Datenschutz im Verband

Arbeitshilfe zum Umgang mit den Datenschutzregelungen in der Jugendverbandsarbeit

BDKJ
Bund der Deutschen Katholischen Jugend
Erzdiözese Köln

Inhalt

Vorwort

Liebe Verbandler*innen,

wie ihr sicherlich bereits wisst, trat am 24. Mai 2018 das neue kirchliche Datenschutzgesetz in Kraft. Und wahrscheinlich ging es euch ähnlich wie uns und ihr musstet bei all den Anforderungen erstmal schwer schlucken. Damit wollen wir aber natürlich nicht in Frage stellen, dass Datenschutz ein wichtiges Thema ist. Schließlich möchte niemand, dass mit seinen*ihren Daten Unfug angestellt wird.

Das bedeutet aber auch, dass einige Zeit in die Umsetzung der Datenschutzregeln investiert werden muss. Diese Arbeit können wir euch auch leider nicht abnehmen. Aber mit der vorliegenden Handreichung wollen wir euch Hilfestellungen geben, um sich mit den wichtigsten Fragestellungen zu beschäftigen. Neben erklärenden Texten findet ihr Checklisten und wichtige Fragestellungen für die Umsetzung.

Neben den Informationen in dieser Handreichung stellen wir einige Muster, wie Einverständniserklärungen oder ein Verarbeitungsverzeichnis sowie weitere Informationen auf unserer Homepage zur Verfügung, die wir bei Bedarf auch regelmäßig erweitern werden.[1] Gerne stehen wir euch auch bei weiteren Fragen rund um den Datenschutz zur Verfügung.

Euer BDKJ-Diözesanvorstand

Annika Jülich Elene Stötzel Renè Fanta Volker Andres

[1] https://www.bdkj-dv-koeln.de/material/datenschutz/

Allgemeine Informationen

Gesetzgeltung

DSGVO = Datenschutzgrundverordnung

Am 25. Mai 2018 löste eine einheitliche EU-Datenschutzgrundverordnung die bisherigen Regelungen ab. Diese Regelung ist Grundlage für die in Deutschland geltenden Datenschutzregelungen. Auch das kirchliche Datenschutzgesetz ist im Einklang mit der DSGVO.

KDG = Kirchliches Datenschutzgesetz[2]

Am 24.Mai 2018 löste das KDG die bisherigen Regelungen zum Datenschutz für kirchliche Rechtsträger ab. An vielen Stellen sind die Regelungen im KDG identisch mit der DSGVO. Es gibt aber einige wenige Stellen, wo es andere Regelungen gibt. Für die katholischen Jugendverbände innerhalb des BDKJ gelten die Regelungen des KDG.

Konferenz der Diözesandatenschutzbeauftragten

Die Konferenz der Diözesandatenschutzbeauftragten fasst regelmäßig Beschlüsse zur Konkretisierung der gesetzlichen Regelungen. Diese Beschlüsse geben die Rechtsauffassung der Diözesandatenschutzbeauftragten wieder. Das heißt, dass die Beschlüsse ebenfalls bei der Umsetzung der Datenschutzregelungen zu beachten sind. Die Beschlüsse der Konferenz der Diözesandatenschutzbeauftragten findet ihr auf der Homepage des Katholischen Datenschutzzentrums.[3]

[2] Den kompletten Gesetzestext findet ihr unter: https://www.datenschutz-kirche.de/sites/default/files/KDG%20i.d.%20Fassung%20des%20Beschlusses%20der%20VV%20vom%2020.11.2017.pdf

[3] https://www.katholisches-datenschutzzentrum.de/infothek/

Begrifflichkeiten

Im Zusammenhang mit der Umsetzung der Datenschutzregelungen werden euch manche Begrifflichkeiten immer wieder begegnen. Die wichtigsten wollen wir euch kurz erklären. Die genauen Formulierungen der gesetzlichen Definition sowie weitere Definitionen findet ihr in § 4 KDG.

Personenbezogene Daten

Alle Informationen, die direkt oder indirekt mit einer natürlichen Person in Verbindung gebracht werden können. Hierzu gehört neben den offensichtlichen, wie dem Namen auch weniger offensichtliche Daten, wie Standortdaten oder Bilddaten.

Besondere Kategorien personenbezogener Daten

Zu den besonderen Kategorien gehören genetische und biometrische Daten, sowie Gesundheitsdaten (z.B. Allergien) oder Daten zum Sexualleben oder der sexuellen Orientierung. Aber auch Informationen zur rassischen und ethnischen Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen. Die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft ist keine besondere Kategorie.

Bei den besonderen Kategorien ist stets Vorsicht geboten! Diese Daten haben einen höheren Schutzbedarf als die normalen personenbezogenen Daten, da prinzipiell durch sie ein höheres Risiko für den Betroffenen besteht. Daher gilt es solche Daten besser zu schützen und möglichst nicht zu intensiv zu verarbeiten.

Verarbeitung

Jede Nutzung der Daten stellt eine Verarbeitung dar. Dabei ist egal, ob dies automatisch oder händisch erfolgt. Beispiele von Verarbeitungstätigkeiten sind: Daten erheben oder speichern, sowie veröffentlichen aber auch Löschen oder Weitergeben.

Verantwortliche*r

Die Person oder Organisation, die über die Verarbeitung der Daten entscheidet. Bei euch ist dies in der Regel eure Ortsgruppe als Ganzes bzw. eure Leitung. Natürlich können weitere Personen, neben den Verantwortlichen Daten verarbeiten.

Auftragsverarbeiter*in

Externe, die in eurem Auftrag Daten verarbeiten, werden Auftragsdatenverarbeiter*innen genannt. Durch die gesetzlichen Vorgaben ist es gefordert, mit diesen eine gesonderte Vereinbarung oder einen gesonderten Auftragsdatenverarbeitungsvertrag (ADV) zu schließen. Ein typisches Beispiel hierfür ist ein IT-Dienstleister, der Geräte oder Server (z.B. für die Homepage) verwaltet.

Empfänger*in

Eine Person oder Organisation, der personenbezogene Daten offengelegt werden.

Dritter

Eine Person oder Organisation neben der betroffenen Person, dem*der Verantwortlichen und für ihn*sie Tätigen und dem*der Auftragsverarbeiter*in. Also alle Personen, die nicht selbst für euch Tätig sind bzw. betroffen sind.

Einwilligung

Die Zustimmung einer Person zur Erfassung und Verarbeitung ihrer Daten. Damit eine Einwilligung gültig ist, muss die Person vorher über den Grund und Zweck der Verarbeitung informiert werden und sie muss freiwillig einwilligen.

Die genauen Formulierungen der gesetzlichen Definition sowie weitere Definitionen findet ihr in §4 KDG. Zusätzlich gibt es eine Arbeitshilfe zu Begriffen im neuen KDG des Katholischen Datenschutzzentrums.[4]

[4] https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2018/04/PH-16-Begriffe-im-neuen-KDG-Rev-1.0.pdf

Bußgeldordnung

Durch die neuen Gesetzgebungen gibt es nun auch neue Bußgeldordnungen. Die Strafenaus der DSGVO sind dabei deutlich höher, als die des KDG. Während die DSGVO von bis zu 10. Mio. Euro oder 20. Mio. Euro spricht, alternativ auch 2 oder 4 Prozent des Jahresumsatzes, ist das maximale Busßgeldim KDG mit bis zu 500.000 Euro benannt. Auch wenn die Zahl deutlich niedriger klingt, ist dies doch ein enormer Betrag. Natürlich wird in der Praxis nicht direkt beim ersten kleineren Verstoß die Höchststrafeausgesprochen, allerdings sollen die Strafen „verhältnismäßig“ angepasst sein. Hierbei fließen dann verschiedene Faktoren mit ein, wie Art des Verstoßes, Umfang des Verstoßes, Vermeidbarkeit des Verstoßes, der Umfang der Daten, Kooperation mit der Datenschutzbehörde, sowie Vorsatz oder Fahrlässigkeit. Prinzipiell raten wir euch also davon ab, bewusst gegen diese Regelungen zu verstoßen!

