FAQ zum Thema Datenschutz in der Jugendpastoral

Grundsätze und Verfahrenshinweise

Bernd Siebertz,
stellvertretender Leiter der Abteilung Jugendseelsorge
Erzbischöfliches Generalvikariat Köln

Am 24. Mai 2018 ist das Gesetz über den Kirchlichen Datenschutz (KDG) in Kraft getreten. Das KDG ist bei allen Einrichtungen anzuwenden, die vorrangig kirchliche Zwecke erfüllen, unabhängig davon, welche Rechtsform sie haben, d.h. auch bei Ortsgruppen von Jugendverbänden, Jugendagenturen, usw.

Im Grundsatz geht es bei den neuen gesetzlichen Regelungen darum, alle personenbezogenen Daten besonders zu schützen. So heißt es in § 1 des KDG:

> *Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch die Verarbeitung seiner personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, und den freien Verkehr solcher Daten zu ermöglichen.*

Das ist sehr sinnvoll. Die Umsetzung erfordert aber einen gewissen Aufwand.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Angaben, die eine Person identifizierbar machen, so zum Beispiel

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail-Adresse
- Kontonummer
- KFZ-Kennzeichen
- Personalausweisnummer, Sozialversicherungsnummer
- Erweiterte Führungszeugnisse
- Standortdaten
- Online-Kennungen
- Fotos

Welche Grundsätze sind bei dem Datenschutz zu beachten?

Rechtmäßigkeit der Verarbeitung

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten wird in § 6 KDG näher konkretisiert. Die Verarbeitung von personenbezogenen Daten ist demnach insbesondere rechtmäßig, wenn eine Rechtsgrundlage für die Datenverarbeitung vorliegt, d. h. insbesondere die Einwilligung der betroffenen Person vorliegt.

Grundsatz der Transparenz

Der Grundsatz der Transparenz soll gewährleisten, dass die betroffenen Personen ihre Rechte wahrnehmen können. Der Grundsatz der Transparenz wird insbesondere durch die Informationspflichten bei der Erhebung von personenbezogenen Daten sowie das Auskunftsrecht der betroffenen Person präzisiert. (§§17 ff.)

Grundsatz der Datenminimierung (Datensparsamkeit)

Personenbezogene Daten müssen dem Zweck angemessen sein. Und sich auf das notwendige Maß beschränken.

[Ausrufezeichen] In der Praxis bedeutet das, nur die Daten abzufragen, die jeweils notwendig sind. Bei der Anmeldung zu einer Ferienfreizeit z. B. nur den Namen des Kindes und die Kontaktdaten der Eltern. Ist die Teilnahme des Kindes dann sicher, können die Kontoverbindung, medizinische Daten oder Besonderheiten in der Ernährung abgefragt werden. Niemand muss wissen, ob ein Kind, das gar nicht mit auf Reisen geht, vegan lebt ist oder gegen Hausstaub allergisch.

Grundsatz der Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden. Und nur für diese Zwecke dürfen sie weiterverarbeitet werden. Eine weitere Verarbeitung zu anderen Zwecken ist nur möglich, sofern die Zwecke der Weiterverarbeitung mit den ursprünglichen Erhebungszwecken vereinbar sind und eine Rechtsgrundlage, also eine Einverständniserklärung oder ein Vertrag hierfür vorliegt.

Richtigkeit der Datenverarbeitung

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Personenbezogene Daten, die nicht mehr richtig sind, müssen unverzüglich gelöscht oder berichtigt werden (§ 7 KDG).

Speicherbegrenzung

Mit der normierten Speicherbeschränkung dürfen personenbezogene Daten nur in einer Form gespeichert werden, die die Identifizierung der Person nur so lange ermöglicht, wie es erforderlich ist. Sobald die Speicherung personenbezogener Daten für den Verarbeitungszweck nicht mehr erforderlich ist, müssen personenbezogene Daten gelöscht werden. Das heißt, er muss vor dem Sammeln der Daten bereits festgelegt sein, wann diese wieder gelöscht werden. (§ 7 KDG)

Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies umfasst auch den Schutz vor unbefugter und unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung der personenbezogenen Daten. Hierfür sind geeignete technische und organisatorische Maßnahmen zu treffen (§ 7 KDG). Die Daten müssen also beispielsweise in geschützten Verzeichnissen abgelegt oder in verschlossenen Schränken abgestellt sein, zu denen nur die Personen Zugang haben, die unbedingt mit den Daten arbeiten müssen.

