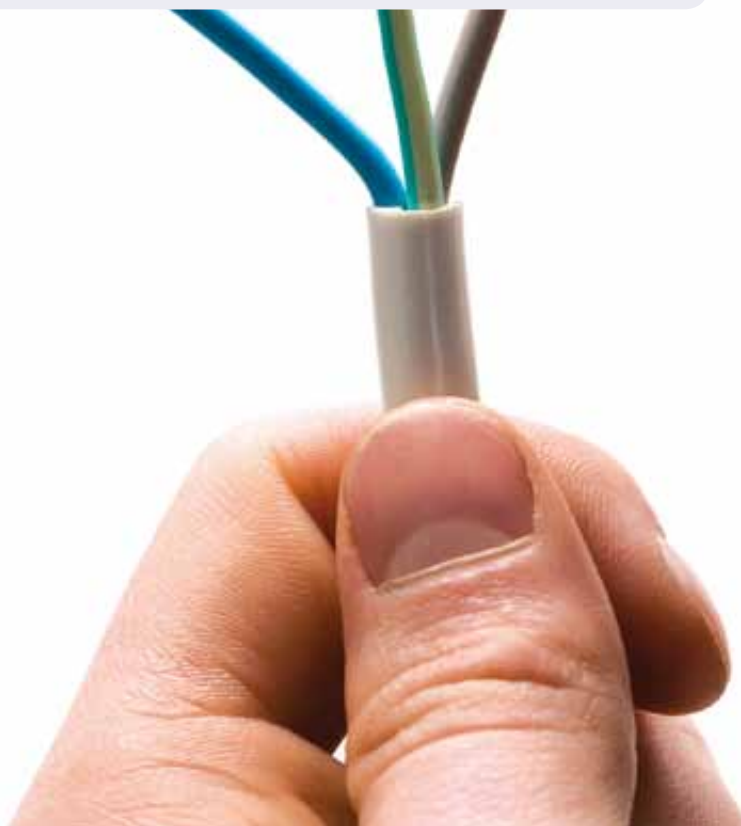
Wenn ein Kind neben dem Besuch der Kindertagesstätte bei einer Förderstelle oder einem Gesundheitsdienst in Behandlung ist, ist in der Regel eine fachliche Abstimmung der Förderung notwendig. Die Einwilligung der Personensorgeberechtigten sollte die behandelnde Stelle und den Zweck der Zusammenarbeit genau benennen (Ein Muster für eine Einwilligungserklärung findet sich auf Seite 22).

### Jugendamt

Bei gewichtigen Anhaltspunkten für eine Gefährdung des Wohls eines Kindes in seinem familiären Umfeld ist eine Übermittlung personenbezogener Daten an das Jugendamt auch ohne Einverständnis der Personensorgeberechtigten zulässig, wenn die Gefährdung nicht anders abgewendet werden kann. Eine entsprechende Verpflichtung des Trägers ist in die Vereinbarung zwischen Jugendamt und Träger zum Schutzauftrag bei Kindeswohlgefährdungen gem. § 8a Abs. 4 Satz 2 SGB VIII aufzunehmen.

### Landesjugendamt

Bei gewichtigen Anhaltspunkten für eine Kindeswohlgefährdung im Verantwortungsbereich der Kindertagesstätte, zum Beispiel Kindesmisshandlung oder entwürdigende Erziehungsmaßnahmen (§ 1631 Abs. 2 BGB), ergibt sich die Zulässigkeit der Weitergabe von Sozialdaten des Kindes an die Erlaubnisbehörde aus der Verpflichtung des Trägers nach § 47 Nr. 2 SGB VIII.



## Fotos und andere Bildaufnahmen vom Kind

Digitalkameras und Camcorder gehören inzwischen zum alltäglichen Inventar von Kindertagesstätten. Auf Elternabenden werden Fotos und Videoaufnahmen zur Vorstellung von Projekten und zur Dokumentation von Aufführungen gezeigt, Bildungs- und Lerndokumentationen zeigen Schnappschüsse von typischen Situationen, Fotoalben erinnern als Abschiedsgeschenk an die Kindergartenzeit.

Der Umgang mit Fotografien und Videoaufnahmen von Kindern in Kindertageseinrichtungen verweist auf einen weiteren Bereich des Persönlichkeitsschutzes, das **Recht am eigenen Bild**. Besondere Gefährdungen bestehen heute insbesondere, weil Bilder inzwischen mühelos manipuliert werden können. Veröffentlichungen im Internet machen die Kinderbilder weltweit für jeden zugänglich.