Datenschutzbehörden

Es gibt im Rahmen des KDG fünf Datenschutzaufsichtsbehörden, die für die einzelnen (Erz-) Bistümer verantwortlich sind. Für die NRW-(Erz-) Bistümer ist das Katholische Datenschutzzentrum in Dortmund zuständig.

Diözesandatenschutzbeauftragter
Katholisches Datenschutzzentrum

Steffen Pau
Brackeler Hellweg 144 - 44309 Dortmund
Tel.: 0231 – 13 89 85 – 0
Fax: 0231 – 13 89 85 - 22
info@kdsz.de - https://www.katholisches-datenschutzzentrum.de/

Rechtsgrundlagen der Datenverarbeitungen

Bei den Gesetzestexten zur Datenverarbeitung handelt es sich um sogenannte „Verbote mit Erlaubnisvorbehalt“. Das heißt konkret, dass alle Datenverarbeitungen verboten sind, es sei denn sie sind durch spezielle Rechtsgrundlagen erlaubt. Macht euch am bestem im Vorhinein klar, welche Rechtsgrundlage hinter einer Verarbeitung steht. Solltet ihr keine Rechtsgrundlage ausmachen können, so dürft Ihr die Verarbeitung auch nicht weiter ausführen.

Die möglichen Rechtsgrundlagen, die euch eine Verarbeitung erlauben, sollen euch nun einmal nähergebracht werden:

a) rechtliche/kirchliche Rechtsvorschrift

Sollte das KDG oder eine andere kirchliche oder staatliche Rechtsvorschrift eine Verarbeitung von personenbezogenen Daten notwendig machen, so ist eine Verarbeitung erlaubt.

b) Einwilligung

Bei der Einwilligung hat ein*e Betroffene*r in die Verarbeitung seiner Daten freiwillig eingewilligt und sie somit rechtskonform gemacht. Hierbei solltet Ihr aber die entsprechenden Regelungen für das Einholen einer solchen Einwilligung beachten. Näheres dazu findet ihr unter dem Punkt Einwilligung (S. 35).

c) Vertragliche Pflichten

Die Verarbeitung ist zur Erfüllung eines Vertrages notwendig. Hierzu zählen insbesondere Dienstleisterverträge oder Arbeitsverträge. Beispiele aus der Jugendarbeit hierfür, sind Anmeldungen zu Veranstaltungen oder Ferienfreizeiten.

d) Rechtliche Verpflichtung

Natürlich dürfen Daten auch im Rahmen von rechtlichen Verpflichtungen verarbeitet werden. Um beispielsweise steuerrechtlichen oder versicherungsrechtlichen Verpflichtungen nachzukommen, müssen diese Daten verarbeitet werden.

e) Lebenswichtige Interessen

Mitunter kann es auch notwendig sein, Daten im Sinne von lebenswichtigen Interessen zu verarbeiten. Insbesondere humanitäre Gründe im Falle von Katastrophen, sollen hierunter fallen.

f) Wahrung einer Aufgabe im kirchlichen Interesse /Ausübung öffentlicher Gewalt

Einige Verarbeitungen erfolgen im kirchlichen Interesse. So ist es beispielsweise im kirchlichen Interesse, auf mögliche Veranstaltungen der Gemeinde hinzuweisen.

g) Berechtigte Interessen

Verarbeitungen, die sich nicht auf eine der übrigen Rechtsgrundlagen berufen können, werden häufig mit berechtigtem Interesse begründet. Hierbei gilt es aber eine Abwägung zwischen den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person und dem berechtigten Interesse des Verantwortlichen durchzuführen. Ein berechtigtes Interesse kann beispielsweise eine Videoüberwachung zum Schutz des Eigentums sein, allerdings nur unter den speziellen Voraussetzungen der Videoüberwachung durch das Gesetz, oder aber auch die Verbesserung von internen Abläufen.

Rechenschaftspflichten

Die neu geschaffenen Datenschutzgesetze fordern nun die sogenannte Rechenschaftspflicht. Das heißt, einem*einer Verantwortlichen muss nun nicht mehr nachgewiesen werden, dass er*sie sich nicht datenschutzkonform verhalten hat, sondern er*sie muss von sich aus selbst beweisen, dass er sich datenschutzkonform verhält.

Für euch in der Praxis heißt das folgendes: Dokumentiert so viel ihr könnt. Alles was in irgendeiner Form (elektronisch oder schriftlich) dokumentiert ist, ist geregelt; alles was nicht dokumentiert ist, ist nicht geregelt. Also achtet darauf, alle Richtlinien/Anweisungen/Dokumente möglichst

nachweisbar aufzubewahren, denn nur so könnt ihr deren Wirksamkeit oder deren Einsatz auch nachweisen.

Verarbeitungsverzeichnis

Eine weitere Anforderung durch das Datenschutzgesetz ist die Erstellung eines Verarbeitungsverzeichnisses. Dieses soll alle Verarbeitungstätigkeiten in eurem Verband bzw. eurer Ortsgruppe erfassen. Angefangen bei den Beitrittserklärungen, über Anmeldungen zu einzelnen Veranstaltungen, bis hin zur Versendung von Newslettern. Hierfür solltet ihr gemeinsam überlegen, wann bei euch jeweils Daten verarbeitet werden und zu welchem Zwecke. Das Verarbeitungsverzeichnis muss möglichst detailliert auflisten, wofür Daten, welche Daten und wie die Daten verarbeitet werden.

Inhalt eines Verarbeitungsverzeichnisses

- Bezeichnung der Verarbeitung
- Welcher Personenkreis verarbeitet die Daten?
- Welche Daten werden verarbeitet?
- Wer hat Zugriff auf die Daten?
- Wozu werden die Daten verarbeitet?
- Wo kommen die Daten her?
- Gibt es eine Auftragsverarbeitung?
- Technische und organisatorische Maßnahmen
- Wann werden die Daten gelöscht?

Als Hilfestellung haben wir eine ausführliche Liste von üblichen Verarbeitungstätigkeiten, sowie ein Verarbeitungsverzeichnis erstellt.[5]

[5] Ihr findet beides unter: https://www.bdkj-dv-koeln.de/material/datenschutz/

Organisatorisches

Nutzung privater Geräte/Accounts/Ressourcen

Die Nutzung von privaten Geräten und Accounts zu verbandlichen Zwecken ist ein schwieriges Feld.

Beispiel:

Ein Verein stellt zu Datenverarbeitungszwecken Laptops zur Verfügung, die privat genutzt werden dürfen. Nach einigen Monaten gehen diese Rechner an den Verein zurück, doch dieser darf auf die darauf gespeicherten Daten nicht zugreifen, da er nach Fernmeldegeheimnis nicht auf die privaten Daten der Nutzer zugreifen darf. Somit sind die Daten für den Verein verloren.

Ähnlich wie in dem Beispiel sieht es aus, wenn private Geräte für den Verband genutzt werden, da dort ebenfalls private Daten anfallen und private Geräte gar nicht an den Verein ausgehändigt werden können. Da dies in der Jugendarbeit die Regel ist, müsst ihr schriftlich Vereinbaren, wie mit privaten Geräten umgegangen wird.