Die Einhaltung der vorgenannten Grundsätze ist zu beachten. Insbesondere ist immer darauf zu achten, dass nur solche Daten gespeichert werden, die zur Erreichung des Zwecks der speichernden Stelle nötig sind. Erforderlich sind danach nur Daten, die sinnvollerweise benötigt werden, um den Anforderungen der jeweiligen Stelle gerecht zu werden. Es ist mithin vorab immer zu prüfen, ob die Verarbeitung von Daten an dem entsprechenden Speicherort im Rahmen des Aufgabenbereiches zur Erreichung des Zwecks an dieser Stelle nötig ist. Oder kurz: Besser weniger, als mehr!

Welche Maßnahmen sind zu veranlassen?

1. Bestellung eines betrieblichen Datenschutzbeauftragten

Unter anderem ist dann ein betrieblicher Datenschutzbeauftragter zu benennen, wenn mindestens 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind. Dazu zählen auch die ehrenamtlichen Helfer.
[Ausrufezeichen] Diese Anforderung lädt dazu ein, genau zu prüfen, wer notwendigerweise mit personenbezogenen Daten arbeiten muss. In der Regel stellt sich heraus, dass der Kreis der Nutzer viel kleiner sein kann, als man vermutet.

2. Inhalt der Website anpassen

Der gesamte Inhalt auf der Website muss die Anforderungen des kirchlichen Datenschutzgesetzes erfüllen, dies gilt auch bereits für früher veröffentliche Inhalte. Ihre Website muss eine Datenschutzerklärung enthalten. In dieser Erklärung muss ausführlich aufgeführt werden, welche Daten bei dem Besuch und bei der Nutzung der Website erhoben und verwendet werden. Zudem muss der Nutzer über seine Rechte aufgeklärt werden.

Beispiele:
- Datenschutzhinweise auf kja.de
- Datenschutzhinweise auf erzbistum-koeln.de

3. Überprüfung der Grundlage für die Verarbeitung von personenbezogenen Daten

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, soweit der Betroffene eingewilligt hat, eine Rechtsvorschrift es erlaubt oder anordnet .

Nach § 6 KDG ist die Datenverarbeitung z. B. zulässig für die Wahrnehmung einer Aufgabe, die im kirchlichen Interesse liegt. Fehlt eine solche Rechtsvorschrift, ist – wie vorstehend angeführt – die Einwilligung der betroffenen Person notwendig. Bei der Einholung der Einwilligung von den Betroffenen sind diese auf den Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung hinzuweisen.

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Sie muss schriftlich erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

Im Hinblick auf den Umgang mit personenbezogenen Daten von Kindern unter 16 Jahren gibt es besondere Anforderungen. Personenbezogene Daten eines Minderjährigen, dem elektronisch eine Dienstleistung oder ein vergleichbares anderes Angebot von einer kirchlichen Stelle gemacht wird, dürfen nur verarbeitet werden, wenn der Minderjährige das 16. Lebensjahr vollendet hat. Hat der Minderjährige das 16. Lebensjahr noch nicht vollendet, ist die Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Personensorgeberechtigten erteilt wird.

4. Überprüfung von Auftragsdatenvereinbarungen

Charakteristisch für die Auftragsdatenverarbeitung ist, dass externe Dienstleister damit beauftragt sind, personenbezogene Daten zu verarbeiten. Das ist zum Beispiel dann der Fall, wenn der Trägerverein einer Offenen Tür ein Steuerberatungsbüro mit der Buchführung beauftragt hat.

Die Verantwortung für die ordnungsgemäße Datenverarbeitung verbleibt bei dem Auftraggeber, d. h. er muss sich um den Datenschutz kümmern.