Nach § 22 Kunsturhebergesetz (KunstUrhG) dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Bei Kindern ist die Einwilligung der Personensorgeberechtigten notwendig. Ausnahmen bilden nach § 23 Abs. 1 KunstUrhG Abbildungen von Personen der Zeitgeschichte, Bilder, bei denen Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen, Bilder von Teilnehmern an öffentlichen Versammlungen und Aufzügen oder Bilder, die einem höheren Interesse der Kunst dienen. Aber auch in diesen Fällen wäre eine Verbreitung und Schaustellung ohne Einwilligung unzulässig, wenn dadurch das berechnete Interesse des Abgebildeten verletzt wird (§ 23 Abs. 2 KunstUrhG).

Bei einer Veröffentlichung von Kinderfotos, insbesondere im Internet, kann generell davon ausgegangen werden, dass eine Einwilligung notwendig ist. **Diese sollte nicht allgemein, sondern stets konkret auf ein bestimmtes Bild bezogen sein und den Hinweis enthalten, dass die Einwilligung jederzeit widerrufen werden kann.**

Für Aufnahmen, die nur für den internen Gebrauch und die Vorführung in der Einrichtung verwendet werden, genügt ein generelles Einverständnis in dem Betreuungsvertrag. Dabei ist selbstverständlich die **Zweckbindung** zu beachten.

Ebenfalls im Betreuungsvertrag sollte die Verpflichtung der Eltern festgelegt werden, dass Bilder und Videoaufnahmen, auf denen (auch) andere als die eigenen Kinder abgebildet werden, nicht im Internet veröffentlicht oder an andere weitergegeben werden dürfen.

Die unbefugte Verbreitung und Verwertung von Bildern kann gem. § 33 Abs. 1 KunstUrhG mit einer Geldstrafe oder mit Freiheitsstrafe bis zu einem Jahr geahndet werden. Das heimliche Fotografieren von Kindern in einem besonders geschützten Raum (Toilette, Dusche) kann – auch ohne die Weitergabe an Dritte – gem. § 201a Strafgesetzbuch (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen) strafbar sein.

## Wer hat ein Recht auf Auskunft und Akteneinsicht?

Zum Datenschutz gehört auch, dass die Betroffenen die Möglichkeit haben müssen, festzustellen, welche Informationen über sie in der Einrichtung vorhanden sind. Die Datenschutzvorschriften enthalten Rechte des Betroffenen auf Auskunft über die gespeicherten Daten und über deren Herkunft (Vgl. § 13 KDO). Das Auskunftsrecht bezieht sich also auf Daten, die auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung und Nutzung erfasst werden (Vgl. § 2 Abs. 4 Nr. 1 KDO). Ein Recht auf Einsicht in die Akten lässt sich daraus jedoch nicht herleiten. Dennoch sollten Kindertagesstätten den Eltern – etwa durch Vereinbarungen im Betreuungsvertrag oder mit einer Selbstverpflichtung - ein Recht auf „Akteneinsicht“, z.B. in die Bildungs- und Lerndokumentationen geben. Denn wenn, wie oben ausgeführt, diese Form der Informationssammlung zum notwendigen „Handwerkzeug“ der Kindertagesstätten gehört, muss den Eltern auf der anderen Seite die Möglichkeit eröffnet werden, sich selbst ein Bild zu machen. Die Erziehungspartner-schaft zwischen dem pädagogischen Team der Kindertagesstätte und den Eltern gebietet es, dass hier ein Austausch stattfindet. Eltern sollten daher nicht nur auf Nachfrage Einsichtsmöglichkeiten erhalten, sondern aktiv auf diese Möglichkeit hingewiesen werden. Allerdings muss auch berücksichtigt werden, dass Bildungs- und Lerndokumentationen Momentaufnahmen sind, die Position des Beobachters mit einbeziehen und dass es oft für die Interpretation wichtig ist, den Kontext der Entstehung zu kennen. Es kann sich daher als sinnvoll erweisen, wenn bei der Akteneinsicht die Möglichkeit für Rückfragen an das pädagogische Personal besteht.

Manche Beobachtungsbögen enthalten auch von den Eltern auszufüllende Teile, in denen beispielsweise abgefragt wird, mit welcher Stimmung das Kind vom Kindergarten nach Hause kommt, wie es zuhause spielt oder ob es sich in der Kindergruppe akzeptiert fühlt. Beobachtung und Dokumentation wird so als gemeinsame Aufgabe von Kindergarten und Eltern angesehen. Fragen der Akteneinsicht stellen sich dann nicht.



Das Transparenzgebot hat dort seine Grenzen, wenn es um persönliche Aufzeichnungen und Notizen geht, die sich die pädagogischen Fachkräfte im Rahmen ihrer Tätigkeit machen. Ein Recht auf Einsicht in persönliche Notizen besteht nicht. Den Eltern sollten jedoch die Möglichkeit gegeben werden, im Rahmen eines Elterngesprächs über die aus den Beobachtungen gewonnenen Erkenntnisse der pädagogischen Fachkraft informiert zu werden.