Falls ihr Geräte habt, die dem Verband gehören, müssen wir eigentlich empfehlen die private Nutzung zu verbieten, sodass nur verbandseigene Daten drauf gespeichert sein dürfen. Alternativ könnt ihr die private Nutzung auch erlauben. Dann sollten allerdings klare Regeln aufgestellt werden, wo private Daten zu speichern sind. Dies kann ein privater Ordner sein oder private Daten werden nur auf externen Geräten gesichert. Zusätzlich empfehlen wir eine schriftliche Erklärung auf Verzicht des Fernmeldegeheimnisses, in der der*die Mitarbeiter*in erklärt, dass der Verband auf seine*ihre privaten Daten zugreifen darf.

Unsere Empfehlung daher an euch:

Erstellt möglichst eine Richtlinie, wie mit privaten Geräten umzugehen ist und auch wozu sie genutzt werden dürfen und wozu nicht. Ebenfalls sollte die Nutzung von verbandseigenen Geräten geregelt sein. Wir wollen euch nicht vorschreiben, welcher Weg für euch der Richtige ist. Es macht sicherlich auch einen Unterschied, ob in eurer Gruppe nur Ehrenamtliche oder auch Hauptamtliche mitarbeiten.

Fragen, die ihr in einer Richtlinie beantwortet werden sollten:

- Darf ich mein privates Gerät zu Verbandszwecken nutzen?
- Wenn ja, wo werden private Daten gesichert?
- Wo speichere ich die Verbandsdaten?
- Was darf ich mit dem verbandseigenen Gerät tun (private Nutzung etc.)?
- Wie sichere ich die Geräte gegenüber Unbefugten Zugriff (Passwörter, Wegschließen, Verschlüsseln etc.)
- Gebe ich über Apps auf den Geräten die Daten an andere weiter (Messenger, Soziale Netzwerke etc.)?
- Gibt es eine Vereinbarung bezüglich des Fernmeldegeheimnisses?
- …

Datensparsamkeit

Die gesetzlichen Regelungen fordern, dass möglichst nur die Mengen an Daten zu verarbeiten sind, die für den konkreten Zweck notwendig sind.

Dieses Prinzip soll die Betroffenen davor schützen, zu viele nicht notwendige Daten preisgeben zu müssen. Andererseits erleichtert es auch die Arbeit der Verantwortlichen, denn diese sammeln so nur die Daten, die sie tatsächlich benötigen.

Beispiel 1:

Bei der Anmeldung zu einem Newsletter werden Namen, Adresse, Telefonnummer und die Mail-Adresse erfasst. Für die Verschickung des Newsletters ist allerdings die Mail-Adresse ausreichend. Zusätzlich kann für eine persönliche Anrede der Namen erfasst werden. Die übrigen Daten sind allerdings nicht nötig.

Macht euch also bei euren Verarbeitungen klar, welche Daten ihr für welche Verarbeitung benötigt. Mithilfe des Verarbeitungsverzeichnis (Vgl. S. 11) kann so beispielsweise eine Übersicht erstellt werden. Streicht ggf. die Möglichkeit zur Angabe von nicht benötigten Daten aus Anmeldeformularen etc., sodass für euch gar nicht erst die Möglichkeit besteht, unnötige Daten zu sammeln.

Beispiel 2:

Für Ferienfreizeiten wird eine Teilnahmeliste mit allen Daten erfasst. Hierzu gehören selbstverständlich Namen, Adresse, Alter, Allergien, Medikamenteneinnahme etc. Diese Liste muss jedoch nicht allen Leiter*innen zugänglich gemacht werden. Für die Küche ist es ausreichend, zu wissen wer eine Allergie hat oder nicht alles essen darf bzw. will. Die übrigen Daten sind für sie irrelevant.

Überlegt bei euren Veranstaltungen genau, wer welche Informationen für seine Tätigkeiten braucht. Natürlich erfasst die Hauptleitung alle Daten aber nicht alle Informationen sind für alle Leiter*innen gleichermaßen nötig.

Haftung

Falls es doch einmal zu einem Datenschutzverstoß kommen sollte und es werden Strafen ausgesprochen, so regelt sich die Haftung genauso wie bei anderen Verstößen auch: Der Verein haftet mit seinem Vereinsvermögen oder, je nach Regelung, kann es zu persönlichen finanziellen Haftung der rechtlichen Vertreter kommen. Insbesondere kann der Vorstand dann mit dem Privatvermögen haften, wenn ein Organisationsmangel, also beispielsweise ein nicht dokumentiertes und implementiertes System oder fahrlässiges bzw. vorsätzliches Handeln zum Schaden geführt hat.

Daher sollte sich jeder Vorstand selbstverständlich mit dem Datenschutz auseinandersetzen.

Datenschutzbeauftragte*r

Der*die Datenschutzbeauftragte ist in erster Linie eine Kontrollinstanz. Er*sie soll auf die Einhaltung des KDG und anderer Rechtsvorschriften hinarbeiten. Dazu hat er*sie

- die Anwendung von Datenverarbeitungsprogrammen zu überwachen,
- den*die Verantwortliche*n zu beraten,
- die mit der Verarbeitung tätigen Personen mit Erfordernissen des Datenschutzes vertraut zu machen (Unterweisungen),
- bei der Durchführung der Datenschutz-Folgenabschätzung zu beraten und zu unterstützen,
- sowie mit der Datenschutzaufsicht zusammenzuarbeiten.

Dabei ist er*sie der Leitung der jeweiligen Einrichtung unterstellt und ist in der Erfüllung seiner*ihrer Aufgaben nicht an Anweisungen gebunden. Er*sie ist frühzeitig in alle datenschutzrelevanten Fragen mit einzubeziehen.

Wann brauchen wir als Ortgruppe/ Regionalverband/ Diözesanverband einen Datenschutzbeauftragten?

Wenn….

- in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind.

➔ *Hierzu gehören sowohl Ehren- wie auch Hauptamtliche. In den meisten Fällen werden, zumindest in den Ortsgruppen/ Regionalverbänden, nicht 10 Personen ständig mit personenbezogenen Daten arbeiten.*

- die Kerntätigkeit des*der Verantwortlichen in der Durchführung von Verarbeitungstätigkeiten liegt, die aufgrund ihrer Art/ ihres Umfangs/ Ihres Zwecks eine regelmäßige, systematische Überwachung von betroffenen Personen erforderlich macht

➔ *Dies trifft in den seltensten Fällen auf die Jugendverbände zu.*

- Die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung von besonderen Kategorien von personenbezogenen Daten oder über strafrechtliche Verurteilungen/Straftaten besteht.

➔ *Dies trifft in den seltensten Fällen auf die Jugendverbände zu.*

Wer darf alles Datenschutzbeauftragte*r (DSB) werden?

Fast jede*r. Wichtig ist nur, dass die anderen Aufgaben und Pflichten des DSB nicht in einem Interessenkonflikt mit seiner Tätigkeit als DSB stehen. Dazu würden Leiter*innen von Datenverarbeitungen zählen (IT-Administrator*in, Marketing-Leiter*in etc.) aber auch die Leitung des Verbandes (z.B. Vorstand, Geschäftsführung etc.). Die Anforderungen zur Fachkenntnis des DSB findet ihr in dem Beschluss der Konferenz der Diözesandatenschutzbeauftragten: „Fachkunde für bDSB in der katholischen Kirche“.[6]

[6] Beschluss vom 08. Februar 2018: Zu Mindestinhalten der Fachkunde betrieblicher Datenschutzbeauftragte(r): https://www.katholisches-datenschutzzentrum.de/infothek/

Unterscheidung zwischen Ehren-/ Hauptamtlichen

Prinzipiell unterscheidet das KDG nicht zwischen Ehren-/ und Hauptämtern bzw. Hauptberuflichen. Insbesondere bei der Frage nach dem*der Datenschutzbeauftragten und der Anzahl der verarbeitenden Personen werden alle mitgezählt.

