ARBEITSHILFE DATENSCHUTZ

BDKJ Bund der Deutschen Katholischen Jugend

afj
Arbeitsstelle für Jugendseelsorge der Deutschen Bischofskonferenz

jhd Bundeszentrale für Katholische Jugendarbeit Jugendhaus Düsseldorf

INHALT

PRÄAMBEL – WARUM EIGENTLICH DATEN SCHÜTZEN?

Kein WhatsApp mehr, ständig irgendwelche E-Mails wegen geänderter Datenschutz-Bestimmungen und auf jeder Website ein fettes Pop-up wegen Cookies… gibt es eigentlich ein Thema, das noch mehr nervt als Datenschutz? Was soll das Ganze eigentlich? Und warum dazu jetzt noch eine Arbeitshilfe für die Jugendarbeit und Jugendpastoral?

Bevor es Missverständnisse gibt: Auch der Schutz von Daten ist wichtig. Das ist dann das Thema Datensicherheit mit allen dazu notwendigen technisch-organisatorischen Maßnahmen. Aber das ist eigentlich eine andere Geschichte. Worum es bei Datenschutz-Gesetzen[1] wirklich geht, ist etwas anderes: Es geht um den Schutz von Menschen und deren Grundrechten! Die Idee, dass ich selbst entscheiden darf, wer welche Daten bzw. Informationen von mir hat und wer was damit machen darf, ist noch gar nicht so alt. Diese sogenannte informationelle Selbstbestimmung geht zurück auf die 80er Jahre des letzten Jahrhunderts. Damals sollte es eine vollständige Erhebung umfassender persönlicher Daten aller Bewohnerinnen und Bewohner der alten Bundesrepublik geben – womit der bzw. die Einzelne für den Staat, Kommunen und Gemeinden quasi gläsern geworden wäre. Massive zivile Gegenwehr und ein Rechtsstreit führten dazu, dass diese Vollerfassung untersagt wurde; seitdem gibt es den Abgleich zwischen behördlich gespeicherten Daten und tatsächlicher Bevölkerung nur noch als Stichproben (Mikrozensus).

Angesichts einer immer umfassenderen Digitalisierung, die alle Lebensbereiche erfasst, hat sich die Diskussion um Datenschutz mittlerweile deutlich verlagert: Statt Bürger/-innen gegenüber einem potenziell übergriffigen Staat zu schützen, geht es heute vor allem darum, Nutzer/-innen von Apps, Diensten und Plattformen vor Tracking, Profiling und anderen fragwürdigen Big-Data-Nutzungen durch die international tätigen Anbieter zu bewahren und sie in der Durchsetzung ihrer informationellen Selbstbestimmung zu unterstützen. Sinn und Zweck des Datenschutzes ist es also, Menschen und deren informationelle Selbstbestimmung zu schützen und nicht „Daten“ an sich!

[1] Das Thema ist aktuell aufgrund der EU-Datenschutzgrundverordnung (EU-DSGVO bzw. noch kürzer DSGVO), des daraufhin novellierten Bundesdatenschutzgesetzes (BDSG) sowie der kirchlichen Regelungen zum Datenschutz im katholischen Kirchlichen Datenschutzgesetzt (KDG) und dem Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD).

Diese positive Motivation hat unter anderem zur Erarbeitung der EU-DSGVO geführt, die seit 2016 in Kraft und seit 25. Mai 2018 für alle EU-Staaten verbindlich ist. Das heißt, dass bis zu spätestens diesem Zeitpunkt nationale Regelungen überprüft und ebenso wie davon abgeleitete Gesetze angepasst werden mussten. Dabei sind leider einige rechtliche Gestaltungsmöglichkeiten („Öffnungsklauseln“) nicht genutzt worden, so dass an mancher Stelle der Eindruck entsteht, dass für den Alltag nicht sonderlich passende Regelungen gefunden wurden. Außerdem gibt es häufig Abwägungen zwischen unterschiedlichen Rechtsprinzipien, z. B. verschiedenen „Rechtfertigungsgründen“ für Datenspeicherung, die in der Praxis dann zu vorübergehenden oder andauernden Unsicherheiten führen. Vieles ist derzeit unklar und muss ggf. gerichtlich geklärt werden.

Die vorliegende Broschüre will daher für den Bereich der kirchlichen Jugendarbeit und Jugendpastoral zentrale Fragen aufgreifen und zu einer praxisorientierten Klärung beitragen. Im Zweifelsfall gilt: Keep calm and comply with GDPR – keine Panik, bitte! Dabei wollen wir nicht nur fragen, was jeweils alles verboten ist, sondern auch nach den positiven Gestaltungsmöglichkeiten schauen. Eine besondere Chance liegt dabei darin, dass das KDG, das Datenschutzgesetz der Katholischen Kirche, binnen drei Jahren überprüft und ggf. überarbeitet werden soll.

Bis dahin klären wir auf, was personenbezogene Daten eigentlich sind, was Datenvermeidung und Datensparsamkeit bedeuten, welche weiteren Prinzipien dem Datenschutz noch zugrunde liegen, und was wir alle von einem funktionierenden Datenschutz haben – auch in Jugendarbeit und Jugendpastoral.

Prof. Andreas Büsch, Leiter der Clearingstelle Medienkompetenz der Deutschen Bischfskonferenz an der KH Mainz

EINFÜHRUNG

„Das Datenschutzrecht verlangt nichts Unvernünftiges. Wenn es nicht vernünftig ist, dann ist es kein Datenschutz“, schrieb der baden-württembergische Landesdatenschutzbeauftragte Stefan Brink vor kurzem auf Twitter. Zugegeben: Tatsächlich ist es dann doch etwas komplizierter, mit vielen Paragraphen, einigen Zweifelsfällen und sehr wenigen klaren Ansagen von Gerichten. Ganz verkehrt lag der Datenschützer damit aber nicht: Das Datenschutzrecht, sowohl das europäische wie das kirchliche, baut auf einigen nachvollziehbaren Grundsätzen auf, deren Verständnis sehr dabei hilft, eine gute Handhabe für den eigenen Umgang mit personenbezogenen Daten zu finden.

Der oberste Grundsatz dabei: Datenschutz ist keine bürokratische Selbstbespiegelung, sondern schützt Grundrechte – er schützt die Privatsphäre und das Recht auf informationelle Selbstbestimmung. Das bedeutet: Man selbst darf entscheiden, welche Informationen über einen selbst wie verwendet werden; andere dürfen nicht einfach mit meinen Daten machen, was sie wollen. Will ich, dass ich mit meinem echten Namen in Suchmaschinen auftauche? Wen geht meine Handynummer etwas an? Sollen Kinderbilder in sozialen Netzen gepostet werden? Das alles sind Fragen, auf die es keine allgemeingültige Antwort gibt: Jede und jeder muss sie für sich selbst beantworten. Das Datenschutzrecht schafft den gesetzlichen Rahmen, dass das auch wirklich möglich ist – und deshalb wirkt es oft sehr streng: Um auch tatsächlich sicherzustellen, dass Menschen ihr Grundrecht auf informationelle Selbstbestimmung nicht von anderen aus der Hand genommen wird, die darauf keine Rücksicht nehmen.

Um diesen Grundrechtsschutz umzusetzen, haben die Gesetzgeber des KDG sowie der europäische Gesetzgeber bei der DSGVO ein sehr starkes Instrument gewählt: Das Verbot mit Erlaubnisvorbehalt. Zunächst ist jede Verarbeitung von personenbezogenen Daten verboten – außer, es gibt dafür eine rechtliche Grundlage. Die bekannteste davon ist die Einwilligung, also die Bestätigung der betroffenen Person: Ja, Du darfst meine Daten für diese bestimmten Zwecke verwenden.

Wenn die erste Prüfung ergeben hat, dass eine Verarbeitung zulässig ist, kommt der nächste Schritt. Die Verarbeitung ist weiteren Kriterien unterworfen, die das KDG benennt. Die Formulierungen in dem „Grundsätze für die Verarbeitung personenbezogener Daten“ überschriebenen Paragraphen 7 des KDG klingen zunächst sehr abstrakt. Doch die sechs dort niedergelegten allgemeinen Grundsätze sind, wenn man darüber nachdenkt, sehr naheliegend und

einsichtig. Am Beispiel der Verarbeitung von Daten bei einem Sommerlager wird schnell klar, dass diese Kriterien in der Praxis zum größten Teil Selbstverständliches abdecken:

§ 7 (1) KDG Personenbezogene Daten müssen	Für das Sommerlager bedeutet das
▶ a) auf rechtmäßige und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden; [Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz]	▶ Wer Daten erhebt, ist an die geltenden Gesetze gebunden, und die betroffenen Personen haben ein Anrecht darauf zu wissen, dass und wie die rechtlichen Spielregeln eingehalten werden. Schon bei der Gestaltung der Anmeldung muss ich überlegen und transparent machen, wofür ich Daten benötige und wissen, wie und wo ich die verarbeite – und jederzeit in der Lage sein, das auch den Menschen zu erklären, die das Formular ausfüllen.
▶ b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; [Zweckbindung]	▶ Wer eine Sommerlageranmeldung unterschreibt, der will über die angegebene E-Mail-Adresse die Einladung zum Elternabend bekommen, über die angegebene Handy-Nummer angerufen werden, wenn das Kind sich das Knie geprellt hat, und sicherstellen, dass die Lagerküche weiß, wer keine Erdnüsse essen darf. Die Mail-Adresse aber ungefragt in allgemeine Verteiler eintragen, die Telefonnummer an die Pfarrei weitergeben, damit sie fürs Fundraising für die neue Orgel verwendet werden kann: Das geht nicht. Die Einwilligung, Fotos den anderen Teilnehmenden zur Verfügung zu stellen, beinhaltet nicht automatisch, dieses Foto für die Werbung fürs Lager im nächsten Jahr verwenden zu dürfen.