5. Generelle Überprüfung von Verträgen

Auch die Datenschutzregelungen in anderen Verträgen sind im Hinblick auf die Anforderungen des KDG zu überprüfen. So müssen z. B. sämtliche Anmeldungen u. ä. im Hinblick auf die vorliegenden Einwilligungen überprüft werden.

6. Erfüllung der Informationspflichten und damit einhergehende Rechte des Betroffenen

Der Verantwortliche für die Datenverarbeitung hat gegenüber den betroffenen Personen bestimmte Informationspflichten zu erfüllen (§§ 14 bis 16 KDG).

Die betroffenen Personen haben Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch, die nicht durch Rechtsgeschäfte ausgeschlossen oder beschränkt werden dürfen (§§ 17 – 25 KDG).

Das bedeutet in der Praxis, dass man sehr genau wissen sollte, wo Daten abgelegt sind. Ansonsten kann man die Anforderungen nicht erfüllen. Es spricht viel dafür nur einen Ort zu haben, an dem Daten abgelegt sind.

7. Gewährleistung von Datensicherheit und IT-Sicherheit

Das KDG verlangt bei der Datenverarbeitung, geeignete technische und organisatorische Maßnahmen zu treffen um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu gehören beispielsweise Verschlüsselungstechnologien, taugliche Passwortpolice, laufende Software-Updates, Einsatz von Firewalls, Virenschutz etc. und das Auslagern sensibler Daten in Rechenzentren sowie der Zugangsschutz für Serverräume und Aktenarchive.

8. Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten

Gemäß § 31 KDG hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, zu führen. Dieses Verzeichnis hat die in § 31 KDG angegebenen Angaben zu enthalten. Ersichtlich muss insbesondere sein, aus welchem Grund und auf welche Weise und von wem personenbezogene Daten verarbeitet werden. Es handelt sich hier um eine fortlaufende Tätigkeit. Sofern sich Prozesse ändern, muss dies für einen Außenstehenden nachvollziehbar dokumentiert werden. Kommt beispielsweise eine neue Software zum Einsatz oder werden Daten zusätzlich ausgewertet, muss dies angegeben werden.
[Ausrufezeichen] Es muss schriftlich festgehalten werden, wie und wo Daten vorgehalten werden und wann diese wieder gelöscht werden. Ändert sich im Laufe der Zeit das Verfahren, dann muss es neu beschrieben werden.

9. Ergreifen von Maßnahmen bei Datenpannen

Gemäß § 33 KDG ist binnen 72 Stunden nach Bekanntwerden eines datenschutzrechtlichen Vorfalls, der eine Gefahr für die Rechte und Freiheit natürlicher Personen darstellt, der zuständigen Aufsichtsbehörde eine Meldung zu machen.

10. Recht auf Löschung

Man muss in der Lage sein, personenbezogene Daten jeder Person komplett zu löschen, wenn sie es verlangt und kein berechtigtes Interesse entgegensteht.

Wie hat eine Erklärung über die Einwilligung zur Speicherung und Verarbeitung von personenbezogenen Daten auszusehen?

Nachfolgend erhalten Sie ein Muster bezüglich einer Einwilligung bei der Speicherung und Verarbeitung von Daten im Rahmen der Teilnahme an einer Ferienfreizeit.

Muster

Ich, (Name/Vorname/Anschrift – im Fall von Minderjährigen auch die entsprechenden Angaben der Erziehungsberechtigten) bin damit einverstanden, dass meine folgenden Daten zum Zweck der Teilnahme an der Ferienfreizeit .....gespeichert und verarbeitet werden.

.....
.....
.....

Mir ist bekannt, dass die Einwilligung bezüglich der Speicherung und Verarbeitung der vorstehenden Angaben freiwillig erfolgt.

Die Einwilligung zur Datenspeicherung und Datenverarbeitung kann jederzeit ganz oder teilweise mit Wirkung für die Zukunft widerrufen werden. Schreiben Sie dazu eine E-Mail an .....Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Ein ausgeübter Widerruf kann .....zur Folge haben.