Umgang mit Externen

Auftragsverarbeiter*in

Mit Externen, die für euch Daten verarbeiten (z.B. IT-Dienstleister, Papierentsorger) muss ein Auftragsdatenverarbeitungsvertrag (ADV) geschlossen werden. Dieser Vertrag sichert euch ab und verpflichtet den*die Auftragsverarbeiter*in, sich bei der Verarbeitung eurer Daten auch an die geltenden Regeln zu halten.

Inhalte, die eine solche Vereinbarung enthalten muss sind:

- Gegenstand der Datenverarbeitung
- Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien betroffener Personen
- Rechte und Pflichten des Verantwortlichen
- Er ergreift alle Maßnahmen nach § 26 KDG
- Er gewährleistet, dass alle zur Verarbeitung der personenbezogenen Daten befugten Personen durch den*die Auftragsverarbeiter*in zur Vertraulichkeit und Verschwiegenheit verpflichtet wurden.
- Die Daten werden nur auf dokumentierte Weise verarbeitet.
- Er*sie hält die Bestimmungen für die Inanspruchnahme der Dienste eines*einer weiteren Auftragsverarbeiter*in ein.
- Er*sie unterstützt ggf. den*die Verantwortliche*n mithilfe technischer und organisatorischer Maßnahmen zur Beantwortung von Anträgen auf Wahrnehmung der Rechte des*der Betroffenen.

- Es wird eine Regelung getroffen, was mit den Daten nach Abschluss der Erbringung der Leistung passiert, also ob sie gelöscht oder zurückgegeben werden, sofern keine Aufbewahrungsfristen existieren.

Wenn ein*e Auftragsverarbeiter*in sich nicht an die Weisung des*der Verantwortlichen hält und die Daten zu anderen Zwecken verarbeitet, wird er*sie selbst zum*zur Verantwortlichen und ist für die entsprechende Verarbeitung verantwortlich. Bei unsachgemäßer Verarbeitung kann der*die Auftragsverarbeiter*in auch mit in den Schadensersatz eingebunden werden. Der*die Auftragsverarbeiter*in darf die Daten nicht in einem Drittland verarbeiten.

Was ist jetzt zu tun?

- Erstellt eine Übersicht, die alle Externen enthält, die für euch Daten verarbeiten.
- Schließt mit allen externen Auftragsdatenverarbeiter*innen eine entsprechende Vereinbarung.

Tipp: Die meisten großen Anbieter bieten einen vorgefertigten Auftragsdatenverarbeitungsvertrag, sodass ihr keinen eigenen erstellen müsst.

Geheimhaltungsvereinbarung

Es kann bei euch auch vorkommen, dass ihr mit Externen zusammenarbeitet, die nicht als Auftragsverarbeiter*innen arbeiten, aber dennoch Zugriff auf personenbezogene Daten haben. Einige klassische Beispiele hierfür sind Reinigungskräfte, Berater*innen oder Lieferanten.

Um euch hier abzusichern, solltet ihr mit denen eine Vereinbarung schließen, die mindestens folgendes enthält:

- Den tätigen Personen ist es untersagt, die Daten unbefugt zu verarbeiten.
- Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort
- Die Weitergabe ist nur nach den gesetzlichen oder vertraglichen Bedingungen erlaubt

Was ist jetzt zu tun?

Prüft, ob ihr mit weiteren Externen eine Geheimhaltungsvereinbarung abschließen müsst und schließt diese gegebenenfalls ab.

Gemeinsame Verantwortliche

Es ist auch möglich, dass zwei Organisationen eine gemeinsame Verantwortlichkeit haben. Dies ist beispielsweise der Fall, wenn ihr mit einer anderen Pfarrei zusammen eine Veranstaltung durchführt.

Bei gemeinsam Verantwortlichen haben beide Verantwortlichen die Sorgfalt und Pflichten des Datenschutzes zu beachten. Allerdings gibt es oft unterschiedliche Interessen bei der Verarbeitung oder andere Verfahren zur Datenverarbeitung.

Wichtig hierbei ist, dass klare Regelungen getroffen werden, wer welchen Verpflichtungen des KDG nachkommt. Am einfachsten ist dies in einer gemeinsamen Vereinbarung zu treffen, die die folgenden Punkte beinhalten sollte:

- Wer erfüllt welche Verpflichtung gemäß des KDG?
- Wer kommt den Informationspflichten nach § 15 KDG und § 16 KDG nach?
- Die jeweiligen tatsächlichen Funktionen der Verantwortlichen
- Beziehung der Verantwortlichen zur betroffenen Person
- Informationen zu den stattfindenden Verarbeitungen und der betroffenen Daten

Es gelten also ähnliche Voraussetzungen wie bei den Auftragsdatenverarbeiter*innen.

Macht euch also klar, wer mit euch zusammenarbeitet und in welcher Funktion. Unterscheidet ganz klar, wer jetzt als Auftragsverarbeiter*in arbeitet, wer zur Geheimhaltung zu verpflichten ist und wer eventuell ein gemeinsame*r Verantwortliche*r ist.

Umgang mit Daten

Datenweitergabe

Andere kirchliche Organisationen

Es kommt immer wieder vor, dass Daten an andere kirchliche Stellen weitergegeben müssen. Dies können beispielweise die Pfarrgemeinde, die Katholische Jugendagentur (KJA) oder der Dachverband sein.

Die Weitergabe ist erlaubt, wenn diese für die Erfüllung eurer Aufgaben oder der empfangenden Organisation notwendig sind und eine gültige Rechtsgrundlage (vgl.

Rechtsgrundlagen der Datenverarbeitungen, S.9) für die Verarbeitung vorliegt. Ihr müsst also begründen können, warum eine Verarbeitung bei euch durchgeführt werden darf und warum es rechtens ist, dass ihr diese Daten für die jeweilige Stelle offenlegt.

Beispiel:

Wenn ihr für eine Veranstaltung KJP-Mittel als Zuschuss erhalten wollt, müsst ihr bestimmte Daten wie eine Teilnahmeliste an den BDKJ weitergeben. Die Offenlegung der Daten ist notwendig und somit zulässig, da nur dadurch über die Höhe und Rechtmäßigkeit des Zuschusses entschieden werden kann. Die erforderlichen Daten, die ihr zur Verfügung stellt, müssen nach einer Rechtsgrundlage erfasst worden sein, beispielsweise aufgrund eines Vertrages oder einer Einwilligung.

Weiterhin müssen bei einer Offenlegung weitere Punkte beachtet werden:

- Die Interessen der Betroffenen müssen gewahrt bleiben.
- Wenn ihr Daten zur Verfügung stellt, tragt ihr die Verantwortung für die Zulässigkeit
- Wenn die empfangende Organisation Daten anfordert, trägt sie die Verantwortung für die Zulässigkeit
- Die Daten wurden für den entsprechenden Zweck erhoben

- Eine Offenlegung von nicht notwendigen Daten ist nur dann erlaubt, wenn eine Trennung der Daten nicht oder nur mit unvertretbarem Aufwand erfolgen kann.

Drittländer

Solltet ihr eure Daten in Drittländer übertragen, so sind einige besondere Aspekte zu beachten. Prinzipiell ist die Übertragung in Drittländer nur gestattet, wenn der*die Empfänger*in der Daten sich auf die Einhaltung des KDG oder anderer Vorschriften verpflichtet.