## Wie müssen personenbezogene Daten aufbewahrt werden?

Um möglichem Missbrauch vorzubeugen sind Unterlagen mit personenbezogenen Daten in Kindertageseinrichtungen grundsätzlich so aufzubewahren, dass sie vor unbefugtem Zugriff geschützt sind. Personalunterlagen und Einkommensnachweise der Eltern, standardisierte Beobachtungsbögen und ähnlich sensible Daten gehören in abschließbare Schränke, die in separaten Räumen (Büro- oder Personalraum) stehen sollten. Portfolios müssen nicht unbedingt in abschließbaren Stahlschränken aufbewahrt werden. Je nach Inhalt kann es aber notwendig sein, sie vor neugierigen Kindern oder Besuchern zu schützen. In anderen Fällen gehört es zum Konzept der Portfolios, dass die Kinder jederzeit nachschauen und zeigen können, was sie geschaffen und geschafft haben. Hier wird der Datenschutz durch Vereinbarungen mit den Kindern gewährleistet, dass jeder im Prinzip nur in seine eigenen Unterlagen schauen kann und die „Einsicht in fremde Akten“ nur mit Zustimmung des Betroffenen erfolgen darf. Die Kultur des Umgangs mit fremden Daten wird so spielerisch zum Lernziel im Kindergarten.

Für Personalakten gilt in der Regel eine Aufbewahrungsfrist von 5 Jahren nach deren Abschluss. Die Frist bezieht sich auf die Personalakte (Grundakte und Teilakten); sie gilt nicht für Nebenakten sowie für automatisiert gespeicherte Personalaktendaten, die in der Grundakte oder in den Teilakten vorhanden sind. Diese sind zu vernichten, sobald sie nicht mehr benötigt werden, keinesfalls dürfen sie über die genannte Frist von 5 Jahren hinaus aufbewahrt werden. Haushaltsrelevante Akten und Unterlagen, die der Rechnungsprüfung unterliegen (z.B. Abrechnungsunterlagen für die Einkommensberechnung bei Elternbeiträgen) sollten nach Ende der Betreuungszeit 6 Jahre aufbewahrt werden. Wenn nicht mehr benötigte Daten von ausgeschiedenen Kindern (Adressenliste von Ehemaligen für spätere Einladungen) aufbewahrt werden sollen, ist das Einverständnis der Eltern einzuholen und die Zweckbindung festzulegen.


## Wer kontrolliert den Datenschutz?

Die Kontrolle des Datenschutzes obliegt im kirchlichen Bereich den Datenschutzbeauftragten der Kirchen. Der Bischof bestellt für den Bereich seines Bistums einen Diözesandatenschutzbeauftragten (Vgl. § 16 KDO), der über die Einhaltung der KDO sowie anderer Vorschriften über den Datenschutz wacht (Vgl. § 17 Abs. 1 KDO). Er kann Datenschutzverstöße gegenüber der für die Kindertagesstätte zuständigen aufsichtführenden Stelle beanstanden und diese zu einer Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auffordern (Vgl. § 18 Abs. 1 KDO). Er hat jedoch keine Befugnis, Sanktionen zu verhängen. Allerdings führen Beanstandungen des Datenschutzbeauftragten in der Regel dazu, dass die zuständigen aufsichtführenden Stellen von sich aus tätig werden und die Mängel beseitigen oder – wenn nötig – arbeitsrechtliche Konsequenzen einleiten. Mit der Beanstandung kann der Diözesandatenschutzbeauftragte Vorschläge zur Beseitigung der Mängel oder zu sonstigen Verbesserungen des Datenschutzes verbinden.

Der Kontrolle vorgelagert ist die Beratungsfunktion des Diözesandatenschutzbeauftragten. Träger, Einrichtungsleitungen, Mitarbeiterinnen und Mitarbeiter sowie die Eltern können sich bei Zweifelsfragen an den Datenschutzbeauftragten wenden und seine fachliche Stellungnahme einholen.

### Ansprechpartner im Bistum Trier

- Kirchlicher Datenschutz Bistum Trier:  
Rechtsdirektor Hartmut Junkes  
Ursulinenstraße 67, 66111 Saarbrücken  
Fon 06819068221, kabusa@t-online.de



Anordnung über den  
kirchlichen Datenschutz (KDO)

## Präambel

Aufgabe der Datenverarbeitung im kirchlichen Bereich ist es, die Tätigkeit der Dienststellen und Einrichtungen der Katholischen Kirche zu fördern. Dabei muss gewährleistet sein, dass der Einzelne durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht geschützt wird. Aufgrund des Rechtes der Katholischen Kirche, ihre Angelegenheiten selbst zu regeln, wird zu diesem Zweck die folgende Anordnung erlassen:

## § 1 Zweck und Anwendungsbereich

- (1) Zweck dieser Anordnung ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
- (2) Diese Anordnung gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch:
1. das Bistum, die Kirchengemeinden, die Kirchenstiftungen und die Kirchengemeindeverbände,
  2. den Deutschen Caritasverband, die Diözesan-Caritasverbände, ihre Untergliederungen und ihre Fachverbände ohne Rücksicht auf ihre Rechtsform,
  3. die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform.
- (3) Soweit besondere kirchliche oder staatliche Rechtsvorschriften auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieser Anordnung vor. Die Verpflichtung zur Wahrung des Beicht- und Seelsorgegeheimnisses, anderer gesetzlicher Geheimhaltungspflichten oder von anderen Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

## § 2 Begriffsbestimmungen

- (1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).
- (2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.
- (3) Erheben ist das Beschaffen von Daten über den Betroffenen.
- (4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren,
1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,

2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
  3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
    - a) die Daten an den Dritten weitergegeben werden
    - oder
    - b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abrufen,
  4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
  5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.
- (5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.
- (6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbarer natürlichen Person zugeordnet werden können.
- (7) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.
- (8) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.
- (9) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieser Anordnung personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.
- (10) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Dazu gehört nicht die Zugehörigkeit zu einer Kirche oder sonstigen Religionsgemeinschaft.

(11) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger, 1. die an den Betroffenen ausgegeben werden, 2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und 3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

### **§ 2a Datenvermeidung und Datensparsamkeit**

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

### **§ 3 Zulässigkeit der Datenerhebung, -verarbeitung oder -nutzung**

(1) Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, soweit 1. diese Anordnung oder eine andere kirchliche oder eine staatliche Rechtsvorschrift sie erlaubt oder anordnet oder 2. der Betroffene eingewilligt hat. (2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Sie bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. (3) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Abs. 2 Satz 3 auch dann vor, wenn durch die Schriftform der

bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Abs. 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszweckes ergibt, schriftlich festzuhalten.

(4) Soweit besondere Arten personenbezogener Daten (§ 2 Abs. 10) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

### **§ 3a Meldepflicht und Verzeichnis**

(1) Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, Verfahren automatisierter Verarbeitung vor Inbetriebnahme dem Diözesandatenschutzbeauftragten zu melden.

(2) Die Meldung hat folgende Angaben zu enthalten

1. Name und Anschrift der verantwortlichen Stelle,
2. Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung der Stelle berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
4. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
5. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
6. Regelfristen für die Löschung der Daten,
7. eine geplante Datenübermittlung ins Ausland,
8. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 6 KDO zur Gewährleistung der Sicherheit der Bearbeitung angemessen sind,
9. zugriffsberechtigte Personen.

(3) Die Meldepflicht entfällt, wenn für die verantwortliche Stelle ein betrieblicher Datenschutzbeauftragter nach § 18a bestellt wurde oder bei ihr höchstens zehn Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut sind.

(4) Die Angaben nach Abs. 2 sind von der kirchlichen Stelle in einem Verzeichnis vorzuhalten. Sie macht die Angaben nach Abs. 2 Nr. 1 bis 7 auf Antrag jedermann in geeigneter Weise verfügbar, der ein berechtigtes Interesse nachweist.

### **§ 4 Datengeheimnis**

Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

### **§ 5 Unabdingbare Rechte des Betroffenen**

(1) Die Rechte des Betroffenen auf Auskunft (§ 13) und auf Berichtigung, Löschung oder Sperrung (§ 14) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen automatisiert in einer Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage, festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene zu unterrichten.

### **§ 5a Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen**

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder
2. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbei-

tung oder Nutzung entsprechend § 13a zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

### **§ 5b Mobile personenbezogene Speicher- und Verarbeitungsmedien**

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie er seine Rechte nach den §§ 13 und 14 ausüben kann und über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

### **§ 6 Technische und organisatorische Maßnahmen**

Kirchliche Stellen im Geltungsbereich des § 1 Abs. 2, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieser Anordnung, insbesondere die in der Anlage zu dieser Anordnung genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

### **§ 7 Einrichtung automatisierter Abrufverfahren**

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufes bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der zu übermittelnden Daten,
4. nach § 6 erforderliche technische und organisatorische Maßnahmen.

(3) Über die Einrichtung von Abrufverfahren ist der Diözesandatenschutzbeauftragte unter Mitteilung der Festlegungen des Abs. 2 zu unterrichten.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts nutzen kann.