Phone
Mail
Safari
Music
Calculator
Settings
Newsstand
iTunes Store
App Store
Passbook
Notes
Reminders
Stocks
Game Center

▶ c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein; insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und der Aufwand nicht außer Verhältnis zum angestrebten Schutzzweck steht; [Datenminimierung]	▶ Kontaktadressen, Bankverbindung, Allergien: Das braucht man fürs Lager. Beruf der Eltern? Die Krankengeschichte von der Geburt an? Mitgliedschaften in anderen Vereinen? Dafür gibt's keinen Grund, das in der Anmeldung abzufragen. Statistiken sind nützlich, um damit das eigene Angebot zu prüfen – aber statt einer Geburtstagsliste mit Name und genauem Alter tut es auch die anonyme Strichliste, um festzustellen, dass man ein Problem hat, 13–15-Jährige Teilnehmende zu gewinnen.
▶ d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden; [Richtigkeit]	▶ Wenn die Daten vom Anmeldeformular in die Liste für die Lagerleitung wandern, dann müssen die auch stimmen – und wenn ich oder die betroffene Person feststellen, dass dabei etwas durcheinandergekommen ist, dann wird die falsche Allergie, die veraltete E-Mail-Adresse gelöscht oder korrigiert.
▶ e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; [Speicherbegrenzung]	▶ Probleme machen vor allem Daten, die man hat: Es ist sinnvoll, die Unterlagen vergangener Sommerlager aufs Nötige zu reduzieren. Sobald das Sommerlager vorbei ist, brauche ich sensible Informationen zum Beispiel zur Gesundheit nicht mehr. Also: Weg damit! Für die Zuschüsse vom Landesjugendplan muss ich aber vielleicht doch Teilnehmendenlisten eine Weile aufbewahren – aber wirklich nur mit den Informationen, die dort benötigt werden, und nur so lange, wie die Zuschussordnung es vorschreibt.

- f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

  [Integrität und Vertraulichkeit]

- Nicht alle Beteiligten müssen Zugriff auf alle Daten haben – nicht, weil man sich nicht vertraut, sondern weil das die Punkte reduziert, an denen Fehler gemacht werden können: Das Küchenteam braucht keine Bankverbindungen der Teilnehmenden, die Kassenwartin keine Informationen über Allergien. Der Ordner mit den Anmeldungen, in dem Gesundheitsdaten und Bankverbindungen, Adressen und Kontaktpersonen stehen, gehört nicht offen ins Regal im Gruppenraum; mindestens ein abgeschlossener Schrank sollte es schon sein. Und so praktisch der Cloud-Speicher auch ist: Auch da muss sichergestellt werden, dass nicht alle Zugriff haben und der gewählte Dienst den rechtlichen Anforderungen genügt.

Für die eigene Arbeit ist schon viel gewonnen, wenn man diese Grundsätze im Hinterkopf behält. Immer, wenn personenbezogene Daten erhoben und verarbeitet werden – und das ist vom Ministrant/-innen-Plan über die Mitgliederverwaltung bis hin zur Gestaltung von Webseite und Social-Media-Auftritten ziemlich viel –, lohnt es sich, im Kopf ein paar an diesen Prinzipien orientierte Kontrollfragen durchzuspielen: Brauche ich diese Daten wirklich an dieser Stelle – oder erreiche ich mein Ziel auch ohne sie? Wie lange muss ich diese Daten aufbewahren, und welche rechtliche Grundlage habe ich dafür? Wie stelle ich sicher, dass ich dann die Daten wieder lösche? Weiß ich, was und wo ich überhaupt Daten aufbewahre – und kann ich jederzeit Betroffenen und mir selbst Rechenschaft darüber ablegen? Habe ich die Daten angemessen gegen Verlust, Diebstahl oder auch bloße Schusseligkeit gesichert?

Wer auf alle diese Fragen Antworten geben kann, hat leider noch nicht alle Pflichten des Gesetzes erfüllt – aber eine hervorragende Grundlage, um auf der Basis der weiteren Informationen in dieser Arbeitshilfe datenschutzkonform zu arbeiten, die Datenschutzgesetze und ihre praktischen Konsequenzen nachzuvollziehen und damit die informationelle Selbstbestimmung der Mitglieder und Teilnehmenden zu schützen.

Felix Neumann, Redakteur bei katholisch.de

Grundsatzfragen und Definitionen

Wo finde ich das Gesetz über den Kirchlichen Datenschutz (KDG)?
Das von den Diözesanbischöfen für ihre jeweilige (Erz-)Diözese erlassene KDG ist in den entsprechenden Amtsblättern der (Erz-)Diözesen veröffentlicht. Es findet sich sowohl auf den Webseiten der (Erz-)Diözesen als auch auf den Webseiten der jeweils zuständigen Diözesandatenschutzbeauftragten (Datenschutzzentren). Links zu den (Erz-)Diözesen und den insgesamt fünf Katholischen Datenschutzzentren finden sich auf der Homepage der Deutschen Bischofskonferenz unter:

www.dbk.de/katholische-kirche/bistumskarte
www.dbk.de/ueber-uns/verband-der-dioezesen-deutschlands-vdd/dokumente

Auch wenn jeder Bischof ein eigenes KDG für seine Diözese in Kraft gesetzt hat, sind die Gesetze nahezu gleichlautend.

Für wen gilt das KDG? Und welches KDG gilt?
Das KDG gilt für kirchliche Stellen im Bereich der katholischen Kirche. Dazu gehören nicht nur Diözesen, Kirchengemeinden und Kirchengemeindeverbände etc., sondern auch sonstige kirchliche Rechtsträger, also beispielsweise ein Verband (vgl. § 3 KDG). Die sogenannten „Orden päpstlichen Rechts" haben ein eigenes Datenschutzgesetz, die „Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts" (falls Zweifel bestehen, ob der jeweilige Orden darunter fällt: Einfach den oder die zuständige/-n Obere/-n fragen).

Das jeweilige kirchliche Datenschutzgesetz wird dabei von jedem einzelnen Diözesanbischof erlassen, das Gesetz für die päpstlichen Ordensgemeinschaften von den Ordensgemeinschaften selbst. Damit gibt es formal viele verschiedene KDGs; diese unterscheiden sich aber in ihren Regelungen in der Regel nicht und entsprechen auch weitgehend den staatlichen Regeln der DSGVO.

Die Bundesstelle eines Verbands unterfällt in der Regel dem KDG des Bischofs, in dessen Diözese der Verband seinen Sitz hat. Für die Diözesanstellen des Verbands gilt in der Regel das KDG des jeweiligen Diözesanbischofs. Die verbandlichen Gruppen vor Ort unterfallen, auch wenn sie kein eigenständiger Verein sind, in der Regel dem KDG des Bischofs, in dessen Diözese sie gelegen sind. Es kann also sein, dass für die Bundesstelle das KDG eines Bischofs und für die Diözesanstelle das KDG eines anderen Bischofs gilt. Aber keine Sorge: Die KDGs, die die Bischöfe für ihre Diözesen in Kraft gesetzt haben, sind wie gesagt nahezu gleichlautend, so dass dies kein Problem sein sollte.

Die nichtverbandliche Pfarrjugend, z. B. Ministrant/-innengruppen, sind, was die Geltung des KDG anbelangt, der Kirchengemeinde zuzuordnen, in der sie aktiv sind. Für sie gilt also das KDG, das auch für die Kirchengemeinde gilt. Vergleichbares kann auch für verbandliche Ortsgruppen gelten.

Manchmal, z. B. bei Fördervereinen, kann es sein, dass eine Einrichtung nicht unter kirchliches Recht fällt. Die Kirchlichkeit einer Einrichtung bestimmt sich anhand einer Zusammenschau verschiedener Kriterien. Die Kriterien sind in der Datenschutz-FAQ der Bischofskonferenz – Link siehe unten, S. 19 – genannt. Bei Fördervereinen liegt der Zweck häufig ausschließlich in der materiellen oder immateriellen Förderung einer anderen Einrichtung, so dass keine Kirchlichkeit im rechtlichen Sinne vorliegt. Wird die Kirchlichkeit einer Einrichtung verneint, gilt für sie staatliches Datenschutzrecht (also die EU-Datenschutzgrundverordnung, das Bundesdatenschutzgesetz sowie das entsprechende Landesdatenschutzgesetz). Aber kirchliches und staatliches Datenschutzrecht sind sich inhaltlich im Wesentlichen ähnlich, lediglich andere Datenschutzaufsichten sind zuständig.

Besteht Unsicherheit darüber, ob eine Einrichtung kirchlich ist oder welches Datenschutzrecht gilt, sollte dies zeitnah mit der örtlich zuständigen Diözese oder dem örtlich zuständigen Katholischen Datenschutzzentrum (siehe unten) geklärt werden.

Was ist, wenn das KDG nicht gilt?
Fällt eine Einrichtung nicht unter den Anwendungsbereich des KDG, gelten die EU-Datenschutzgrundverordnung (EU-DSGVO), das Bundesdatenschutzgesetz sowie das entsprechende Landesdatenschutzgesetz. Im evangelischen Bereich gilt das Datenschutzgesetz der EKD (DSG-EKD). Bei ökumenischen Trägerschaften ist im Dialog mit den Datenschutzaufsichten zu klären, ob das katholische oder das evangelische Datenschutzgesetz angewendet wird. Ganz wichtig: Einen datenschutzrechtlich freien Raum kann es nicht geben!