Ich wurde im Rahmen eines separaten Informationsschreibens darüber informiert, dass ich jederzeit Auskunft über meine gespeicherten personenbezogenen Daten erhalte (§ 17 KDG), deren Berichtigung (§ 18 KDG), Löschung (§ 19 KDG) oder Einschränkung der Verarbeitung (§ 20 KDG) verlangen sowie mein Recht auf Datenübertragbarkeit (§ 22 KDG) geltend machen kann. Ebenfalls wurde ich dahingehend informiert, dass ich jederzeit gegen die Verarbeitung der mich betreffenden personenbezogenen Daten Widerspruch einlegen kann.

Ort, Datum .....

.....
Unterschrift

Wie ist mit der Nutzung von WhatsApp umzugehen?

Die Nutzung von WhatsApp im Arbeitsalltag hat gleich mehrere Fallstricke. Bereits zum Zeitpunkt der Installation synchronisiert WhatsApp das komplette Adressbuch und versendet die Daten in die USA. Somit liegen auch Handynummern von Personen bei der Mutterfirma facebook vor, die gar kein WhatsApp verwenden. Der Messenger greift insoweit auf Informationen von Personen zu, die das nie erlaubt haben bzw. noch nicht einmal wissen, dass ihre Daten auf einem amerikanischen Server gespeichert sind.
Aufgrund der Tatsache, dass die Daten auf Servern der Mutterfirma facebook in den USA gespeichert werden, welche nicht dem europäischen Datenschutzrecht unterliegen und der Messenger-Dienst als Identifizierungsmerkmal das jeweilige Handy-Telefonbuch, also personenbezogene Daten nutzt, ist die Nutzung von WhatsApp nicht mit dem Kirchlichen Datenschutzgesetz kompatibel.
[Ausrufezeichen]Demgemäß hat die Konferenz der Diözesandatenschutzbeauftragten beschlossen, dass eine dienstliche Nutzung von WhatsApp nicht zulässig ist. So dürfen keinerlei dienstliche Informationen über diesen Dienst ausgetauscht werden. Soweit die App auf dienstlichen Geräten installiert ist, erfolgt die Benutzung ausschließlich privat. Der Besitzer des Gerätes trägt die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften. Mitarbeiterinnen und Mitarbeiter sind angewiesen, die Berechtigung der App, auf Kontakte zuzugreifen, auszuschalten.

Die Diözesandatenschutzbeauftragten gehen im Rahmen ihres Beschlusses in der Regel von hauptberuflichen Mitarbeitern der Kirche aus. Insoweit sind die Formulierungen nicht immer auf den jugendpastoralen Bereich zu übertragen. Erwähnt wird jedoch in den Vorgaben der Diözesandatenschutzbeauftragten die Nutzung des Messenger zu privaten Zwecken. Diesbezüglich wird ausgeführt, dass – soweit der Messenger zu privaten Zwecken eingesetzt wird - durch Anleitungen in der Downloadseite versucht werden soll, die Nutzer zu einer datenschutzgerechten Einstellung zu bewegen, die weiteren Schaden verhindert. Als minimalste Maßnahme sollte der Zugang zu den Kontaktdaten für WhatsApp gesperrt werden, d. h. die Nutzer sind anzuweisen, die Berechtigung der App, auf Kontakte zuzugreifen, auszuschalten.

Hier ist folgendermaßen vorzugehen:

Apple-Geräte: Einstellungen>Datenschutz> Kontakte> WhatsApp

Android-Geräte (erst ab Android 6.0 möglich): Einstellungen>Apps> (WhatsApp) > Berechtigungen

Weiterhin sollten die Jugendlichen dazu angehalten werden, keine Adresslisten, Passwörter, Protokolle o.ä. über den Messenger auszutauschen.