### **§ 8 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag**

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieser Anordnung und anderer Vorschriften über den Datenschutz verantwortlich. Die in § 5 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung (§ 2 Abs. 3), Datenverarbeitung (§ 2 Abs. 4) oder -nutzung (§ 2 Abs. 5), die technischen und organisatorischen Maßnahmen (§ 6) und etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen diese Anordnung oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Die Absätze 1 bis 3 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

### **§ 9 Datenerhebung**

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stellen erforderlich ist.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
- 2.a) die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,

2. die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und

3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss, zu unterrichten. Werden sie beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

(4) Werden personenbezogene Daten statt beim Betroffenen bei einer nichtkirchlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft ermächtigt, sonst auf die Freiwilligkeit ihrer Angaben, hinzuweisen.

(5) Das Erheben besonderer Arten personenbezogener Daten (§ 2 Abs. 10) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder dies aus Gründen eines wichtigen öffentlichen Interesses zwingend erforderlich ist,
2. der Betroffene nach Maßgabe des § 3 Abs. 4 eingewilligt hat,
3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat oder es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich ist,
5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist oder dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
6. der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert,
7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,

8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,

9. dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist.

## **§ 10 Datenspeicherung, -veränderung und -nutzung**

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt und kirchliche Interessen nicht entgegenstehen,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr einer Gefahr für die öffentliche Sicherheit oder erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder

zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,

8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

10. der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 2 Abs.10) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 9 Abs. 5 Nr. 1 bis 6 oder 9 zulassen würden oder
2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das kirchliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des kirchlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 2 Abs. 10) zu den in § 9 Abs. 5 Nr. 7 genannten Zwecken richtet sich nach den für die in § 9 Abs. 5 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

### **§ 11 Datenübermittlung an kirchliche und öffentliche Stellen**

(1) Die Übermittlung personenbezogener Daten an Stellen im Geltungsbereich des § 1 ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder der empfangenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen der empfangenden kirchlichen Stelle, trägt diese die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben der empfangenden kirchlichen Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 7 Abs. 4 bleibt unberührt.

(3) Die empfangende kirchliche Stelle darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihr übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 10 Abs. 2 zulässig

(4) Für die Übermittlung personenbezogener Daten an öffentliche Stellen und an kirchliche Stellen außerhalb des Geltungsbereichs des § 1 gelten die Abs. 1–3 entsprechend, sofern sichergestellt ist, dass bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Abs. 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechnete Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) Abs. 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer kirchlichen Stelle weitergegeben werden.

### **§ 12 Datenübermittlung an nicht kirchliche und nicht öffentliche Stellen**

(1) Die Übermittlung personenbezogener Daten an nicht kirchliche Stellen, nicht öffentliche Stellen oder Personen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden, oder
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 2 Abs. 10) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 10 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, wenn die Unterrichtung wegen der Art der personenbezogenen Daten unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen nicht geboten erscheint, wenn die Unterrichtung die öffentliche Sicherheit gefährden oder dem kirchlichen Wohl Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

### **§ 13 Auskunft an den Betroffenen**

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über:

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und

3. den Zweck der Speicherung.  
In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Das Bistum bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung.

(2) Abs. 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsgemäßer oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Die Auskunftserteilung unterbleibt soweit,

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft dem kirchlichen Wohl Nachteile bereiten würde,
3. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden würde,
4. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen oder rechtlichen Gründe auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Diözesandatenschutzbeauftragten wenden kann.

(5) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Diözesandatenschutzbeauftragten zu erteilen, soweit nicht das Bistum im Einzelfall feststellt, dass dadurch das kirchliche Wohl beeinträchtigt wird. Die Mitteilung des Diözesandatenschutzbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(6) Die Auskunft ist unentgeltlich.

### § 13a Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder
3. die Speicherung oder Übermittlung der personenbezogenen Daten durch eine Rechtsvorschrift ausdrücklich vorgesehen ist.

(3) § 13 Abs. 2 und 3 gelten entsprechend.

### § 14 Berichtigung, Löschung oder Sperrung von Daten; Widerspruchsrecht

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

(2) Personenbezogene Daten, die auto-

tomatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
  2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.
- (3) An die Stelle einer Löschung tritt eine Sperrung, soweit
1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstellen,
  2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden oder
  3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.
- (4) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.
- (5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.
- (6) Personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die verantwortliche Stelle im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.
- (7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn
1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen, im überwiegenden

Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.
- (8) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

### § 15 Anrufung des Diözesandatenschutzbeauftragten

Jedermann kann sich an den Diözesandatenschutzbeauftragten wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch Stellen gemäß § 1 Abs. 2 in seinen Rechten verletzt worden zu sein.

### § 16 Bestellung und Rechtsstellung des Diözesandatenschutzbeauftragten

(1) Der Bischof bestellt für den Bereich seines Bistums einen Diözesandatenschutzbeauftragten. Die Bestellung erfolgt für die Dauer von drei Jahren. Wiederbestellung ist möglich. Bei Vorliegen eines wichtigen Grundes, kann der Bischof vorzeitig die Bestellung zurücknehmen. Auf Antrag des Beauftragten nimmt der Bischof die Bestellung zurück.

