Checkliste zum kirchlichen Datenschutz

Am 24.05.2018 wird das neue Gesetz über den kirchlichen Datenschutz (KDG) in Kraft treten. Damit wird die europäische Datenschutzgrundverordnung (DSGVO) in kirchliches Recht überführt.

Jede natürliche oder juristische Person, Behörde Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, ist ein sog. Verantwortlicher im Sinne des Datenschutzes. Dieser ist insb. dafür verantwortlich, dass er die Anforderungen des KDG einhält.
Diese Checkliste dient dazu, für die Verantwortlichen die wesentlichen Anforderungen exemplarisch zusammenzustellen, im Umgang mit der Verarbeitung personenbezogener Daten Handlungssicherheit zu bieten und einen Leitfaden aufzuzeigen, anhand dessen jeder, der mit der Verarbeitung personenbezogener Daten betraut ist, selbständig umgehen kann.
Zu beachten ist, dass sich der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheiden kann. In dieser Checkliste wird deshalb der vereinfachte Regelfall angenommen. Möglichkeiten zur Vertiefung und Auskunft finden Sie am Ende des Textes.

1. Frage: Habe ich mit personenbezogenen Daten zu tun?

☐ Ja
☐ Nein

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Personenbezogene Daten können sowohl in Papierform oder in elektronischer Form vorliegen.

Diese sind zum Beispiel:

- Name
- Adressdaten
- Vertragsstammdaten
- Daten zu Bank- oder Kreditkartenkonten
- IT-Nutzungsdaten (z. B. Verbindungsdaten, Logging-Informationen)
- Kennnummern
- Standortdaten
- besondere Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann
- Bilder, Videoaufnahmen

Wenn personenbezogene Daten auf Papier oder elektronisch verarbeitet werden, müssen die nachstehenden Fragen beantwortet werden.

2. Frage: Wenn ich personenbezogene Daten erhebe oder verarbeite bzw. nutze, dann mache ich das auf welcher Rechtsgrundlage?

- ☐ Rechtsgrundlage im KDG oder in anderen Gesetzen oder Verordnungen.
- ☐ Einwilligungserklärung erforderlich.
- ☐ Wenn keine Rechtsgrundlage, dann keine Datenverarbeitung zulässig.

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn eine Rechtsgrundlage hierfür gegeben ist.

Diese Rechtsgrundlage kann sich aus dem KDG selbst ergeben oder aus anderen kirchlichen oder staatlichen Rechtsvorschriften (§ 6 Abs. 1 lit. a KDG).

Vor jeder Verarbeitung personenbezogener Daten ist daher zu prüfen, ob eine Rechtsgrundlage gegeben ist.

Beispiel:
Sie schließen mit einem Mieter einen Mietvertrag. Sie dürfen zum Zweck der Verwaltung und Durchführung des Mietverhältnisses die Daten aufgrund des Mietvertrages speichern.

Liegt keine (kirchen-)gesetzliche Rechtsgrundlage vor, kann eine Datenverarbeitung nur erfolgen, wenn der Betroffene in die Datenverarbeitung eingewilligt hat (§ 6 Abs. 1 lit. b KDG i.V.m. § 8 KDG).

Beispiel:
Sie wollen die Daten eines Spenders in eine Spenderliste aufnehmen, damit der Spender regelmäßig über neue Spendenprojekte informiert wird. Dies dürfen Sie nur tun, wenn der Spender ausdrücklich darin eingewilligt hat.

3. Frage: Wenn ich eine Einwilligungserklärung benötige, wie muss diese aussehen?

- ☐ Einwilligungserklärung liegt vor.

Die Einwilligungserklärung muss bestimmten gesetzlichen Anforderungen entsprechen, insbesondere muss sie

- auf den Zweck der Verarbeitung hinweisen (siehe 6. Frage),
- auf die Folgen einer Verweigerung hinweisen,
- freiwillig erteilt werden, worauf in der Einwilligung hinzuweise ist,
- jederzeit widerrufen werden können, worauf in der Einwilligung hinzuweisen ist,
- muss grundsätzlich schriftlich erteilt werden.

Mustertext für Einwilligungserklärung:

> Die Einwilligung ist jederzeit für die Zukunft widerruflich. Der Widerruf ist schriftlich beim _____ einzulegen.
> Bei Druckwerken ist die Einwilligung jedoch nicht mehr widerruflich, sobald der Druckauftrag erteilt ist. Gleiches gilt auch für bereits weitergegebene Daten, Fotos etc. (auch in digitaler Form).
> Wird die Einwilligung nicht widerrufen, gilt sie zeitlich unbeschränkt, d.h. auch über die Beendigung der Zugehörigkeit zur _____ hinaus.