Da dies nicht immer einfach zu durchschauen ist, empfehlen wir euch darauf zu achten, dass eure Daten nur auf Servern in Deutschland, der EU bzw. in Ländern die zusätzlich als angemessen gelten gespeichert sind. Als angemessen gelten die EWR-Staaten Norwegen, Island, Liechtenstein, sowie Argentinien, Andorra Guernsey, Isle of Man, Jersey, Kanada, Neuseeland, Israel, Schweiz, Färöer-Inseln, Uruguay.

Nutzung von Datenbeständen

Prinzipiell dürft ihr eure bestehenden Datenbestände nur für die Zwecke nutzen, für die ihr sie erhoben habt. Also wenn ihr eure Daten zur Mitgliederdatenverwaltung erhoben habt, dann dürft ihr sie auch nur dafür nutzen.

Allerdings gibt es die Möglichkeit, diese Daten trotzdem für andere Zwecke nutzen zu können. Das ist aber nur zulässig, wenn…

- Eine Rechtsvorschrift dies vorsieht (vgl.
- Rechtsgrundlagen der Datenverarbeitungen S.9)
- Die betroffene Person eingewilligt hat
- Offensichtlich ist, dass es im Sinne des Betroffenen liegt
- Angaben überprüft werden müssen (bei tatsächlichen Anhaltspunkten für Fehlerhaftigkeit)
- Die Daten allgemein zugänglich sind oder der*die Verantwortliche sie veröffentlichen dürfte (außer das schutzwürdige Interesse der*des Betroffenen überwiegt)

- Es zur Abwehr einer Gefahr für die öffentliche Sicherheit notwendig ist
- Es zur Verfolgung von Straftaten/ Strafvollzugsmaßnahmen/ Vollstreckung von Bußgeldentscheidungen notwendig ist.
- Es zur Abwehr von schwerwiegenden Beeinträchtigung der Rechte eines Dritten erforderlich ist
- Der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert.

Wenn ihr eure bestehenden Datenbestände anders nutzen wollt, macht euch klar wofür ihr die Daten nutzen wollt und ob es mit dem ursprünglichen Zweck nicht vereinbar ist. Im Zweifel holt euch einfach eine neue Einwilligung ein.

Umgang mit Teilnahmelisten

Bei der Erstellung und Verwendung von Teilnahmelisten gilt das Prinzip der Datensparsamkeit. Stellt euch dafür folgende Fragen:

- Welche Daten werden für die Durchführung der Maßnahme benötigt?
- Wer braucht welche Informationen für seine Tätigkeit?
- Wie kann ich die nötigen Informationen sinnvoll weitergeben?

Beispiel:

Bei einer Ferienfreizeit teilt ihr jedem Zelt Leiter*innen als Ansprechpersonen und Zeltleitung zu. Diese sind dafür verantwortlich, dass die Teilnehmenden in ihrem Zelt ihre benötigten Medikamente einnehmen. Es ist ausreichend, wenn die Zeltleitungen über die Medikamenteneinnahme der Teilnehmenden in ihrem Zelt Bescheid wissen und nicht alle Leiter*innen.

Aber: Es kann natürlich auch nötig sein, dass für die Durchführung eures Zeltlager weitere Leiter*innen über die benötigten Medikamente einzelner Teilnehmenden Bescheid wissen müssen.

Löschen von Daten

Prinzipiell müsst ihr alle Daten löschen, sobald der Zweck zur Verarbeitung erloschen ist. Beachtet hierbei aber auch immer gesetzliche Aufbewahrungsfristen. Schaut daher mal in eure Archive und Datenbestände, welche Daten ihr vorliegen habt und prüft dann, welche Aufbewahrungsfristen hierbei gelten.

Relevante Aufbewahrungsfristen

- Mitgliederlisten: 6 Jahre
- Abrechnungsunterlagen: 10 Jahre
- Unterlagen von Maßnahmen (z.B. Teilnahmelisten): 10 Jahre
- Jahresabschlüsse: 10 Jahre
- Abgelehnte Bewerbungen: 2 Monate
- Briefe: 6 Jahre
- Fahrtenbücher: 10 Jahre
- Inventar: 10 Jahre
- Quittungen/ Rechnungen: 10 Jahre
- Verträge: 10 Jahre
- …

In bestimmten Fällen kann es über die gesetzlichen Aufbewahrungsfristen für euch sinnvoll sein, einige Daten weiterhin aufzubewahren. Hier müsst ihr euch die gleichen Fragen entsprechend dem berechtigten Interesse stellen (vgl. S.10).

Sonderfall: Bewerbungsunterlagen

Hierbei müsst ihr etwas aufpassen! Sobald eine Bewerbung abgelehnt wurde, so ist der Zweck erloschen und ihr müsst die Daten löschen. Um euch aber gegenüber möglicher Klagen aufgrund des Diskriminierungsgrundsatzes zu schützen, könnt ihr die Daten noch zwei Monate lang aufbewahren, dann sind diese aber endgültig zu vernichten. Möchtet ihr die Bewerbung länger aufbewahren (mögliche Stelle in absehbarer Zeit), so solltet ihr euch die Einwilligung des Bewerbers einholen.

Online und Internet

Homepages (Online-Auftritte)

Eine Homepage kann viele Vorteile mit sich bringen. Man schafft zum einen eine gute Außenrepräsentation, bietet aber gleichzeitig auch Anderen die Möglichkeit, sich zu informieren. Hierbei gibt es aber einige Punkte zu beachten, damit dies auch datenschutzkonform abläuft.

Datenschutzerklärung

Im Wesentlichen ist die Datenschutzerklärung nichts anderes als das Nachkommen der Informationspflicht für den Verarbeitungsvorgang durch eure „Website“. Hierin wird erklärt, wer auf der Website welche Daten verarbeitet und was mit diesen passiert. Diese Informationen müssen dem*der Besucher*in der Website so zur Verfügung gestellt werden, dass er*sie sie bei der Erhebung seiner*ihrer Daten lesen kann, also bei seinem*ihrem ersten Besuch auf der Website. Das heißt für die Praxis, dass die Datenschutzerklärung von jeder Seite und Unterseite der Homepage aufgerufen werden kann, ähnlich wie das Impressum.

> Die Datenschutzerklärung muss mit einem Klick von jeder Seite aus erreichbar sein und auch als solche erkennbar sein.

Für die Erstellung der Datenschutzerklärung gibt es mittlerweile sogenannte Datenschutzerklärungsgeneratoren. Diese sind zwar häufig auf die DSGVO eingestellt, da die Informationspflichten sich zwischen KDG und DSGVO nicht sonderlich unterscheiden, könnt Ihr diese zur Erstellung von bestimmten Texten verwenden. Die Generatoren gibt es sowohl als kostenlose Variante oder aber auch kostenpflichtig (häufig dann aber individueller und mit möglicher Rechtsabsicherung). Die sicherste (aber teuerste Variante) ist die Erstellung der Datenschutzerklärung durch einen Fachanwalt.

Cookies

Häufig nutzen Websitebetreiber*innen zur Verbesserung der Website sogenannte Cookies. Dies sind kleine Textdateien, die auf dem Rechner des*der Websitebesucher*in gespeichert werden und so diverse Funktionen überwachen können, wie beispielsweise das Verfolgen der Website-Nutzung oder den verwendeten Browser.

Welche Cookies bzw. welche Programme auf der Website Cookies setzen, muss in der Datenschutzerklärung genannt und beschrieben sein. Es gibt auch Cookies, in deren Verwendung eingewilligt werden muss. Dies kann über ein entsprechendes Banner beim Erstaufruf der Website erfolgen.

Was ist jetzt zu tun?