(2) Zum Diözesandatenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Er ist auf die gewissenhafte Erfüllung seiner Pflichten und die Einhaltung des kirchlichen und des für die Kirchen verbindlichen staatlichen Rechts zu verpflichten.

(3) Der Diözesandatenschutzbeauftragte ist in Ausübung seiner Tätigkeit unabhängig und nur dem kirchlichen Recht und dem für die Kirchen verbindlichen staatlichen Recht unterworfen.

(4) Der Diözesandatenschutzbeauftragte ist, auch nach Beendigung seines Auftrages, verpflichtet, über die ihm in seiner Eigenschaft als Diözesandatenschutzbe-



auftragtem bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

(5) Der Diözesandatenschutzbeauftragte darf, auch wenn sein Auftrag beendet ist, über solche Angelegenheiten ohne Genehmigung des Bischofs weder vor Gericht noch außergerichtlich Aussagen oder Erklärungen abgeben. Die Genehmigung, als Zeuge auszusagen, wird in der Regel erteilt. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen.

### **§ 17 Aufgaben des Diözesandatenschutzbeauftragten**

(1) Der Diözesandatenschutzbeauftragte wacht über die Einhaltung der Vorschriften dieser Anordnung sowie anderer Vorschriften über den Datenschutz. Er kann Empfehlungen

zur Verbesserung des Datenschutzes geben. Des Weiteren kann er die bischöfliche Behörde und sonstige kirchliche Dienststellen in seinem Bereich in Fragen des Datenschutzes beraten. Auf Anforderung der bischöflichen Behörde hat der Diözesandatenschutzbeauftragte Gutachten zu erstellen und Berichte zu erstatten.

(2) Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, den Diözesandatenschutzbeauftragten bei der Erfüllung seiner Aufgaben zur unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme,

2. während der Dienstzeit Zutritt zu allen Diensträumen, die der Verarbeitung und Aufbewahrung automatisierter Dateien dienen, zu gewähren, soweit nicht sonstige kirchliche Vorschriften entgegenstehen.

(3) Der Diözesandatenschutzbeauftragte erstattet dem Bischof alle drei Jahre einen Tätigkeitsbericht. Der Tätigkeitsbericht soll auch eine Darstellung der wesentlichen Entwicklungen des Datenschutzes im nichtkirchlichen Bereich enthalten.

(4) Der Diözesandatenschutzbeauftragte wirkt auf die Zusammenarbeit mit den kirchlichen Stellen, insbesondere mit den anderen Diözesandatenschutzbeauftragten, hin.

(5) Zu seinem Aufgabenbereich gehört die Zusammenarbeit mit den staatlichen Beauftragten für den Datenschutz.

### **§ 18 Beanstandungen durch den Diözesandatenschutzbeauftragten**

(1) Stellt der Diözesandatenschutzbeauftragte Verstöße gegen die Vorschriften dieser Anordnung oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er diese gegenüber der zuständigen aufsichtsführenden Stelle und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf.

(2) Der Diözesandatenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt.

(3) Mit der Beanstandung kann der Diözesandatenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gem. Abs. 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandungen des Diözesandatenschutzbeauftragten getroffen worden sind.

### **§ 18a Betrieblicher Beauftragter für den Datenschutz**

(1) Kirchliche Stellen im Sinne des § 1 Abs. 2, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, können einen betrieblichen Datenschutzbeauftragten schriftlich bestellen.

(2) Zum betrieblichen Datenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der kirchlichen Stelle betraut werden. Ein betrieblicher Datenschutzbeauftragter kann von mehreren kirchlichen Stellen bestellt werden.

(3) Der betriebliche Datenschutzbeauftragte ist dem Leiter der kirchlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.

(4) Die kirchlichen Stellen haben den betrieblichen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Betroffene können sich jederzeit

an den betrieblichen Datenschutzbeauftragten wenden.

(5) Im Übrigen findet § 16 entsprechende Anwendung.

### **§ 18b Aufgaben des betrieblichen Datenschutzbeauftragten**

(1) Der betriebliche Datenschutzbeauftragte wirkt auf die Einhaltung dieser Anordnung und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann er sich in Zweifelsfällen an den Diözesandatenschutzbeauftragten gem. § 16 KDO wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieser Anordnung sowie anderer Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem betrieblichen Datenschutzbeauftragten ist von der verantwortlichen Stelle eine Übersicht nach § 3 a Abs. 2 zur Verfügung zu stellen.