Bei Veröffentlichung eines Gruppenfotos führt der spätere Widerruf einer einzelnen Person grundsätzlich nicht dazu, dass das Bild entfernt werden muss.
Mir wurde erläutert, dass die Erklärung meines Einverständnisses völlig freiwillig ist. Aus der Nichterteilung oder dem Widerruf der Einwilligung entstehen keine Nachteile.

4. Frage: Was muss ich mit der Einwilligungserklärung machen?

Die Einwilligungserklärung muss dokumentiert werden, damit im Zweifel der Nachweis erbracht werden kann, dass die betroffene Person in die Datenverarbeitung eingewilligt hat. Idealerweise haben Sie die Einwilligung in Papierform aufgebhoben.

- ☐ Einwilligungserklärung ist dokumentiert.

5. Frage: Was muss ich tun, wenn die betroffene Person der Datenverarbeitung widerspricht?

Wenn die Datenverarbeitung aufgrund einer Einwilligungserklärung erfolgt, dürfen Sie die Daten ab Zugang des Widerrufs nicht weiter verarbeiten.

Wenn die Datenverarbeitung auf einer gesetzlichen Grundlage oder auf Grundlage des KDG erfolgt, dürfen die Daten in diesem Rahmen weiter verarbeitet werden.

- ☐ Einwilligungserklärung wird gelöscht, wenn Widerruf eingegangen ist.

6. Frage: Zu welchem Zweck werden die personenbezogenen Daten erhoben und verarbeitet?

Bereits vor der Datenerhebung muss feststehen bzw. muss festgelegt werden, welche Daten für welche Zwecke verarbeitet werden sollen.

Zwecke können dabei beispielsweise sein:
- Bewerberdaten zum Zweck der Durchführung eines Bewerbungsverfahrens verarbeiten
- Adressdaten zum Zweck der Organisation und Durchführung eines Kurses verarbeiten
- etc.

Die personenbezogenen Daten dürfen nur für die vor Erhebung festgelegten Zwecke verwendet werden.

- ☐ Die Daten werden nur zu dem vorher festgelegten Zweck verwendet.

7. Frage: Was muss ich tun, wenn ich die Daten zu einem anderen Zweck verwenden will?

Grundsätzlich dürfen personenbezogene Daten nur zu dem Zweck verarbeitet werden, zu dem sie erhoben werden.

Das KDG sieht jedoch einen engen Katalog an Ausnahmetatbeständen vor, die eine Datenverarbeitung auch zu einem anderen Zweck erlauben. Wenn Sie hier

- ☐ Grundsätzlich nicht erlaubt.
- ☐ Ggf. liegen Ausnahmevorschriften vor.
- ☐ Einwilligung wurde erteilt.
- ☐ Datenschutzbeauftragter ist einbezogen.

unsicher sind, wenden Sie sich bitte vertrauensvoll an Ihren zuständigen betrieblichen Datenschutzbeauftragten.

Gegebenenfalls kann es auch hier erforderlich sein, eine Einwilligungserklärung einzuholen. Hierzu verfahren Sie wie oben beschrieben.

Beispiel:
Sie dürfen die Anmeldedaten von Teilnehmern eines von Ihnen angebotenen Kurses an zum Zweck der Organisation des Kurses speichern und verarbeiten. Sie dürfen die Anmeldedaten aber nicht verwenden, um den Teilnehmern weitere Kursangebote zu schicken, wenn diese nicht explizit darin eingewilligt haben.

8. Frage: Darf ich alle personenbezogenen Daten erheben und verarbeiten, die mich interessieren?

- ☐ Es werden nur die Daten verarbeitet, die zwingend für den Zweck erforderlich sind.

Aus dem Gebot der Datensparsamkeit folgt, dass nur die personenbezogenen Daten erhoben und verarbeitet werden dürfen, die zwingend für den festgelegten Zweck erforderlich sind. Eine „Vorratsdatenspeicherung“ ist nicht zulässig.

Wenn Sie Daten erheben, müssen Sie bereits darauf achten, nur die Daten zu erheben, die Sie zwingend benötigen.

Achten Sie insbesondere auf Folgendes:

- Bei Anmeldeformularen sind Pflichtangaben und freiwillige Angaben zu kennzeichnen. Die freiwilligen Angaben sind so sparsam wie möglich vorzusehen.
- Notieren Sie nur die Angaben, die Sie für eine Rückantwort oder eindeutige Zuordnung benötigen.