Was ist ein personenbezogenes Datum?
Unter personenbezogenen Daten versteht man sämtliche Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person (Mann, Frau, Kind, Jugendlicher) beziehen. Bestimmbar ist eine Person dann, wenn man sie, ohne dass man ihren Namen kennt, aufgrund bestimmter sonstiger Hinweise, zum Beispiel anhand des Geburtsdatums und des Wohnorts, eindeutig identifizieren kann. Personenbezogene Daten sind zum Beispiel Name, Adresse, Geburtsdatum, Nationalität, Religionszugehörigkeit, Größe, Augenfarbe, Kleidergröße, bestehende Allergien. Auch das Foto einer Person ist ein personenbezogenes Datum.

Die Person, um deren personenbezogene Daten es geht, nennt man „betroffene Person". Nur Daten, die natürliche Personen, also Menschen, betreffen, sind in diesem Sinn personenbezogen. Daten über juristische Personen (z. B. über einen eingetragenen Vereine oder eine GmbH) wie das Gründungsdatum oder das Vermögen eines Vereins sind keine personenbezogenen Daten und fallen daher nicht unter den Schutz des KDGs. Das KDG gilt ausschließlich für die Verarbeitung personenbezogener Daten.

Was versteht man unter besonderen Kategorien personenbezogener Daten?
Besondere Kategorien personenbezogener Daten sind Daten, die, weil es sensible Daten sind, eines speziellen Schutzes bedürfen. Es handelt sich zum Beispiel um Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen, außerdem um genetische Daten (z. B. DNA-Analysen) und biometrische Daten (z. B. Fingerabdrücke, Stimmen- oder Iriserkennungen), Gesundheitsdaten (z. B. Einnahme von Medikamenten) oder Daten zum Sexualleben oder zur sexuellen Orientierung. Die reine Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft ist nach dem KDG keine besondere Kategorie personenbezogener Daten.

Fotos könnten rein theoretisch auch unter den Begriff der biometrischen Daten fallen. Jedoch werden sie nur dann von der Definition des Begriffs „biometrische Daten" erfasst, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer Person ermöglichen (z. B. Abgleich eines Fotos mit einer Gesichtserkennungssoftware).

§ 11 Abs. 1 KDG regelt, dass die Verarbeitung dieser Daten grundsätzlich untersagt ist, es sei denn, eine speziell in § 11 Absatz 2 KDG genannte Ausnahme greift, z. B. die ausdrückliche Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten.

Was versteht man unter Datenverarbeitung?
Der Begriff „Datenverarbeitung" ist sehr weitgehend. Er umfasst alles, was man mit Daten machen kann. Darunter fallen zum Beispiel das Erheben, das Erfassen, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Abfragen, die Verwendung, jede Art der Datenweitergabe (also Übermittlung, Verbreitung oder eine andere Form der Bereitstellung von Daten), aber auch das Löschen und die Vernichtung von Daten.

Wer ist „Verantwortlicher" im datenschutzrechtlichen Sinne?
Verantwortlicher ist nach dem Gesetz „die natürliche oder juristische Person,

Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

Ausschlaggebend ist also, welche Einzelperson oder welches mit mehreren Personen besetzte Kollegialorgan die konkrete Entscheidung über den Umgang mit den personenbezogenen Daten trifft. Das kann die (oberste) Leitung sein, bei einem Verein also je nachdem der Vereinsvorstand in seiner Gesamtheit oder der Vereinsvorsitzende, aber auch die für bestimmte Bereiche zuständige Person bzw. Personenmehrheit. Entscheidend ist, wem vereinsintern in der Praxis die Letztverantwortlichkeit zukommt.

Die Verantwortlichkeit ist also unterschiedlich je nachdem, ob personenbezogene Daten auf Bundesebene, auf Diözesanebene oder auf Ortsebene verarbeitet werden. Sie kann darüber hinaus innerhalb einer Ebene je nach Aufgabenteilung differieren. So kann z. B. innerhalb einer Ortsgruppe der/die Hauptverantwortliche für eine Ferienfreizeit „Verantwortliche/-r“ sein. Denkbar ist auch, dass eine verbandliche Ortsgruppe im Auftrag der Kirchengemeinde tätig ist. In einem solchen Fall könnte(n) Verantwortliche/r im datenschutzrechtlichen Sinne auch der Pfarrer der Kirchengemeinde und/oder deren Kirchenvorstand sein.

Im Rahmen der nichtverbandlichen Jugendarbeit innerhalb einer Kirchengemeinde ist grundsätzlich der Pfarrer und/oder der Kirchenvorstand „Verantwortliche/-r“. Überträgt er jedoch die Ministrant/-innenarbeit eigenverantwortlich einer anderen Person, die dann eigenständig über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, so ist diese „Verantwortliche/-r“ im Sinne des KDG.

Was ist ein/-e Auftragsverarbeiter/-in?
„Auftragsverarbeiter/-in“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Werden z. B. die Adressdaten der Vereinsmitglieder an eine andere Einrichtung, z. B. einen Verlag oder eine Behindertenwerkstatt, weitergeleitet mit dem Auftrag, die Mitgliederzeitschrift an die Vereinsmitglieder zu versenden, oder erfolgt die Prüfung oder Wartung von Datenverarbeitungsanlagen durch einen Externen, handelt es sich um eine Auftragsverarbeitung, vgl. § 29 KDG.

Keine Auftragsverarbeitung liegt beispielsweise dann vor, wenn die Ortsgruppe für eine bestimmte Veranstaltung von ihren Mitgliedern Zuschusslisten aus-

füllen lässt und diese Listen an den Diözesanverband weitergeleitet werden, der dann entsprechende Zuschüsse zahlt. Hier handelt es sich um eine Offenlegung personenbezogener Daten nach § 9 KDG. Auch bei der Weiterleitung personenbezogener Daten von Kommunionkindern durch die Kirchengemeinde an die verbandliche Ortsgruppe, die die jährliche Sternsingeraktion durchführt, handelt es sich nicht um eine Auftragsverarbeitung, sondern um eine „Offenlegung" in o.g. Sinn.

Wann ist eine Datenverarbeitung rechtmäßig?
Es gibt sieben Voraussetzungen, unter denen eine Datenverarbeitung rechtmäßig ist:

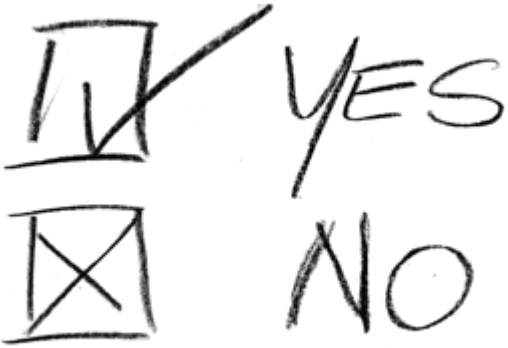
- Ein Gesetz oder eine andere Rechtsvorschrift (egal ob kirchlich oder staatlich) erlaubt die Datenverarbeitung oder ordnet sie sogar an. Hier sind beispielhaft das KDG selbst oder die seitens des Bischofs erlassene Präventionsordnung zu nennen.
- Es liegt eine Einwilligung der betroffenen Person (bei Kindern und Jugendlichen des/der Personensorgeberechtigten) vor. Genaueres zur Einwilligung siehe unten.
- Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich. Unter diesen Rechtfertigungsgrund fällt z. B. die Verarbeitung von Mitgliederdaten bei einem Verein. Dazu gehört beispielsweise der Versand der Mitgliederzeitschrift oder der Einladung zur Weihnachtsfeier an die Vereinsmitglieder.
- Die Verarbeitung ist zur Erfüllung einer rechtlichen (gesetzlichen, nicht vertraglichen) Verpflichtung erforderlich, der der Verantwortliche unterliegt. Hierzu zählen z. B. bestimmte gesetzliche Dokumentations- und Aufbewahrungspflichten im Handels- und Steuerrecht.
- Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. Gedacht ist hier beispielsweise an die Bewältigung von Epidemien oder Natur- und ähnlichen Katastrophen sowie an die Abwehr von Seuchengefahren oder von Tötungs- und Körperverletzungsdelikten im Wege vorbeugender Datenverarbeitung. Für besondere Kategorien personenbezogener Daten, z. B. Gesundheitsdaten, ist hier eine Ausnahme vorgesehen: Zum Schutz lebenswichtiger Interessen dürfen diese Daten nur verarbeitet werden, wenn die betroffene Person aus körperlichen Gründen (z. B. Bewusstlosigkeit) oder rechtlichen Gründen (Kinder unter 16 Jahren) außerstande ist, ihre Einwilligung zu geben, vgl. § 11 Abs. 2 lit. c) KDG.

- Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im kirchlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Hier reicht es nicht aus, dass irgendein kirchliches Interesse besteht. Es muss sich um eine Aufgabe handeln, die dem Verantwortlichen tatsächlich übertragen wurde und die durch eine Rechtsvorschrift (z. B. das kirchliche Recht im Codex Iuris Canonici) definiert ist. Diese Voraussetzung wird bei Jugendverbänden wohl eher nicht greifen.

- Die Verarbeitung ist zur Wahrung der berechtigten Interessen der/des Verantwortlichen oder einer/eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um eine/-n Minderjährige/-n handelt.

Wie muss eine Einwilligung erfolgen?
In vielen Fällen ist eine Einwilligung (vgl. § 8 KDG) erforderlich, damit personenbezogene Daten rechtmäßig verarbeitet werden können. Die Einwilligung muss durch die betroffene Person selbst oder ihren gesetzlichen Vertreter erfolgen. Bei Minderjährigen sind dies in der Regel beide Elternteile. Insbesondere dann, wenn die Eltern eines Kindes zwar getrennt leben, aber beide noch die Personensorge für das gemeinsame Kind haben, kann es von großer Wichtigkeit sein, die Einwilligung beider Elternteile bzw. aller sorgeberechtigter Personen einzuholen! Ausnahmsweise, nämlich dann, wenn die Personensorge zum Beispiel nach einer Scheidung nur einem Elternteil zugesprochen ist, reicht die Einwilligung des personensorgeberechtigten Elternteils aus.