(3) Der betriebliche Datenschutzbeauftragte macht die Angaben nach § 3 a Abs. 2 Nr. 1 bis 7 auf Antrag jedermann in geeigneter Weise verfügbar, der ein berechtigtes Interesse nachweist.

### **§ 19 Ermächtigungen**

Die zur Durchführung dieser Anordnung erforderlichen Regelungen trifft der Generalvikar. Er legt insbesondere fest:

- a) den Inhalt der Meldung gem. § 3a,
- b) den Inhalt der schriftlichen Verpflichtungserklärung gem. § 4 Satz 2,
- c) die technischen und organisatorischen Maßnahmen gem. § 6 Satz 1.

### **§ 20 Schlussbestimmung**

Diese Anordnung tritt am 1. Januar 2004 in Kraft. Gleichzeitig tritt die Anordnung über den kirchlichen Datenschutz - KDO vom 15. Dezember 1993 außer Kraft. Trier, 20. Oktober 2003

## Anlage zur KDO

### Verpflichtungserklärung der Mitarbeiterinnen und Mitarbeiter zum Datenschutz

#### Ich verpflichte mich,

1. die Anordnung über den kirchlichen Datenschutz – KDO – des Bistums Trier vom 1.11.2003 sowie die anderen für meine Tätigkeit geltenden Datenschutzregelungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen sorgfältig einzuhalten und bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Bestimmungen hingewiesen wurde. Ich wurde ferner darauf hingewiesen, dass die KDO und die Texte der übrigen für meine Tätigkeit geltenden Datenschutzvorschriften bei

eingesehen und auch für kurze Zeit ausgeliehen werden können,

2. das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten.  
Ich bin darüber belehrt worden, dass ein Verstoß gegen das Datengeheimnis gleichzeitig einen Verstoß gegen die Schweigepflicht darstellt, der disziplinarrechtliche beziehungsweise arbeitsrechtliche/rechtliche Folgen haben kann.

Diese Erklärung wird zu den Akten genommen.

Vor- und Zuname, Anschrift

Ort, Datum, Unterschrift

- 20 Einverständnis für die Veröffentlichung von Gruppenfotos auf der Homepage der Kita
- 21 Vereinbarung zum Datenschutz bei Fotos und Videoaufnahmen, Recht am Bild
- 22 Einwilligung zur Zusammenarbeit bei der Behandlung des Kindes
- 23 Einwilligung zur Zusammenarbeit mit der Grundschule

## Muster als Kopiervorlagen



## Einverständnis für die Veröffentlichung von Gruppenfotos auf der Homepage der Kita

Name der Einrichtung

Liebe Eltern,

wir betreiben unter folgender Adresse

eine Homepage im Internet, die Interessenten Einblick in unsere Arbeit geben soll.

Name des Kindes

Mit der Veröffentlichung von Gruppenfotos, auf denen auch mein Kind abgebildet ist, bin ich einverstanden.

Datum, Name, Unterschrift der/des Personensorgeberechtigten

Die Homepage kann von jedem Internet-Benutzer angesehen werden, Besucher können Bilder der Homepage auf ihren privaten PC herunterladen. Deshalb sind wir mit der Veröffentlichung von Fotos unserer Kinder sehr vorsichtig. Aber häufig kann eine Veranstaltung in der Kita oder ein Projekt der Kinder für Interessenten nur anschaulich und gut dokumentiert werden, wenn dabei auch Bilder der Kinder gezeigt werden.

Eine Veröffentlichung von Bildern im Internet kann selbstverständlich nur dann erfolgen, wenn die Eltern der abgebildeten Kinder hiervon Kenntnis haben und ihr Einverständnis erklärt haben. Außerdem sehen wir uns verpflichtet, auch die Kinder selbst um ihr Einverständnis zu bitten, wenn wir von ihnen Bilder im Internet veröffentlichen. Einzelfotos oder Fotos, auf denen bis zu drei Kinder abgebildet sind, werden nur dann im Internet veröffentlicht, wenn die Eltern und die betroffenen Kinder hierzu ausdrücklich ihr Einverständnis erklärt haben.

Bei Fotos, auf denen mehr als drei Kinder abgebildet sind (Gruppenfotos) bitten wir Sie vorab um ihr Einverständnis zur Veröffentlichung auf unserer Homepage mit der beigefügten Erklärung. Die Einverständniserklärung kann jederzeit widerrufen werden. Wenn für einen der abgebildeten Personen das Einverständnis widerrufen wird, nehmen wir das Bild unverzüglich von der Homepage. Bitte beachten Sie jedoch, dass die Kita auf die Speicherung an anderer Stelle keinen Einfluss hat. Zum Schutz vor unbefugter Verwertung werden die auf der Homepage veröffentlichten Bilder im einem Copyright-Vermerk versehen.