Erkundigt euch, welche Cookies ihr verwendet und wozu. Entscheidet dann, ob der einfache Hinweis in den Datenschutzerklärungen ausreicht oder ob ihr noch ein zusätzliches Banner einbauen solltet. Das Banner kann natürlich auch freiwillig von euch eingebaut werden.

Online-Anmeldungen/ Kontaktformulare

Bei Online-Anmeldungen oder auch Kontaktformularen gibt es ebenfalls einige Dinge zu beachten. Wichtig ist hierbei, dass die Formulare so spezifisch wie möglich sind und nur die Daten abgefragt werden, die auch für den Zweck nötig sind. Für die Anmeldung zu einer Veranstaltung werden sicherlich andere Daten benötigt, als für ein einfaches Kontaktformular.

Die einzugebenden Daten sind nach dem Prinzip der Datensparsamkeit zu sammeln. Markiert also die Angaben, die zwingend zur weiteren Verarbeitung notwendig sind als solche Pflichtangaben. Weitere optionale Angaben, wie ein alternativer Benachrichtigungsweg per Mail, sollten sich von den Pflichtangaben abheben. Verzichtet auf Dateneingaben, die nichts mit der weiteren Verarbeitung zu tun haben. Ein Feld für Kommentare oder Anmerkungen, in denen weitere Eingaben eingetragen werden können, ist natürlich weiterhin erlaubt aber verzichtet beispielsweise beim Anmelden eines Newsletters auf das Sammeln einer Telefonnummer. Achtet darauf, welche Rechtsgrundlagen der Datenverarbeitungen (vgl. S.9) hinter eurer

Verarbeitung steht. Beruht das Anmeldeformular rein auf einer Einwilligung, so muss dies auch deutlich gekennzeichnet sein. Zusätzliche, freiwillige Angaben die nichts mit dem jeweiligen Zweck zu tun haben, müssen auch als solche deklariert werden. Weitere Infos findet Ihr unter Punkt Einwilligung (S.35).

Was ist jetzt zu tun?

- Welche Formulare habt ihr auf eurer Homepage?
- Welche Daten werden erfasst?
- Wo können weniger Daten erfasst werden?

Newsletter und Werbung

Werbung ist prinzipiell keine schlechte Sache. Man möchte Leute für seine Projekte gewinnen und stellt ihnen daher Informationen zur Verfügung. Doch was ist dabei zu beachten?

Prinzipiell ist das Thema Werbung kein Datenschutzthema, sondern Verbraucherschutz. Der*die Verbraucher*in soll vor ungewollter und aufdringlicher Werbung geschützt werden. Daher lässt sich Werbung laut Datenschutz oftmals nur mit einer Einwilligung begründen. Der Verbraucher muss also konkret in die bestimmten Zwecke einwilligen. Achtet hierbei auf das Kopplungsverbot, also den Werbeversand mit anderen Zwecken zwangsweise zu verknüpfen. Bietet die Möglichkeit zur Werbeeinwilligung stets als eine freiwillige optionale Möglichkeit, die keine Nachteile für den*die Betroffenen mit sich ziehen kann.

Newsletter und Werbung dürfen nur nach einer Einwilligung verschickt werden.

Bei Newslettern verhält es sich ähnlich. Diese werden häufig auf Basis einer Einwilligung versendet und bedienen sich dabei dem Double Opt-In-Prinzip. Das heißt, dass ein*e Betroffene*r zweimal explizit einwilligt, diesen Newsletter zu erhalten. So soll gewährleistet werden, dass nur die Betroffenen einen Newsletter erhalten, die es auch wirklich wollen.

Achtet bei Newslettern ebenfalls auf das Prinzip der Datensparsamkeit, denn in der Regel benötigt man dafür nicht mehr als eine E-Mail-Adresse und ggf. einen Namen zur Anrede.

Was ist jetzt zu tun?

- Überprüft, ob ihr bisher Werbung oder Newsletter versendet.
- Wenn die Antwort darauf ja ist, überprüft eure bisherigen Einwilligungen.
- Wenn die Antwort darauf ja ist, überprüft euer Formular für zukünftige Einwilligungen.

Digitales und Social Media

Social Media

Soziale Medien oder soziale Netzwerke stellen eine Möglichkeit dar, Informationen in der Öffentlichkeit bereitzustellen. Allerding müsst ihr hierbei auch einige Aspekte beachten, um datenschutzkonform zu bleiben. Vor allem bei der Veröffentlichung von Fotos und weiterer personenbezogener Daten, müsst ihr darauf achten, dass nur zulässige Informationen veröffentlicht werden. Dies kann durch eine Einwilligung (Vgl. S. 35) oder andere Rechtsgrundlagen der Datenverarbeitungen (Vgl. S.9) erfolgen. Wenn ihr euch bei einer Sache nicht sicher seid, prüft lieber erneut, ob ihr es veröffentlichen dürft oder nicht.

Sonderfall Facebook:

Im Oktober 2018 hat die Konferenz der Diözesandatenschutzbeauftragten eine Empfehlung ausgesprochen, dass auf das Betreiben von Facebook-Fanpages verzichtet werden soll. Nach aktueller Einschätzung müssen verschiedene Punkte erfüllt werden, damit eine entsprechende Seite Betrieben werden kann. Die entsprechenden Informationen stellen wir euch auf unserer Homepage zur Verfügung.[7]

[7] https://www.bdkj-dv-koeln.de/material/datenschutz/

Programme

Die Sorgfalt und Datenschutzkonformität eurer Datenverarbeitung hängt nicht zuletzt von den verwendeten Programmen ab.

Wichtig ist, dass ihr nur Software verwendet, der ihr auch vertraut. Um das zu gewährleisten stellen Software-Entwickler Informationen zur Verfügung, welche Daten wie verarbeitet werden und wohin sie übertragen werden. Durch die Vielzahl an Programmen lässt sich nicht pauschal sagen welche konform und welche nicht konform sind.

Mögliche Auswahlkriterien für Software:

- **Lizensierte Software:** Verwendet möglichst nur lizensierte Software, keine Raubkopien!
- **Zertifikate/Standards:** Manche Programme sind zertifiziert oder unterliegen bestimmten Standards. Erkundigt euch, ob eure Programme eventuell ein Zertifikat haben oder einem (oder mehreren) Standards folgen.
- **Übertragung:** Erkundigt euch, wo eventuell Daten hinübertragen werden und zu welchem Zweck und insbesondere ob die Daten in ein Drittland übertragen werden.
- **Vertrauenswürdige Quellen:** Bezieht die Programme nur aus vertrauenswürdigen Quellen, bei denen ihr euch sicher sein könnt, dass sie euch keine Schadsoftware mit einschleusen.

Beim Erstellen des Verarbeitungsverzeichnisses (Vgl. S. 11) kann eine Programmübersicht ebenfalls sehr hilfreich sein. Anhand dieser könnt ihr für euch selbst verdeutlichen, welche Programme ihr wozu nutzt. Hierbei können euch schon einige Probleme der Programme auffallen.

Was ist jetzt zu tun?

- Prüft welche Programme ihr zu Verarbeitungen von Daten verwendet und ob diese auch Datenschutzkonform sind.

Clouds

Viele von euch nutzen bereits Clouds, um Daten untereinander zu teilen oder als Speichermöglichkeit, um von mehreren Geräten ortsunabhängig auf diese Daten zuzugreifen. Allerdings ist es im Sinne des Datenschutzes notwendig, dass ihr euch vergewissert welche Clouds ihr überhaupt nutzen dürft.

Die wichtigste Frage bei der Auswahl einer passenden Cloud ist:

Wo werden die Daten tatsächlich gespeichert?