Die Einwilligung kann nur wirksam erfolgen, wenn die betroffene Person bzw. deren Vertreter/-in ausreichend informiert ist, also genau weiß, in was sie einwilligt. Eine Einwilligung muss freiwillig und für einen bestimmten Fall (also z. B. mit Blick auf die Veröffentlichung eines bestimmten Fotos) abgegeben werden.



Sie muss in der Regel schriftlich erfolgen, also z. B. durch ausdrückliche Erklärung oder Ankreuzen. Nicht zulässig ist eine sog. konkludente Einwilligung, bei der aus dem Fehlen einer Reaktion auf eine Einwilligung geschlossen wird.

Auf die Schriftform einer Einwilligung kann verzichtet werden, wenn wegen besonderer Umstände eine andere Form angemessen ist. Dies kann zum Beispiel bei Filmaufnahmen während einer Großveranstaltung der Fall sein. Hier könnte man Hinweisschilder aufstellen, die darauf aufmerksam machen, dass in einem bestimmten Bereich gefilmt wird, in einem anderen Bereich nicht. Dann kann jede/-r frei entscheiden, wohin er oder sie geht; durch das Betreten des Filmbereichs gibt man zu erkennen, dass man in die Datenverarbeitung einwilligt.

Welche Informationspflichten bestehen?
Die Informationspflichten des Verantwortlichen sind ausführlich in den §§ 14 bis 16 KDG geregelt. Die Informationspflichten haben unterschiedlichen Umfang je nachdem, ob die Daten unmittelbar bei der betroffenen Person (§ 15 KDG) oder über Dritte bzw. aus anderen Quellen (§ 16 KDG) erhoben werden. Gegebenenfalls empfiehlt es sich, Informationsblätter für die betroffenen Personen bereit zu halten.

Werden Daten direkt bei der betroffenen Person erhoben, ist diese nach § 15 KDG unter anderem über den Namen und die Kontaktdaten des Verantwortlichen, den Zweck, für den die Daten verarbeitet werden sollen einschließlich der Rechtsgrundlage für die Verarbeitung (s.o.: Wann ist eine Datenverarbeitung rechtmäßig? s. auch § 6 KDG) sowie darüber zu informieren, an wen die Daten weitergegeben werden. Unter anderem ist auch zu informieren über die Dauer der Datenspeicherung, die Rechte des Betroffenen gegenüber dem Verantwortlichen (u. a. Auskunfts-, Berichtigungs-, Löschungs- und Widerspruchsrecht), das Bestehen eines Beschwerderechts gegenüber der Datenschutzaufsicht. Werden Daten zu einem anderen Zweck als zu dem, zu dem sie erhoben worden sind, verarbeitet, ist auch diesbezüglich zu informieren. Ausnahmen von der Informationspflicht regeln § 15 Absätze 4 und 5. Eine Ausnahme ist insbesondere dann gegeben, wenn die Informationserteilung an die betroffene Person einen unverhältnismäßigen Aufwand erfordern würde und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls als gering anzusehen ist.

Werden Daten mittelbar, das heißt, über eine dritte Person oder aus anderen Quellen erhoben, sind noch weitergehende Informationen erforderlich, u. a. um welche Daten es sich handelt und woher diese Daten stammen (s. § 16 KDG). Auch hier gibt es Ausnahmen (Absätze 4 und 5). So erübrigt sich eine In-

formation beispielsweise dann, wenn die betroffene Person bereits über die Informationen verfügt oder die Erteilung der Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

Welche Rechte haben betroffene Personen?
Betroffene Personen haben gegenüber dem Verantwortlichen zahlreiche Rechte, unter anderem

- das Recht auf Auskunft darüber, ob sie betreffende personenbezogene Daten verarbeitet werden, und, sollte dies der Fall sein, auf weitere in § 17 KDG im Einzelnen genau benannte Informationen,
- das Recht auf Berichtigung, wenn personenbezogene Daten unrichtig sind (§ 18 KDG),
- unter bestimmten, in § 19 KDG im Einzelnen aufgeführten Voraussetzungen das Recht auf Löschung ihrer Daten,
- das in § 23 KDG geregelte Recht auf Einlegung eines Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten.

Diese Rechte bestehen allerdings nicht uneingeschränkt, sondern nur unter in der jeweiligen Norm näher bestimmten Voraussetzungen. Näheres findet sich unter §§ 17 bis 25 KDG.

Welche Pflichten hat der/die Verantwortliche?
Neben den Informationspflichten hat der/die Verantwortliche weitere Pflichten. Sie finden sich unter den §§ 31 bis 35 KDG.

- So ist beispielsweise unter bestimmten Voraussetzungen ein Verzeichnis von Verarbeitungstätigkeiten zu führen (s. § 31 KDG), welches die konkreten Verarbeitungsprozesse einschließlich Verarbeitungsablauf, Verarbeitungszweck, Kreis der Betroffenen, Hard- und Software etc. beschreibt.
- Des Weiteren sind Verletzungen des Schutzes personenbezogener Daten binnen 72 Stunden (!) der zuständigen Datenschutzaufsicht zu melden (§ 33 KDG) und sind betroffene Personen über diese Verletzung zu informieren (§ 34 KDG).
- Bringt eine bestimmte Form der Verarbeitung (insbesondere bei Verwendung neuer Technologien) ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich, so ist nach Maßgabe des § 35 KDG eine Datenschutz-Folgenabschätzung vorzunehmen.

An welches Datenschutzzentrum kann ich mich wenden?
Welches Datenschutzzentrum zuständig ist, richtet sich nach dem Sitz der kirchlichen Einrichtung. Es gibt insgesamt fünf Katholische Datenschutzzentren:

- Katholisches Datenschutzzentrum Frankfurt/Main für das Erzbistum Freiburg und die Bistümer Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier,
- Katholisches Datenschutzzentrum KdöR für die nordrhein-westfälischen (Erz-)Diözesen,
- Der Diözesandatenschutzbeauftragte der (Erz-)Bistümer Hamburg, Hildesheim, Osnabrück und des Bischöflich Münsterschen Offizialats in Vechta i.O.,
- der Diözesandatenschutzbeauftragte für die bayerischen (Erz-)Diözesen, Diözesandatenschutzbeauftragter der ostdeutschen Bistümer.

Links zu den Katholischen Datenschutzzentren finden sich auf der Homepage der Deutschen Bischofskonferenz unter www.dbk.de/ueber-uns/verband-der-dioezesen-deutschlands-vdd/dokumente/

Wo finde ich weiterführende Informationen?
Die Datenschutzzentren halten auf ihren Homepages (Links unter www.dbk.de/ueber-uns/verband-der-dioezesen-deutschlands-vdd/dokumente/) hilfreiche Informationen in Form von Praxishilfen, Mustern etc. bereit. Zum Teil ist der Bezug eines Newsletters möglich.

Antworten auf häufig gestellte Fragen finden sich auf der Homepage der Deutschen Bischofskonferenz unter www.dbk.de/themen/kirche-staat-und-recht/datenschutz-faq/.

Martina Burke, juristische Referentin in der Rechtsabteilung des Verbandes der Diözesen Deutschlands (VDD) KöR, Bonn.

ARBEITSHILFEN

Entwurf zur Gruppenstunde zur Datensouveränität

Gruppenstunde Datensouveränität

Dauer: 1 Std. bis 1,5 Std.

TN-Alter: beliebig

TN-Zahl: 5-20 Personen

Material: Endlosrolle, Krepp-Band, Memory-Spiel

Vorbereitung: 15 min.

Thematischer Einstieg: Was sind denn Daten?

Zur Erstellung einer Mindmap werden die Teilnehmer/-innen eingeladen, sämtliche Begriffe auf ein ausreichend großes Stück Papier mit dem Satz in der Mitte zu schreiben

Einordnung: Was bedeutet welcher Begriff?

- Datenschutz
- Datennutzung
- Datenerhebung
- Datensparsamkeit
- Datenklau
- Datenpreisgabe
- Datenschutzgesetz
- Datenverwertung
- personenbezogene Daten
- Privatsphäre
- Geheimnis

- …

Je nach Rückfragen der Gruppe können die Begriffe gemeinsam besprochen werden.

Hinführung zu Datensouveränität

Auf dem Boden sind mit Krepp-Band die Ziffern 1, 5 und 10 angebracht. Die folgenden Fragen werden vorgelesen. Die Teilnehmenden können sich von 1 (stimme gar nicht zu) über 5 (unentschlossen) bis 10 (stimme voll zu) beliebig positionieren.

1. Nutzungsbedingungen lese ich immer durch.
2. Ich gebe bei Abfragen immer Geburtsdatum, Telefonnummer, Wohnort und Interessen an.
3. Ich schaue immer nach, welche Daten mein Handy sammelt.
4. Wenn etwas kostenfrei ist, gebe ich Apps für mein Handy auch nicht notwendige Zugriffsrechte auf Bilder, Telefonbuch und Social Media wie Instagram oder Facebook
5. Wenn Apps wie Instagram oder Snapchat Daten sammeln, mache ich mir keine Gedanken

6. Ich gehe immer sehr bewusst damit um, welche Daten ich angebe und welche Rechte ich einräume.

Die aufgestellten Personen sollen bei jeder Frage freiwillig erzählen können, weshalb sie sich entsprechend positioniert haben. So entsteht eine Gesprächsebene, die zum kritischen Denken und Problembewusstsein einlädt.

Je nach Fortschreiten der Zeit können Fragen ausgelassen werden oder Abfragen im Laufe der Methode verkürzt werden.