Zudem sollten die Jugendlichen vorab die entsprechenden Hinweise zur Nutzung von WhatsApp erhalten, welche wie folgt aussehen können:

> *„Wenn Sie WhatsApp auf Ihrem Mobilgerät installieren und nutzen, stimmen Sie den Allgemeinen Geschäftsbedingungen von WhatsApp zu, auf die wir keinen Einfluss haben. Diese beinhalten u.a., dass die WhatsApp Inc. Zugriff auf alle Telefonnummern und die auf den Mobilgeräten gespeicherten Kontakte, d.h. auch auf solche, welche WhatsApp nicht nutzen, erhält. Die Daten werden auf Servern bei der Mutterfirma facebook in den USA gespeichert, welche nicht dem europäischen Datenschutzrecht unterliegen. Eine solche Nutzung wird daher aufgrund der Anforderungen nach dem Kirchlichen Datenschutzgesetz untersagt .“*

Dies kann vor Ort über die Anmeldung zum entsprechenden Angebot erfolgen. Die Jugendlichen können dies selbst erklären, da sie über 16 Jahre alt sind (vgl. Allgemeine Geschäftsbedingungen von WhatsApp). Soweit sie jünger sind und WhatsApp dementsprechend nicht nutzen dürfen, muss eine entsprechende Erklärung der Eltern eingeholt werden.

Alle Nicht-WhatsApp-Nutzer muss man ebenfalls über die Weitergabe ihrer Daten an Facebook informieren.

Letztlich gibt es Alternativen zu WhatsApp, d.h. zum Beispiel den Messenger-Dienst Hoccer oder den Messenger-Dienst Signal. Weiterhin wird von den Diözesandatenschutzbeauftragten auch der Messenger-Dienst Wire vorgeschlagen. Die vorgenannten Messenger-Dienste können unter datenschutzrechtlichen Gesichtspunkten genutzt werden.

Was ist bei der Verarbeitung und Veröffentlichung von Bildern und Fotografien zu beachten?

In der Regel werden beim Fotografieren von Menschen dann personenbezogene Daten erhoben, wenn die Bilder digital (§ 2 Abs. 1 KDG) im Sinne einer automatisierten Verarbeitung aufgenommen werden und zur Identifikation des Aufgenommenen geeignet sind. Auch hier gilt insoweit das Verbot mit Erlaubnisvorbehalt, d.h. auch eine Verarbeitung von Fotos ist generell nur durch eine Rechtfertigung möglich. Es muss mithin entweder eine gesetzliche Grundlage oder die Einwilligung des Betroffenen in die Verarbeitung vorliegen. Dies bezieht sich auf das Erheben und Speichern der Fotos sowie im Hinblick auf die Veröffentlichung der Fotos.

Die Veröffentlichung von Bildern, z.B. im Internet, kann ebenfalls wie das Erheben und Speichern der Bilder nach § 6 Abs. 1 lit.g) rechtmäßig sein, d.h. zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erfolgen. Hier ist eine Abwägung von diesen Interessen mit den Grundrechten oder den Grundfreiheiten der betroffenen Personen erforderlich. Als Hilfestellung bei der Interessenabwägung können unabhängig davon, ob das Kunsturhebergesetz neben dem KDG Anwendung findet, zumindest die dort genannten Kriterien und die dazu ergangenen Entscheidungen der Gerichte dienen. Soweit beispielsweise Bildnisse aus dem Bereich der Zeitgeschichte veröffentlicht werden oder Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeiten erscheinen, spricht dies dafür, dass die Abwägung mit den betroffenen Rechten zugunsten der Interessen des Fotografen an einer Veröffentlichung ausfällt. Gleiches gilt für Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben.

Auf der anderen Seite spricht vieles dafür, dass nicht mehr von einem bloßen Beiwerk im Rahmen der Aufnahme auszugehen ist, wenn einzelne Personen hervorgehoben werden oder einzelne oder wenige Personen Gegenstand der Bilder sind.

Zu beachten sind die Regelungen zum Schutz der Minderjährigen, auf die sich die Konferenz der Diözesandatenschutzbeauftragten im April geeinigt hat. Bei Bildern von Kindern unter 16 Jahren ist vor Veröffentlichung die Einwilligung der Sorgeberechtigten für jedes einzelne Bild einzuholen.