Am besten werden die Daten in Deutschland oder der EU gespeichert und nicht in Drittländer (vgl.S.20). Alle Cloudanbieter stellen euch Informationen zur Verfügung, in welchem Land die Daten verarbeitet (also gespeichert) werden.

Einige Cloud-Anbieter stellen ihre (kostenfreien) Cloudservices nur zu privaten Zwecken zur Verfügung. Dementsprechend dürft ihr diese nicht für verbandliche Zwecke nutzen. Die Angaben hierzu findet ihr in den AGBs des jeweiligen Anbieters.

Was ist jetzt zu tun?

- Wenn ihr bereits eine Cloud verwendet, prüft ob die Daten auf Deutschen bzw. EU-Servern liegen. Ansonsten wechselt euren Cloud-Anbieter
- Schaut auch noch einmal, ob die Cloud für verbandliche Zwecke genutzt werden darf

Messenger

Die Nutzung von Messenger-Diensten ist ein schwieriges Thema. Die Datenschutzbehörden haben dazu ihre Meinungen und Ansichten mitgeteilt, welche hier einmal für euch dargestellt werden sollen:

Kriterien für Messenger Dienste:

- Serverstandort: Die Verarbeitung der Daten darf nur dann in einem Drittland erfolgen, wenn ein Angemessenheitsbeschluss, geeignete Garantien oder die Einwilligung der Betroffenen Person vorliegt. Die Datenschutzbeauftragten raten von einer Verarbeitung in Drittländern ab, sofern nicht eine Verschlüsselung nach dem Stand der Technik angeboten wird.
- Sicherer Datentransport: Die Inhalte der Kommunikation sollten Ende-zu-Ende verschlüsselt sein. Die Verschlüsselung sollte nicht „optional zuschaltbar“ sein, sie sollte vorgegeben sein.
- Datenminimierung: Es sollten nur Daten im Umfang der notwendigen Maße verarbeitet werden, dass gilt insbesondere für die Metadaten (z.B. Wer ist wann online? Welche Kontakte hat man? Die IP-Adresse des Gerätes).
- Respektieren der Rechte Dritter: Es dürfen nur die Daten von Betroffenen weitergegeben werden, die der Nutzung oder Kommunikation zugestimmt haben. Einige Dienste nehmen aber auch Daten von Betroffenen auf, die dies nicht getan haben, ohne das der Nutzer darauf Einfluss hat.
- Nutzung: Nicht jeder Messenger-Dienst darf zu geschäftlichen Zwecken genutzt werden. Es gilt also die Lizenzbedingungen der Dienste zu prüfen, inwieweit die Dienste genutzt werden dürfen.

Für euch ist also wichtig festzuhalten, welchen Messenger-Dienst ihr nutzen wollt, und was dieser Dienst tut. Prinzipiell sind sie nicht verboten, aber oftmals sind die oben genannten Aspekte so umfangreich, dass man die Dienste nicht mehr nutzen kann.

Für die interne Kommunikation dürfen gerne Messenger genutzt werden (Macht es zur Not mithilfe einer schriftlichen Einwilligung konform). Achtet aber stets darauf, welche Daten ihr übertragen wollt und dürft. Manche Dienste erlauben es auch, den Zugriff auf bestimmte Daten einzuschränken. Schaut dazu mal in euren App-Einstellungen nach, ob ihr dort nicht einige Dinge rausnehmen könnt, die nicht notwendig sind. Oftmals führt dies zu Einschränkungen auf die Funktionalität des Dienstes. Das kann dann für die private Nutzung wieder hinderlich sein.

Aspekte, die ihr für eine mögliche Einwilligung beachten solltet:

- Freiwilligkeit der Einwilligung, keine Nachteile bei Nicht-Einwilligung
- Weitergabe von Daten einschränken (ggf. auf Kosten der Funktionalität)
- Festlegung, welche Daten über den Messenger ausgetauscht/weitergegeben werden dürfen.

Was ist jetzt zu tun?

- Welchen Messenger nutzt ihr für eure verbandliche Kommunikation? Ist dieser Datenschutzkonform? Einigt euch auf im Zweifel auf einen neuen Messenger.
- Macht die Nutzung ggf. durch eine Einwilligung konform.

Umgang mit Bildern

Veröffentlichung von Bildern

Bei der Veröffentlichung von Bildern muss neben den Datenschutzregeln auch das Urheberrecht bedacht werden. Auch für den Umgang mit Bildern gilt, dass eine Rechtsgrundlage (vgl.

Rechtsgrundlagen der Datenverarbeitungen, S.9) benötigt wird. Hierbei wird zwischen „Erheben und Speichern“ und „Veröffentlichen“ unterschieden.

Mögliche Rechtsgrundlagen für das Erheben und Speichern

- Berechtigtes Interessen, mit einer Abwägung eurer Interessen, sowie den Rechten und Freiheiten des*der Betroffenen
- Wahrung von kirchlichen Interessen, mit einer Abwägung kirchlicher Interessen und den Rechten und Freiheiten des Betroffenen
- Im Rahmen zugewiesener Aufgaben von Seiten der Kirche, für die die Verarbeitung notwendig ist.

Die gleichen Rechtsgrundlagen können für die Veröffentlichung herangezogen werden, insbesondere das berechtigte Interesse. Als weitere Abwägung können die Reglungen des Kunsturhebergesetzes herangezogen werden.

Erlaubte Veröffentlichungen laut Kunsturhebergesetz[8]:

- Bildern aus der Zeitgeschichte
- Bildern, in denen Personen nur als Beiwerk erscheinen (neben einer Landschaft/ Örtlichkeit)
- Bildern von Versammlungen, Aufzügen, ähnlichen Vorgängen, an denen die Dargestellten teilgenommen haben
- Bildnisse, die nicht auf Bestellung angefertigt worden sind, sondern die Verbreitung einem höheren Interesse der Kunst dient

[8] Vgl. §23 Kunsturhebergesetz.

Wenn einzelne Personen hervorgehoben sind oder nur einzelne bzw. wenige Personen Gegenstand des Bildes sind, so ist nicht mehr von einem Beiwerk auszugehen und die Abwägung würde gegen eine Veröffentlichung ausfallen.

Für euch heißt das also folgendes:

- Welche Rechtgrundlage steht hinter der Aufnahme und Veröffentlichung der Bilder steht?
- Welche Risiken und Freiheiten könntet ihr durch die Verarbeitung verletzen?
- Entscheidet dann, ob ihr die Bilder veröffentlichen wollt oder nicht.

Eine Ausnahme dieser Reglungen gilt für Fotos von Minderjährigen.

Fotos von Minderjährigen (U 16)

Für Minderjährige unter 16 Jahren gilt, dass sie besonders schutzbedürftig sind. Bei der Abwägung vor der Veröffentlichung von Bildern ist das Alter der abgebildeten Personen ein entscheidender Faktor. Wenn eine Abwägung erforderlich ist, kann diese nur zu Gunsten der*des Betroffenen erfolgen. Prinzipiell ist auch immer der*die Personenfürsorgeberechtigte miteinzubeziehen.

Konkret heißt das:

Die Verarbeitung und Veröffentlichung von Bildern für unter 16-Jährige kann nur dann rechtskonform sein, wenn eine Einwilligung vorliegt, die den Anforderungen des KDG genügt. Das heißt es muss vor der Veröffentlichung eine Einwilligung für das Konkrete Bild eingeholt werden.

Weitergabe von Bildern

Die Weitergabe von Bildern, z.B. an die Teilnehmenden einer Veranstaltung, ist anders geregelt, da hier die Bilder nur einem bestimmten Personenkreis zur Verfügung gestellt wird. Durch diesen begrenzten Personenkreis handelt es sich nicht um eine Veröffentlichung. Dies ist allerdings auch von der Größe des Personenkreises abhängig.