Bewusster Umgang mit persönlichen Daten = Datensouveränität

Eine beliebte App (z. B. Insta, Facebook, WhatsApp, Snapchat…) kostet nichts – aber es sind große Unternehmen dahinter, die sogar an der Börse notiert sind und entsprechend Gewinn erzielen wollen.

Der Gewinn muss durch eine Leistung des Unternehmens erbracht werden.

Daten können durchaus Preis gegeben werden.

Es muss ein Bewusstsein für die persönliche Sphäre im Hinterkopf bleiben. Welche Daten sind „höchstpersönlich", welche sind intim und welche kann ich problemlos mitteilen.

Auch die Daten „von anderen" müssen im Hinterkopf bleiben: Telefonnummern, Chats in Messenger-Diensten, Freunde auf Facebook….

Datensouveränität ist etwas anderes als Datensparsamkeit. Es geht um einen vernünftigen und durchdachten Umgang mit den Daten.

Der BDKJ setzt sich für eine vernünftige Balance zwischen Datenschutzgesetzen, Nutzung und Bewusstsein ein. Dafür geht er auf Akteur/-innen in Staat und Kirche zu.

Schluss: **Wie kann ich mit meinen Daten souverän(er) umgehen**?

Jede/-r nimmt für sich einen Vorsatz mit, den sie/er konkret umsetzt. Wer diesen mit der Gruppe teilen mag, ist herzlich eingeladen.

www.youngdata.de

www.klicksafe.de/materialien

www.datenschutz-berlin.de/fileadmin/user_upload/pdf/medienkompetenz/2018-BlnBDI-Broschuere_Soziale_Netzwerke.pdf

Thomas Andonie ist Vorsitzender des Bundes der Deutschen katholischen Jugend (BDKJ). Er wurde auf der Hauptversammlung 2017 in das Amt gewählt.

MUSTERVORLAGEN

KDG-Vorlage zur Einwilligung in die Veröffentlichung personenbezogener Daten und Fotos

Name und Anschrift des Trägers / Verbandes, ggf. Logo

Einwilligung in die Veröffentlichung personenbezogener Daten und Fotos

Liebe*r Freiwillige*r/Teilnehmende*r/....,
wir möchten Foto-, Video- und Tonaufnahmen für Werbung für die Freiwilligendienste/.... auf unserer Homepage, bei Facebook, in Zeitungen und Zeitschriften sowie bei Werbeveranstaltungen in Schulen, auf Messen etc. nutzen. Hierzu möchten wir auch von Ihnen Fotos, Videos und Tonaufnahmen verwenden. Damit uns dies rechtlich möglich ist, benötigen wir Ihre Einwilligung, die wir im Folgenden einholen möchten.

.....
Name, Vorname [Druckbuchstaben]

Ich willige in die Veröffentlichung von personenbezogenen Daten einschließlich Fotos, Videos und Tonaufnahmen der oben genannten Person in folgenden Medien ein:

„**analoge Medien**“, bspw. Flyer, Zeitungen, Zeitschriften von *Träger/Verband*

☐ Ja ☐ Nein

„**digitale Medien**“, bspw. Webseiten, Facebook, Präsentationen von *Träger/Verband*

☐ Ja ☐ Nein

Bei der Veröffentlichung im **Internet** können die personenbezogenen Daten (einschließlich Fotos) weltweit abgerufen und gespeichert werden. Darauf, wer die Daten abruft oder zu welchem Zweck der Abruf erfolgt hat *Träger/Verband* keinen Einfluss.
Zum Teil können die Daten auch über Suchmaschinen aufgefunden werden. Dabei kann nicht ausgeschlossen werden, dass andere Personen oder Unternehmen die Daten mit weiteren im Internet verfügbaren personenbezogenen Daten verknüpfen und damit ein Persönlichkeitsprofil erstellen, die Daten verändern oder zu anderen Zwecken nutzen. Im Internet veröffentlichte Daten können nicht/nur schwer wieder entfernt werden

☐ Ja ☐ Nein

Sofern Fotos veröffentlicht werden, erfolgt die Auswahl des jeweiligen Fotos, soweit möglich, in Abstimmung mit der abgebildeten Person. In jedem Fall werden die Fotos vor Veröffentlichung durch *Träger/Verband* inhaltlich geprüft (rechtswidrige Inhalte, kompromittierende Situationen).

Sonderregelung bei Minderjährigen

Entsprechend der Entschließung der Konferenz der Beauftragten für den Datenschutz zur Veröffentlichung von Fotos von Minderjährigen unter 16 Jahre, wird jedes Foto vor Veröffentlichung vorgelegt und eine Einwilligung für jedes vorgelegte Foto separat eingeholt.

Die Einwilligung muss mit dem jeweiligen Foto hinreichend verbunden sein. Das/Die zu veröffentlichende/n Foto/s wurden vorgelegt und

- ☐ sind mit dieser Erklärung verbunden (bspw. angeheftet oder angeklebt).
- ☐ sind eindeutig benannt (Bezeichnung des digitalen Fotos auf dem Speicherträger).

Die Rechteeinräumung an den Fotos erfolgt ohne Vergütung und umfasst auch das Recht zur Bearbeitung, soweit die Bearbeitung nicht entstellend ist.

Die Einwilligung ist jederzeit schriftlich für die Zukunft bei *Träger/Verband* widerruflich.

Bei Druckwerken ist die Einwilligung nicht mehr widerruflich, wenn der Druckauftrag erteilt ist.

Wird die Einwilligung nicht widerrufen, gilt sie zeitlich unbeschränkt.

Die Einwilligung ist freiwillig. Aus der Nichterteilung oder dem Widerruf der Einwilligung entstehen keine Nachteile.

…… ……

Ort, Datum Unterschrift der abgebildeten Person ab Vollendung des 14. Lebensjahres

……

Zusätzlich Unterschrift aller Erziehungsberechtigten
bis Vollendung des 16. Lebensjahres der abgebildeten Person

Verzeichnis von Verarbeitungstätigkeiten

eines Verantwortlichen gemäß § 31 Abs.1 KDG

Erstellungsdatum: _____

Version: _____

A. Vorblatt (nur einmal auszufüllen, gilt für alle Verarbeitungen)

A.1 Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person / juristische Person / Behörde / Einrichtung

Name
Anschrift
Telefon, Email-Adresse

Sollten im Sinne des § 28 mehrere Verantwortliche gemeinsam für die Verarbeitung verantwortlich sein, sind alle gemeinsam Verantwortlichen zu benennen.

A.2 Angaben zum gesetzlichen Vertreter (Leitung) des Verantwortlichen

Name, Funktion
Anschrift
Telefon, Email-Adresse

A.3 Angaben zur Person des Datenschutzbeauftragten

Bei externen Datenschutzbeauftragten auch Angaben zum beauftragten Unternehmen

Name
Anschrift
Telefon, Email-Adresse

VzV 180620
KDSZ 2018

B. Beschreibung der Verarbeitung

(pro Verfahren auszufüllen)

Laufende Nr.	
Stand	
Version	

B.1 Bezeichnung

Bezeichnung der Verarbeitung
Ggf. Einführungszeitpunkt (wenn bekannt)

B.2 Fachliche Zuständigkeit

Fachabteilung, Ansprechpartner, Funktion
Kontaktdaten

B.3 Verarbeitungsablauf

Kurze Beschreibung der Verarbeitung (operativ) mit den wichtigsten Prozessschritten. Evtl. Verweis auf bestehende Dokumentation/Prozessbeschreibung o.ä. ☐ **Dokumentation ist als Anlage beigefügt**

B.4 Zwecke der Verarbeitung

Zweckbestimmung	
Rechtsgrundlage	
+ kirchliche oder staatliche Rechtsvorschrift	☐ Welche?
+ Erlaubnistatbestand des KDG	
- **Vertrag oder Vertragsanbahnung mit dem Betroffenen**	☐ Bitte näher bezeichnen
- **Erfüllung einer rechtlichen Verpflichtung des**	☐ Welche?

VzV 180620
KDSZ 2018

Verantwortlichen	
- **Schutz lebenswichtiger Interessen der betroffenen Person**	☐ Welche?
- **Wahrnehmung einer Aufgabe im kirchlichen Interesse**	☐ Welche?
- **Interessensabwägung**	☐ Bitte näher beschreiben ☐ **Dokumentation ist als Anlage beigefügt**
+ Einwilligung des Betroffenen	☐ In welcher Form? ☐ **Muster ist als Anlage beigefügt**

B.5 Kreis der Betroffenen

Kategorien betroffener Personen

z.B. Beschäftigte, Patienten, Angehörige, Interessenten, Kunden, Vertragspartner, Besucher, Lieferanten, Passanten

Sind Jugendliche oder Kinder betroffen? Wenn ja, welche Besonderheiten werden im Verfahren berücksichtigt?

Bitte erläutern!

Dient das Verfahren einem „Profiling" (d.h. einer automatisierten Bewertung persönlicher Aspekte, insbesondere um z.B. Arbeitsleistung, wirtschaftliche Lage, Gesundheit oder Bewegungsprofile zu analysieren und vorherzusagen)?

Bitte erläutern!