9. Frage: Darf ich personenbezogene Daten an Dritte weitergeben?

- ☐ Die Weitergabe ist aufgrund gesetzlicher Anforderungen zulässig.
- ☐ Wenn die Datenweitergabe nicht zulässig ist, dürfen die Daten nicht weitergegeben werden.
- ☐ Datenschutzbeauftragter ist einbezogen.
- ☐ Die Praxis der Datenweitergabe ist überprüft und geregelt.

Das hängt zunächst davon ab, an wen die Daten weitergegeben werden sollen. Je nach Empfänger gibt es unterschiedliche gesetzliche Anforderungen.

a) Wenn die Daten an eine kirchliche oder öffentliche Stelle weitergegeben werden sollen, dann ist dies nur zulässig, wenn die Weitergabe zur Erfüllung von Aufgaben Ihrer Dienststelle oder zur Erfüllung von Aufgaben der anderen Dienststelle erforderlich ist und dafür eine Rechtsgrundlage nach § 6 KDG vorliegt. (§ 9 Abs. 1 KDG)

b) Wenn die Daten an eine nicht kirchliche oder nicht öffentliche Stelle weitergegeben werden sollen, dann ist dies nur zulässig, wenn die Weitergabe zur Erfüllung von Aufgaben Ihrer Dienststelle erforderlich ist, dafür eine Rechtgrundlage nach § 6 KDG vorliegt sowie der Empfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Offenlegung hat, es sei denn, dass Grund zu der

Annahme besteht, dass durch die Offenlegung die Wahrnehmung des Auftrags der Kirche gefährdet würde. (§ 10 Abs. 1 KDG)

Die rechtliche Einordnung kann im Einzelfall schwierig sein. Wenn Sie hier unsicher sind, wenden Sie sich bitte vertrauensvoll an Ihren zuständigen betrieblichen Datenschutzbeauftragten.

Beispiel:
Sie dürfen die Anmeldedaten von Teilnehmern eines von Ihnen angebotenen Kurses an die Buchhaltung zum Zweck der Abwicklung des Zahlungsvorganges bzgl. der Kursgebühr weitergeben. Sie dürfen die Anmeldedaten aber nicht an eine andere Dienststelle weitergeben, die die Daten für eigene Werbezwecke nutzen will.

Bedenken Sie bitte auch Folgendes:

Wenn Sie Daten zulässigerweise an andere Kollegen oder Dienststellen weitergeben, muss immer sichergestellt sein, dass die Daten im Fall eines Löschbegehrens oder bei Ablauf der Aufbewahrungsfrist an allen Stellen auch tatsächlich gelöscht werden.

Prüfen Sie daher Folgendes:
- Auf welchem Weg gebe ich Daten an andere weiter (z. B. per E-Mail)?
- Wo werden die Daten bei mir und bei den anderen gespeichert?
- Ist sichergestellt, dass die Daten an allen Stellen auch tatsächlich gelöscht werden können?
- Ist dies nicht der Fall, ist zu klären, ob die Praxis der Datenweitergabe so fortgeführt werden kann oder wie die Löschanforderungen sichergestellt werden können.

10. Frage: Was ist zu tun, wenn ich personenbezogene Daten an einen Dritten übermitteln muss, weil dieser für mich Dienstleistungen erbringt, z. B. eine Druckerei oder ein Scandienstleister?

- ☐ Vertrag zur Auftragsverarbeitung ist geschlossen.
- ☐ Datenschutzbeauftragter ist einbezogen.

Wenn der Dritte die personenbezogenen Daten in Ihrem Auftrag verarbeitet (z. B. eine Druckerei druckt in Ihrem Auftrag Briefe mit Adressdaten), handelt es sich höchstwahrscheinlich um einen sog. Auftragsverarbeiter. In solchen Fällen ist zwingend ergänzend zu dem Dienstleistungsvertrag ein Vertrag zur Auftragsverarbeitung abzuschließen.

Praxishinweise:
- Im Einzelfall kann es schwierig sein festzustellen, ob Auftragsverarbeitung vorliegt. Bitte scheuen Sie sich nicht, Ihren betrieblichen Datenschutzbeauftragten zu fragen.
- Es ist ein Mustervertrag zu verwenden, den Sie bei Ihrem betrieblichen Datenschutzbeauftragten erhalten.

11. Frage: Ich muss Daten ins Ausland übermitteln – was ist dabei zu beachten?

- ☐ Datenschutzbeauftragter ist einbezogen.