Genau wie bei der Veröffentlichung von Daten (also auch Bildern) müsst ihr eine Rechtsgrundlage (vgl. Rechtsgrundlagen der Datenverarbeitungen, S.9) haben, auf die Ihr die Weitergabe stützen könnt. Am einfachsten ist dies mit einer Einwilligung zu regeln. Bei der Einwilligung solltet ihr festhalten, an wen die Daten weitergegeben werden und das diese nicht zu missbrauchen sind (z.B. unerlaubte Weitergabe, Nutzung nicht geschäftlich etc.).[9]

Achtet bei dieser Weitergabe besonders darauf, wer seine Einwilligung nicht erteilt hat, denn ihre*seine Daten (also Bilder) dürft ihr nicht weitergeben.

[9] Eine Mustereinwilligung findest du unter: https://www.bdkj-dv-koeln.de/material/datenschutz/

Einwilligung

Solltet ihr keine Rechtsgrundlage für die Verarbeitung von Daten finden können, so bleibt euch immer noch die Möglichkeit der Einwilligung. Wir empfehlen euch, von euren Mitarbeiter*innen bzw. Leiter*innen generell eine solche Einwilligung einzuholen, damit ihr bei diesen durchweg auf der sicheren Seite der Rechtsgrundlagen seid.

Eine Rechtskonforme Einwilligung enthält:

- Freiwilligkeit: Die Verarbeitung muss freiwillig erfolgen. Ein Aspekt kann sein, dass die Einwilligung zu einer Verarbeitung notwendig ist, die nicht zur Erfüllung eines Vertrages erforderlich ist,
- Anlassbezogen auf einen bestimmten Fall,
- Informationen zur Datenverarbeitung,
- Unmissverständliche Willensbekundung,
- In Form einer schriftlichen Erklärung: Ihr müsst nachweisen, dass ein Betroffener seine Einwilligung erteilt hat. Am einfachsten ist die Schriftform.
- Folgen der Nicht-Einwilligung: Ihr müsst auf mögliche Folgen einer Nicht-Einwilligung hinweisen („Durch ihre Nicht-Einwilligung erhalten sie kein Angebot“ etc.)
- Hinweis auf besondere Kategorien personenbezogener Daten: Ihr müsst euch für den Fall, dass ihr besonders schützenswerte Daten nach § 4 Abs. 1) KDG verarbeitet, explizit nochmal auf diese beziehen.
- Jederzeitiges Widerrufsrecht: Der Betroffene muss jederzeit und so einfach wie die Einwilligungserteilung diese Widerrufen können.

- Personen, die das 16. Lebensjahr noch nicht vollendet haben: Die Einwilligung muss durch den Personensorgeberechtigten für das jeweils konkrete Bild erteilt werden.

Muster Einwilligung für Bilder[10]

Name und Anschrift der Organisation: _____

Wir möchten im Rahmen unserer Tätigkeit zu Zwecke der Öffentlichkeitsarbeit aufgenommene Bilder im Rahmen Bezeichnung der Maßnahme in Pressemitteilungen, sozialen Medien, Printmedien und auf unserer Website veröffentlichen. Damit diese Verarbeitung rechtskonform ist, bitten wir Sie/dich im Folgenden um ihre/ deine Einwilligung.

Einwilligung

Mit der Unterschrift bestätige ich, dass ich in die Veröffentlichung von Bildern, die mich als Person zeigen, einwillige. Ich willige ein, dass die Bilder in folgenden Medien veröffentlicht werden dürfen:

- Pressemitteilungen des Veranstalters ☐
- Soziale Medien ☐
- Printmedien (Pfarrbrief, Zeitschrift etc.) ☐
- Homepage ☐

Mir ist bewusst, dass meine Daten öffentlich eingesehen werden können. Trotz aller möglichen Maßnahmen ist es möglich, dass, insbesondere bei der Veröffentlichung im Internet, meine Daten von Dritten weiterverwendet und weitergegeben werden können.

Diese Einwilligung erfolgt auf freiwilliger Basis und kann jederzeit widerrufen werden. Für einen Widerruf wenden Sie sich/ wende du dich bitte schriftlich an den oben genannten Verantwortlichen oder per Mail an Kontaktmailadresse Ein Widerruf berührt die Rechtmäßigkeit der bis dato stattgefundenen Verarbeitung nicht. Die Ausübung von anderen Datenverarbeitungen durch den Verantwortlichen wird durch eine Nicht-Einwilligung nicht beeinträchtigt.

[10] Eine digitale Version findest du unter: https://www.bdkj-dv-koeln.de/material/datenschutz/

Diese Einwilligung gilt bis zum Zeitpunkt an dem Sie/du diese Einwilligung widerrufen.

Sie haben/ Du hast entsprechend dem KDG auch ihre/ deine bestehenden Betroffenenrechte. Darunter fallen das Recht auf Auskunft, das Recht auf Berichtigung, das Recht auf Widerruf, das Recht auf Löschung und Einschränkung sowie das Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde. Die für den Name der Organisation zuständige Aufsichtsbehörde finden sie unter https://www.katholisches-datenschutzzentrum.de/. Für eine Wahrung der genannten Rechte wenden Sie sich bitte an den Verantwortlichen.

Datum Name Unterschrift

Checkliste: Was ist zu tun?

Nach dem wir euch nun einen Überblick über die einzelnen Regelungen gegeben haben, wollen wir euch eine Checkliste als Hilfestellung geben, an der ihr euch entlanghangeln könnt, um bei euch vor Ort die Datenschutzregelungen zu erfüllen:

- Brauchen wir einen Datenschutzbeauftragten?
- Haben wir eine Datenschutzerklärung auf der Homepage?
- Welche Daten fragen wir wo auf der Homepage ab und brauchen wir diese jeweils?
- Wie wollen wir mit privaten bzw. verbandlichen Geräten umgehen?
- Welche Programme nutzen wir und brauchen wir für die Datenverarbeitung?
- Welche Cloud nutzen wir und ist diese Datenschutzkonform?
- Welchen Messenger nutzen wir wie zukünftig?
- Wollen wir eine generelle Einwilligung für die Veröffentlichung von Bildern unserer Leiter*innen bzw. Mitarbeitenden?
- Wer Verarbeitet für uns Daten und haben wir einen Auftragsverarbeitungsvertrag geschlossen?
- Erstellt ein Verarbeitungsverzeichnis.

Fragen die ihr euch bei jeder Veranstaltung neu stellen müsst:

- Welche Informationen brauchen wir für die Durchführung der jeweiligen Maßnahme?
- Wer braucht welche dieser Informationen?
- Wurden die nötigen Einwilligungen zur Verarbeitung eingeholt?
    - Veröffentlichung von Bildern
    - Generelle Datenverarbeitung
    - Versendung von Newslettern bzw. Werbung

Impressum

Herausgeber
Bund der Deutschen Katholischen Jugend Erzdiözese Köln, Steinfelder Gasse 20-22, 50670 Köln, info@bdkj-dv-koeln.de

Redaktion
Volker Andres, BDKJ-Diözesanvorsitzender (V.i.S.d.P.)
Andreas Kayser, imatec GmbH

Quellen
Imatec GmbH
Katholisches Datenschutzzentrum
Kirchliches Datenschutzgesetz (KDG)

Korrektur
Kevin Kiewell

Haftungsausschluss
Die Handreichung haben wir mit bestem Wissen und Gewissen erstellt. Dennoch übernehmen wir keine Haftung, falls sich Fehler eingeschlichen haben oder sich gesetzliche Regelungen ändern sollten.