B.6 Datenkategorien, Datenherkunft und Löschfristen

Kategorien der verarbeiteten personenbezogenen Daten

Persönliche Daten:

- ☐ **Name/Vorname/Anrede/Titel**
- ☐ **Adresse**
- ☐ **Kontaktdaten (Tel. Fax, E-Mail)**
- ☐ **Geburtsdatum**
- ☐ **Fotos**
- ☐ **Interessen/Präferenzen**

Abrechnungsdaten:

- ☐ **Zahlungsdaten**
- ☐ **Bankverbindungsdaten/Kreditkartendaten**
- ☐ **Bonitätsdaten**

- ☐ **Gesundheitsdaten**

Personaldaten:

VzV 180620
KDSZ 2018

☐ **Lebenslauf**
☐ **Zeiterfassungsdaten**
☐ **Lohn-und Gehaltsdaten**
☐ **Qualifikationsdaten/Leistungs- und/oder Potenzialbeurteilung**
☐ **Sozialversicherungsdaten**

☐ **Vertragsdaten**

☐ **IT-Nutzungsdaten (Log Daten/Protokolldateien, IP-Adresse...)**
☐ **Standortdaten**

☐ **Sonstige:**

Besondere Kategorien personenbezogener Daten (siehe § 4 Abs. 2 KDG)

Werden besondere Kategorien personenbezogener Daten verarbeitet?
Wenn ja, welche?

☐ **Es werden keine Daten aus besonderen Kategorien personenbezogener Daten verarbeitet.**

☐ **Es werden Daten aus besonderen Kategorien personenbezogener Daten verarbeitet, und zwar:**

Definition und Zuordnung von Datenschutzklassen

Welchen Datenschutzklassen gemäß KDO-DVO werden die Datenkategorien (einschließlich der besonderen Kategorien) zugeordnet?

Datenherkunft nach §§ 15 und 16 KDG

Wie und durch wen werden die Daten unmittelbar oder mittelbar erhoben?

Fristen für die Löschung je Datenkategorie

Erfüllung der Informationspflichten nach § 15 bzw. 16 KDG

Wie werden die Informationspflichten gegenüber dem Betroffenen erfüllt?

☐ **Muster ist als Anlage beigefügt**

B.7 Auftragsverarbeitung

Kurzbeschreibung

Welche Verfahrensschritte werden durch einen Auftragnehmer bearbeitet?

☐ **Keine**

☐ **Die folgenden:**

Auftragnehmer (Name und Kontaktdaten) ☐ **Verzeichnis des Verfahrens nach § 31 Abs. 2 KDG (des Auftragsverarbeiters) ist als Anlage beigefügt**

Diese Angaben für jeden Auftragsverarbeiter im Verfahren einzeln machen!

B.8 Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt werden

☐ **intern (Zugriffsberechtigte)** **(Abteilung, Funktion)**
☐ **extern** **Empfängerkategorie** **(Kategorien oder konkret), inkl. Empfänger in Drittländern und internationale Organisationen**
☐ **Drittland oder internationale Organisation (Kategorie)**

B.9 Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

☐ **Datenübermittlung findet nicht statt.** ☐ **Datenübermittlung findet wie folgt statt:**
Nennung der konkreten Datenempfänger:
Dokumentation der geeigneten Garantien ☐ **Dokumentation ist beigefügt**

B.10 Rollenkonzept bei der Verarbeitung

Eingerichtete Rollen von Verarbeitern / Kategorien von Zugriffsberechtigungen

☐ **siehe Anlagen**

B.11 Hardware

Eingesetzte Hardware-Kategorien (Arbeitsplatz-PC, mobile Endgeräte, Server) und mitgeltende Benutzungsanweisungen

☐ **siehe Anlagen**

B.12 Software

Eingesetzte System- und Anwendungssoftware, Bezeichnung und Version (wenn relevant)

☐ **siehe Anlagen**

B.13 Ergebnis der Datenschutz-Folgenabschätzung (§ 35 KDG)

☐ **Eine Datenschutz-Folgenabschätzung nach § 35 KDG wurde durchgeführt.**

☐ **Das Verfahren wurde vor Inkrafttreten des KDG eingeführt, deshalb wurde keine Datenschutz-Folgenabschätzung, sondern eine Vorabkontrolle durchgeführt.**

☐ **Es wurde weder eine Datenschutz-Folgenabschätzung noch eine Vorabkontrolle durchgeführt.**

Bitte Erläutern!

☐ **Die Ergebnisdokumentation ist beigefügt.**

B.14 Technische und organisatorische Maßnahmen gemäß § 26 KDG

B.14.1 Allgemein (unternehmensweit) gültige technische und organisatorische Maßnahmen

(Hier kann ein Verweis auf ein mitgeltendes Dokument, d.h. eine übergreifende TOM-Beschreibung stehen, die für mehrere/alle Verfahren der Einrichtung gilt)

z.B. Angaben zu

- physikalischem Schutz: Zutrittskontrolle, Zugangskontrolle im Rechenzentrum
- organisatorischem Schutz: Zugriffskontrolle, Eingabekontrolle, Weitergabekontrolle, Auftragskontrolle; Trennungsgebot für alle Verfahren der Einrichtung
- technischem Schutz: Verfügbarkeits- und Backup-Konzept, Wiederherstellungskonzept (Desaster-Recovery) auf Datenbank-Ebene

☐ **Referenzierte Dokumente sind als Anlage beigefügt.**

B.14.2 Spezielle technische und organisatorische Maßnahmen für das spezifische Verfahren, die über die allgemeinen Maßnahmen hinausgehen

Hier können spezielle Maßnahmen benannt werden, die für das Verfahren eingerichtet werden. Die folgende Liste ermöglicht die Zuordnung der Maßnahmen zu den Kategorien des § 26 Abs. 1 KDG und der Anlage 1 zum § 6 KDO. In der Regel werden nicht zu allen Kategorien spezielle Maßnahmen benannt werden.

Pseudonymisierung, Anonymisierung und Verschlüsselung	Welche Maßnahmen werden getroffen? Warum wurde so entschieden? (z.B. unter Berücksichtigung der verarbeiteten Daten-Kategorien bzw. Datenschutzklassen)
Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit	Welche besonderen Maßnahmen wurden getroffen? (z.B. wenn besondere Kategorien personenbezogener Daten verarbeitet werden)
Wiederherstellung	Wie wird die verlustfreie Wiederherstellung nach technischen Störungen oder

VzV 180620
KDSZ 2018

	Cyberattacken sichergestellt?
Überprüfung, Bewertung und Evaluierung	Wie wird sichergestellt, dass die Sicherheitsmaßnahmen ständig auf Wirksamkeit überprüft und dem Stand der Technik und einer geänderten Bedrohungslage angepasst werden?
Zutrittskontrolle	Welche besonderen, über die allgemeinen Regelungen hinausgehenden Maßnahmen wurden getroffen? (z.B., wenn die Verarbeitung an besonderen Orten erfolgt)
Zugangskontrolle	Wie wird die unbefugte Nutzung der spezifischen Datenverarbeitungsanlage verhindert oder aufgedeckt? (z.B. besondere zusätzliche Identifizierung durch Token oder Passwörter, evtl. in Kombination. Protokollierung des Systemzugangs etc.)
Zugriffskontrolle	Welche besonderen Regeln zum Umgang mit Datenträgern wurden aufgestellt? Wie wird die Einhaltung kontrolliert? Sind die Daten auf den Datenträgern verschlüsselt?
Weitergabekontrolle	Wie ist die Durchführung der Datenübertragung an Dritte bzw. der notwendigen Datenübermittlung an Auftragnehmer geregelt? Gibt es eine Data Loss Prevention (DLP) Policy, die den unberechtigten Abfluss von Daten verhindert oder erschwert? Werden Daten auf dem Transportweg verschlüsselt?
Eingabekontrolle	Wie wird durchgängig nachvollziehbar, ob und von wem Daten eingegeben, verändert oder entfernt wurden? (Gibt es beispielsweise eine Protokollierung?)
Auftragskontrolle	Existieren für alle Auftragsverarbeitungen ausreichende und geprüfte Verträge? Wie werden die Auftragnehmer kontrolliert?

Trennungsgebot	Wie wird sichergestellt, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden? Gibt es eine Mandantentrennung (logisch über Mandantenkennzeichen, physikalisch in getrennten Datenbanken und per Zugriffssteuerung mittels verschiedener Berechtigungen). Ist ein getrennter Testdatenbestand vorgesehen?

....

Verantwortlicher Datum Unterschrift

WEITERE INFORMATIONEN

KDG-Beurteilung von Messengern und Social-Media-Diensten

Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland

(Sitzung vom 26.07.2018 in Frankfurt)

Beurteilung von Messenger- und anderen Social Media-Diensten

Die Konferenz der Diözesandatenschutzbeauftragten beschließt die nachfolgende Kriterienliste.

Kriterien zur Beurteilung von Messengern und anderen Social Media-Diensten

Vorbemerkung

Die katholischen Datenschutzaufsichten haben nachfolgend die aus ihrer Sicht relevanten Kriterien für die Bewertung und die Auswahl eines geeigneten Messenger-Produktes unter Datenschutz-Gesichtspunkten zusammengestellt. Neben diesen können aber auch andere Kriterien eine Rolle spielen, deren Erfüllung für die legale Verbreitung im kirchlichen Raum förderlich ist.

Kriterien, die ein Dienst aus Sicht des Datenschutzes erfüllen muss

- ***Serverstandort:*** Wo verarbeitet der Dienst-Anbieter die Nutzerdaten? Hält der Provider die Drittlandbestimmungen ein, d.h. keine Datenspeicherung außerhalb der EU bzw. nur in Ländern, deren Datenschutzniveau durch die EU anerkannt ist?