## Datenschutz bei Fotos und Videoaufnahmen, Recht am Bild

Name der Einrichtung

## Vereinbarung zu Fotos und anderen Bildaufnahmen in der Kindertageseinrichtung

Unverzichtbarer Bestandteil der pädagogischen Arbeit in der Kindertagesstätte ist die Beobachtung und Dokumentation der Bildungs- und Lernprozesse des Kindes nach Maßgabe der Konzeption und unter Beachtung des Datenschutzes. Hierzu gehört auch, dass im Rahmen der pädagogischen Arbeit Fotos und Videoaufnahmen des Kindes gemacht werden und gemeinsame Aktivitäten dokumentiert werden.

- Die Eltern haben das Recht auf Auskunft und Einsicht in die von Ihrem Kind gemachten Fotos und Videoaufnahmen. Soweit es sich um Einzelaufnahmen ihres Kindes handelt, haben sie ein Recht auf Sperrung und Löschung.
- Die Weitergabe von internen Aufnahmen an Dritte sowie die Veröffentlichung im Internet sind ohne die ausdrückliche Einwilligung der Eltern nicht zulässig.
- Die Eltern stellen ihrerseits sicher, dass ihnen überlassene Foto- und Videoaufnahmen anderer Kinder oder sonstiger Personen (Eltern, Erzieherinnen etc. ) nicht ohne deren Einverständnis weitergegeben oder veröffentlicht werden. Das Recht am Bild bleibt unberührt.

Datum, Name, Unterschrift der/des Personensorgeberechtigten

Datum, Unterschrift des Trägervertreters

# Einwilligung zur Zusammenarbeit bei der Behandlung des Kindes

Name der Einrichtung

Das Kind

Name des Kindes

besucht die Kindertagesstätte und ist gleichzeitig in Behandlung bei

Behandelnde Stelle (Name, Anschrift)

Um die Förderung des Kindes optimal aufeinander einzustellen ist eine fachliche Zusammenarbeit der Kindertagesstätte mit der behandelnden Stelle notwendig. Hierzu gehören gemeinsame Gespräche über

- den Gesundheitszustand des Kindes
- den Entwicklungsstand und die besonderen Bedürfnisse des Kindes
- die jeweils vorzunehmenden Förderungsmaßnahmen und Unterstützungsleistungen
- den Behandlungsfortschritt und die Wirkungen auf die Entwicklung des Kindes.

Die Personensorgeberechtigten erklären ihr Einverständnis, dass die Kindertagsstätte mit der behandelnden Stelle in der genannten Weise zum Wohle des Kindes zusammenarbeitet. Im Übrigen ist die Kindertagsstätte verpflichtet, den Sozialdatenschutz (§ 35 SGB I) einzuhalten und über den Inhalt der Behandlung gegenüber Dritten Stillschweigen zu bewahren.

Datum, Name, Unterschrift der/des Personensorgeberechtigten

## Einwilligung zur Zusammenarbeit mit der Grundschule

Name der Einrichtung

Die Zusammenarbeit zwischen Kindergarten und Grundschule im letzten Kindergartenjahr und im ersten Schuljahr erfordert zwischen den in den Kindergärten eingesetzten Fachkräften und den Lehrkräften an Grundschulen einen intensiven Informationsaustausch. Gespräche über die individuelle Entwicklung einzelner Kinder sollten möglichst im Beisein der Eltern geführt werden.

Die bei den Trägern der Kindergärten erhobenen personenbezogenen Daten der Kinder und deren Erziehungsberechtigten an die mit der Zusammenarbeit betraute Lehrkraft und an die Schulleitung der betreffenden Grundschulen dürfen nur übermittelt werden, wenn eine schriftliche Einwilligung der Erziehungsberechtigten vorliegt. Dazu gehören auch Daten der Kinder über den Entwicklungsprozess und den Entwicklungsfortschritt.

Die Erziehungsberechtigten haben ein Recht auf Einsicht in die sie und ihre Kinder betreffenden Unterlagen des Kindergartens und auf unentgeltliche Auskunft über die sie und ihre Kinder betreffenden Daten. Die Personensorgeberechtigten erklären ihr Einverständnis, dass der Kindergarten zur Erleichterung des Übergangs in die Grundschule mit den zur Zusammenarbeit betrauten Lehrkräften und der Schulleitung Informationen über die individuelle Entwicklung ihres Kindes austauscht.

Name des Kindes

Name der Grundschule

Datum, Name, Unterschrift der/des Personensorgeberechtigten

# QM

TRI<sup>er</sup> QM<sup>elementar</sup>



Herausgeber:  
Caritasverband für die Diözese Trier e.V.  
Abteilung Kindertageseinrichtungen  
Sichelstraße 10 · 54290 Trier · Telefon 0651-94930  
dicv@caritas-trier.de · www.caritas-trier.de