  Aus §§ 39-41 KDG ergibt sich, dass eine Verarbeitung personenbezogener Daten nur dann in einem Drittland, also außerhalb der EU, stattfinden darf, wenn besondere Bedingungen erfüllt sind. Das können ein Angemessenheitsbeschluss der Europäischen Kommission, geeignete Garantien (§ 40 KDG) oder eine explizite Einwilligung der betroffenen Person (§ 41 Abs. 1 KDG) sein. In jedem Fall führt die Verarbeitung in einem Drittland zu einem deutlich größeren Aufwand bei der Herstellung und Überprüfung der Rechtmäßigkeit der Verarbeitung. Schon aus diesem Grund sowie dem permanenten Risiko, dass die Rechtmäßigkeit durch Änderung z.B. der Gesetzeslage im Drittland entfällt, raten wir von der Verarbeitung in einem Drittland ab, wenn nicht gleichzeitig eine

Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

Verschlüsselung nach dem Stand der Technik angeboten wird. Der Standort in einem Drittland wird weniger problematisch, wenn der zentrale Server nur verschlüsselte Daten zur Weiterleitung erhält, weil der Anbieter dann schon aus technischen Gründen den Inhalt der Kommunikation nicht offenlegen kann.

- ***Sicherer Datentransport:*** Werden die Inhalte der Kommunikation Ende-zu-Ende verschlüsselt, also z.B. auch bei der Zwischenpufferung auf dem Server des Providers?

  Nach § 26 KDG hat der Verarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau zu gewährleisten. Als geeignete Maßnahme wird unter anderem die Verschlüsselung personenbezogener Daten ausdrücklich genannt. § 27 KDG fordert, die Sicherheitsoptionen so zu gestalten, dass bereits durch die Voreinstellung das angemessene Schutzniveau gewahrt wird. Verschlüsselung darf deshalb nicht „optional zuschaltbar" sein, sondern sollte per Default vorgegeben werden. Die Sicherheit der Daten sollte auch nicht nur auf dem Transport, also auf dem Weg vom Endgerät des Senders über den zentralen Server bis zum Endgerät des Empfängers gewährleistet werden, sondern auch, wenn die Daten auf dem Endgerät angekommen sind, durch eine sichere Datenhaltung in der Applikation, die die Daten z.B. gegen ungewolltes Ausspähen durch andere Applikationen auf dem gleichen Endgerät schützt. Dem aktuellen Stand der Technik (im Jahr 2018) entsprechen Transport- und Inhaltsverschlüsselungen nach den Standards TLS 1.2 oder AES 256 bzw. 512-Bit ECC.

  Falls vorhanden, sollten Zertifizierungen des Produktes oder des Anbieters durch unabhängige Institutionen in die Bewertung einfließen.

- ***Datenminimierung:*** Werden die Metadaten der Verbindung so bald wie möglich gelöscht?

  Eine Beschränkung auf das für den Zweck der Verarbeitung notwendige Maß an personenbezogenen Daten wird in § 7, Abs.1 lit c) KDG gefordert. Die Beschränkung gilt für die Menge und den Zeitraum der Verarbeitung und Speicherung. Deshalb ist zu fordern, dass alle personenbezogenen Daten, also Inhalte und Verbindungsdaten der Kommunikation, sobald wie möglich gelöscht werden.

  Eine extreme Datenminimierung zusammen mit einer starken Ende-zu-Ende-Verschlüsselung führt dazu, dass der Provider selbst unter Zwang (z.B. durch staatliche Behörden) technisch nicht in der Lage ist, Daten herauszugeben. Ebenso laufen illegale Angriffe auf die zentralen Server in Leere.

- ***Respektierung der Rechte Dritter:*** Werden nur die Kontaktdaten der an der Kommunikation Beteiligten verwendet und behält der Anwender die Kontrolle über sein Telefonbuch, oder wird z.B. das komplette Telefonbuch an den Provider übermittelt und die Verantwortung für die Information der Betroffenen auf den Anwender abgewälzt?

  Personenbezogene Daten müssen rechtmäßig und für den Betroffenen in nachvollziehbarer Weise verarbeitet werden. (§ 7 Abs. 1 KDG). Der Betroffene hat nach §§ 14 und 15 KDG umfassende Rechte auf Information über den Umfang und die Art der Verarbeitung seiner Daten. Dagegen verstößt regelmäßig die Ausspähung von Adressen und Kontaktdaten des Telefonbuches durch allzu neugierige Applikationen. Manche

Anbieter versuchen über die AGB, die Verantwortung für die Einholung einer Einwilligung der Dritten in die Weitergabe ihrer Daten dem Nutzer aufzubürden, was dieser in der Praxis aber nie leisten kann.

Weitere Kriterien

Zu dem erweiterten Kriterienkreis gehören zum einen die Kosten: Der Entscheider sollte prüfen, ob die Nutzung des Produktes idealerweise für den privaten Nutzer kostenfrei und für die nicht-private Nutzung, also z.B. durch eine kirchliche Einrichtung, relativ erschwinglich ist.

Darüber hinaus sind die Bedingungen der Lizenzvergabe zu prüfen, die meistens in den AGB geregelt wird. Manche Anbieter untersagen die nicht-private Nutzung, andere untersagen lediglich die kommerzielle Anwendung. Während das Produkt im ersten Fall auch durch ehrenamtliche Non-Profit-Organisationen nicht genutzt werden darf, können diese im zweiten Fall – abhängig von den Formulierungen der AGB - doch von einer bestimmungsgemäßen Nutzung ausgehen. Nicht-privaten Nutzern wird manchmal eine spezielle „Business-Lösung“ angeboten, die aber oft mit höheren Lizenzkosten verbunden ist als die Privat-Anwendung. Einige Anbieter fordern ein Mindestalter der Nutzer von 16 oder sogar 18 Jahren, nochmals andere Anbieter stellen ihr Produkt nur für Nutzer mit Wohnsitz in bestimmten Staaten zur Verfügung.

Jeder Entscheider muss sich also ausführlich und umfassend über die Lizenzbedingungen der Produkte informieren.

Frankfurt, 26.07.2018

Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland

(Sitzung vom 10. und 11. Oktober 2018 in Bremen)

Facebook Fanpages

Die Konferenz der Diözesandatenschutzbeauftragten spricht erneut die Empfehlung aus, auf das Betreiben einer Facebook-Fanpage zu verzichten, da eine datenschutzrechtliche Haftung des Betreibers einer Fanpage nicht wirksam ausgeschlossen werden kann.

Bremen, 10. Oktober 2018

Dieser Beschluss knüpft an die Empfehlung der Diözesandatenschutzbeauftragten vom 26. Juli 2018 an, dass die Grundsätze der Datenschutzkonferenz des Bundes und der Länder (DSK) zum EuGH-Urteil vom 05.06.2018 ebenso für kirchliche Einrichtungen gelten, welche eine Fanpage bei Facebook betreiben. Ebenso sollten die kirchlichen Stellen den Fragenkatalog beachten, den die DSK am 05. September 2018 herausgegeben hat.

Die unmittelbar danach erfolgten Anpassungen der vertraglichen Grundlagen von Facebook zu den Insights-Daten können aus Sicht der Konferenz der Diözesandatenschutzbeauftragten die aufgeworfenen datenschutzrechtlichen Fragenstellungen nicht vollständig beantworten.

Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland

(Sitzung vom 17. April 2018 in Würzburg)

Veröffentlichung von Fotos von Kindern und Jugendlichen unter 16 Jahren

Die Konferenz der Diözesandatenschutzbeauftragten beschließt, dass zumindest für die Veröffentlichung von Bildern von Kindern bis zur Vollendung des 16. Lebensjahres die vorherige Einwilligung der Sorgeberechtigten unter Vorlage der jeweils zur Veröffentlichung vorgesehenen Bilder einzuholen ist. Der Beschluss korrespondiert mit der Entschließung der Konferenz der Beauftragten für den Datenschutz der EKD vom 12.04.2018, dem sich die Konferenz anschließt.

Würzburg, 18.04.18

Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

Konferenz der Diözesan-datenschutzbeauftragten der Katholischen Kirche Deutschlands

Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland

(Sitzung vom 10. und 11. Oktober 2018 in Bremen)

Rechtswirksamer Verzicht auf Einwilligungen bei Fotoaufnahmen

Die Konferenz der Diözesandatenschutzbeauftragten beschließt,

1. Eine Einwilligung zur Anfertigung und Veröffentlichung von Fotos, Film und Tonaufnahmen kann auch durch den Minderjährigen erteilt werden, sobald er über die erforderliche Einsichtsfähigkeit verfügt, was regelmäßig spätestens mit der Vollendung des 16. Lebensjahres der Fall ist.
2. Zur Veröffentlichung der Aufnahmen ist zusätzlich eine Einwilligung der Sorgeberechtigten des Minderjährigen erforderlich.
3. Die Grundsätze können nicht dadurch umgangen werden, dass das Elternrecht pauschal durch Vollmacht auf Dritte übertragen oder gänzlich auf das Grundrecht auf informationelle Selbstbestimmung verzichtet wird.

Bremen, 10. Oktober 2018

Erläuterungen zum Beschluss:

Eine einheitliche Definition von Jugendlichen oder Kindern gibt es im deutschen Recht nicht. Jedoch bezeichnet das Jugendgerichtsgesetz als Jugendliche Minderjährige zwischen 14 und 18 Jahren. Wer noch nicht 14 Jahre alt ist, wird als Kind bezeichnet.[1]
Die DSGVO macht demgegenüber keine Unterscheidung zwischen Jugendlichen und Kindern. In der Verordnung wird durchgehend von Kindern gesprochen. Art 8 Abs. 1 DSGVO bringt dennoch eindeutig zum Ausdruck, dass mit dem Begriff „Kinder" alle Personen unter 18 Jahren gemeint sind. Das KDG spricht in § 8 Abs. 8 von Minderjährigen.[2] Es geht nachfolgend also

[1] § 1 Abs. 2 JGG
[2] Ebenso das DSG-EKD (Datenschutzgesetz der evangelischen Kirche) in § 12

Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

um die Einwilligung von unter 18-jährigen Personen unabhängig von der Bezeichnung in den jeweiligen Normen.

Indem die DSGVO in Art. 8 und in Erwägungsgrund 65 S. 2 ausdrücklich die Möglichkeit der Einwilligung von Kindern anspricht, ist festgestellt, dass Geschäftsfähigkeit i. S. d. Bürgerlichen Gesetzbuches für die Einwilligung nicht erforderlich ist.[3]

Die DSGVO legt kein Mindestalter fest, ab dem eine Einwilligung durch einen Minderjährigen wirksam abgegeben werden kann. Lediglich in Artikel 8 Abs. 1 DSGVO, § 8 Abs. 8 KDG wird für den Fall des Angebotes von Diensten der Informationsgesellschaft das einem Kind direkt gemacht wird für die Wirksamkeit der Einwilligung ein Mindestalter von 16 Jahren gefordert.[4] Diese Altersregelung bezieht sich ausschließlich auf den benannten Anwendungsbereich. Eine generelle Voraussetzung für die Einwilligungsfähigkeit von Minderjährigen ist damit nicht festgeschrieben.[5] Insoweit ist keine Änderung durch die Verordnung gegenüber der davor geltenden Richtlinie[6] für solche Sachverhalte erfolgt, die Einwilligungen in Sachverhalte außerhalb dieser Vorschrift betrifft. Wie bislang im deutschen Recht kann deshalb auch weiterhin davon ausgegangen werden, dass die Wirksamkeit der Einwilligung eines Minderjährigen von dessen Einsichtsfähigkeit abhängt.[7], also davon ob der Minderjährige psychisch und intellektuell in der Lage ist, Bedeutung und Tragweite seiner Entscheidung einzuschätzen. Diese Sichtweise wird auch durch den Erwägungsgrund 58 gestützt. Abstrakte Aussagen, wann eine Einsichtsfähigkeit gegeben ist, insbesondere die Knüpfung an ein bestimmtes Alter, scheiden also aus.[8] Bestenfalls als ein Anhaltspunkt kann ab einem Alter von 14 bis 15 Jahren in der Regel vermutet werden[9], dass die Einsichtsfähigkeit gegeben ist, was jedoch nicht von einer Einzelfallprüfung entbindet.[10] Fehlt die Einsichtsfähigkeit, bedarf es der Einwilligung der Erziehungsberechtigten, liegt Einsichtsfähigkeit vor, ist eine doppelte Einwilligung sowohl des Minderjährigen als auch der Erziehungsberechtigten erforderlich.

Das Recht auf informationelle Selbstbestimmung ist als ein an eine bestimmte Person gebundenes Recht, das wegen seines besonderen Charakters im Grundsatz weder übertragbar

[3] Ernst in Paal/Pauly Art. 4 Rn. 66; Schwartmann/Hilgert in Heidelberger Kommentar Art. 8 Rn. 11
[4] Nach § 12 DSG-EKD Mindestalter 14 Jahre.
[5] Kampert in Sydow Europäische Datenschutzgrundverordnung Art. 8 RN. 7; Schwartmann/Hilgert in Heidelberger Kommentar Art. 8 Rn. 10
[6] EU DSRL 95/46/EG vom 24.10.1995
[7] Kampert in Sydow Europäische Datenschutzgrundverordnung Art. 8 RN. 7
[8] Simitis Kommentar zum BDSG § 4a Rn. 21
[9] 40. TB Hessischer Datenschutzbeauftragter
[10] Ernst, DANA 2017, 14

noch vererblich ist,[11] ein höchstpersönliches Recht. Damit muss grundsätzlich auch eine Einwilligung in Bezug auf ein solches Recht höchstpersönlich erklärt werden.[12] Ausnahme von diesem Grundsatz ist die Abgabe der Einwilligungserklärung der Sorgeberechtigten für ihr Kind.[13] Das Recht auf informationelle Selbstbestimmung ist nach der grundlegenden Entscheidung des Bundesverfassungsgerichtes zum Volkszählungsurteil selber ein Grundrecht.[14] Das Einwilligungsrecht der Eltern in dieses Grundrecht ihrer Kinder können die Eltern nur selber ausüben. Ein Verzicht darauf ist nicht möglich.[15] Eine willkürliche Übertragung dieses Rechtes an Dritte scheitert an der Höchstpersönlichkeit dieses Rechtes, bzw. daran, dass es sich hierbei um eine wesentliche Angelegenheit i. S. d. § 1687 I BGB handelt.[16] So ist insbesondere die Übertragung des Sorgerechts im Hinblick auf die Anfertigung von Bild- und Tonaufnahmen auf einen Dritten nicht möglich. Dies muss umso mehr gelten, wenn der Dritte damit eigene Interessen verfolgt. Dies dürfte bei der Anfertigung von Fotos oder Videoaufnahmen durch Kindergärten, Schulen und bei Ferienfreizeiten der Fall sein, da diese zumindest auch der Werbung für diese Einrichtung dienen. Insoweit dürfte ein Interessenkonflikt bei den Beauftragten bestehen.

Eine pauschale Generaleinwilligung für alle gleichgelagerten Fälle für die Dauer der Zugehörigkeit des Minderjährigen in einer Einrichtung ist grundsätzlich unzulässig. Dies wird insbesondere Einwilligungen zur Erstellung von Fotos und deren Veröffentlichung betreffen, die bei Aufnahme in die KITA oder die Schule für die gesamte Aufenthaltszeit erteilt werden. Art 4 Nr. 11 DSGVO wie auch § 8 Nr. 13 KDG definieren „Einwilligung“ als eine Willensbekundung in informierter Weise für einen bestimmten Fall. Eine informierte Einwilligung dürfte in der pauschalen Einwilligung für die Veröffentlichung aller Fotos während der gesamten Aufenthaltsdauer kaum anzunehmen sein.[17] Außerdem kann unter einem „bestimmten Fall“ nicht die Anfertigung von Fotos gemeint sein, sondern nur die Anfertigung und Veröffentlichung eines konkreten, eben bestimmten Fotos.

Eine Veröffentlichung liegt vor, wenn Daten einer nicht genau feststehenden Mehrzahl von Adressaten, die Dritte sind, zugänglich gemacht werden.[18] Sind die Personen miteinander

[11] Duden Recht A-Z. Fachlexikon für Studium, Ausbildung und Beruf. 3. Aufl.
[12] Simitis Kommentar zum BDSG § 4a Rn. 30; Weichert in DKWW Kommentar zum BDSG § 4a Rn. 6; Paal/Pauly Kommentar zur DSGVO Art. 4 Rn.65; 46. TB Hessischer Datenschutzbeauftragte S. 108
[13] Ernst DANA 2017, 14
[14] BVerfGE 65, 1ff.
[15] Palandt Kommentar zum BGB § 1626 RN. 3
[16] So im Ergebnis auch Hoffmann, JAmt 2015, 8
[17] 46. TB hessischer Landesbeauftragte für Datenschutz S. 109
[18] Dammann in Simitis Kommentar zum BDSG § 3 Rn. 157

oder mit dem Veranstalter bekannt, gehören sie nicht zur Öffentlichkeit.[19] Bei KITA´s dürfte deshalb keine Veröffentlichung darin zu sehen sein, wenn Bilder von Kindern innerhalb der Einrichtung ausgehängt werden.[20] Für diese Fälle ist von der ausnahmsweisen Zulässigkeit einer Generaleinwilligung auszugehen. Dies betrifft aber ausdrücklich nur den Innenbereich der Einrichtung im Rahmen der Zweckbindung. Aushänge in Schaukästen oder Veröffentlichung in Flyern sind von dieser Ausnahme nicht umfasst.[21] Für Schulen trifft dies nicht in gleicher Weise zu, da der Kreis der Dritten die Zugang zu der Einrichtung haben nicht wie bei Kindereinrichtungen überschaubar ist.

Ein Verzicht auf Grundrechte ist zumindest dann nicht möglich, wenn das Grundrecht über den einzelnen hinaus auch der Gemeinschaft zugutekommt. Nach Auffassung des Bundesverfassungsgerichts ist die Entfaltung der Persönlichkeit zu gewährleisten, weil Selbstbestimmung eine elementare Funktionsbestimmung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist.[22]

[19] § 15 Abs. 3 UrhG
[20] Caritasverband für das Bistum Trier e.V. Arbeitshilfe Datenschutz in katholischen Tageseinrichtungen für Kinder
[21] Ministerium für Kultus, Jugend und Sport Baden-Württemberg Datenschutzbroschüre Datenschutz in Kindertageseinrichtungen S. 16; Gutenkunst/Fachet Merkblatt für den Datenschutz in evangelischen und katholischen Kindertageseinrichtungen S. 7
[22] BVerfGe 65, 1ff.

Impressum

Herausgeber:
Arbeitsstelle für Jugendseelsorge der Deutschen
Bischofskonferenz (afj)
Carl-Mosterts-Platz 1, 40477 Düsseldorf
E-Mail: info@afj.de

Bund der Deutschen Katholischen Jugend (BDKJ)
Carl-Mosterts-Platz 1, 40477 Düsseldorf
E-Mail: info@bdkj.de

Jugendhaus Düsseldorf e. V. (JHD)
Carl-Mosterts-Platz 1, 40477 Düsseldorf
E-Mail: jhd@jugendhaus-duesseldorf.de

Redaktion:
Thomas Andonie, Prof. Andreas Büsch, Martina Burke, Wolfgang Ehrenlechner, Felix Neumann, Marie Schwinning, Christine Sentz

Layout/Satz: Verlag-Haus-Altenberg.de
Druck: Lokay.de

BDKJ Bund der Deutschen Katholischen Jugend

afj Arbeitsstelle für Jugendseelsorge der Deutschen Bischofskonferenz

jhd Bundeszentrale für Katholische Jugendarbeit Jugendhaus Düsseldorf

Weitere Informationen findet Ihr unter:
www.datenschutz-wiki.org