Jede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder an eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn die gesetzlichen Vorgaben eingehalten werden. (§ 39 KDG)

Stellen Sie sich diese Frage bitte insbesondere dann, wenn:

- Daten in einer Cloud gespeichert werden sollen.
- Daten ins Ausland übermittelt werden sollen, weil z. B. der Dienstleister seinen Sitz im Ausland hat.

Die rechtliche Einordnung kann im Einzelfall schwierig sein. Wenden Sie sich bitte in jedem Fall an Ihren zuständigen betrieblichen Datenschutzbeauftragten.

12. Frage: Darf in meiner Abteilung jeder auf die personenbezogenen Daten zugreifen?

- ☐ Es ist sichergestellt, dass Unberechtigte nicht auf die Daten zugreifen können.

Der Grundsatz der Integrität und Vertraulichkeit verlangt, dass personenbezogene Daten nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Es ist daher sicherzustellen, dass Unberechtigte nicht auf die Daten zugreifen können.

Darauf ist insbesondere zu achten:

- Daten müssen z. B. durch Passwörter geschützt werden.
- Es gibt Rollen- und Berechtigungskonzepte, die die Zugriffe auf Daten regeln.
- Papierakten sind in verschlossenen Büros bzw. verschlossenen Schränken aufzubewahren.
- Gruppenablagen sind nur für einen bestimmten festgelegten Nutzerkreis freigeschalten.

13. Frage: Wie lange darf ich personenbezogene Daten speichern?

- ☐ Es sind gesetzliche Regelungen einzuhalten.
- ☐ Es ist ein Aufbewahrungs- und Löschkonzept festgelegt.

Sie dürfen personenbezogene Daten, die die Identifizierung der betroffenen Personen ermöglichen, nur so lange speichern, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. (§ 7 Abs. 1 lit. e KDG)

Es hängt daher von dem jeweils von Ihnen festgelegten Zweck ab, wie lange die Daten gespeichert werden dürfen.

Überlegen Sie sich daher bitte folgendes:

- Gibt es gesetzliche Regelungen, die mich zwingen, Daten für einen bestimmten Zeitraum zu speichern? Diese sind einzuhalten.
- Welche betrieblichen Erfordernisse habe ich unter Umständen? Diese sind konkret zu benennen und zu dokumentieren.

- Ist zu erwarten, dass die betroffenen Personen Ansprüche geltend machen können und für welchen Zeitraum ist dies zu erwarten? Dies ist konkret zu benennen und zu dokumentieren.
- Im Ergebnis ist daraus ein Konzept zu Aufbewahrungs- und Löschfristen zu entwickeln. Für diese Aufgabe berät und unterstützt der betriebliche Datenschutzbeauftragte.

14. Frage: Was ist zu tun, wenn die Aufbewahrungsfristen abgelaufen sind?

Nach Ablauf der Aufbewahrungsfristen sind die Daten zu löschen.

Dabei ist die Kirchliche Archivordnung zu beachten, auf deren Grundlage im Einzelfall ein physisches Löschen von Daten entfällt.

Wenden Sie sich daher bei Fragen gerne an das Archiv.

- ☐ Die personenbezogenen Daten sind gelöscht oder an das Archiv übermittelt.

15. Frage: Was mache ich, wenn eine betroffene Person die Auskunft über Berichtigung oder Löschung von personenbezogenen Daten verlangt?

Das KDG sieht umfangreiche Betroffenenrechte vor.

Solange noch keine einheitlichen Prozesse zur Wahrnehmung von Betroffenenrechten vorliegen, wenden Sie sich bitte bei derartigen Ersuchen an Ihren zuständigen betrieblichen Datenschutzbeauftragten.

- ☐ Datenschutzbeauftragter ist einbezogen.

16. Frage: Muss ich darüber informieren, was mit den personenbezogenen Daten passiert?

Das KDG sieht vor, dass der Verantwortliche die betroffene Person über bestimmte Modalitäten der Datenverarbeitung informieren muss. Zumindest muss der Verantwortliche darauf hinweisen, wo die Informationen leicht zugänglich sind (z.B. Homepage, Vertragsanlage). Das Gesetz sieht hierzu detaillierte Regelungen sowie Ausnahmen vor. (§§ 15, 16 KDG)

- ☐ Informationen sind erteilt.
- ☐ Datenschutzbeauftragter ist einbezogen.

Beispiele:
- Wenn personenbezogene Daten über eine Webseite erhoben werden (z. B. über ein Anmeldeformular), ist auf der Webseite über die Modalitäten der Datenverarbeitung zu informieren. Dies erfolgt im Rahmen sog. Datenschutzerklärungen.
- Werden Einwilligungserklärungen eingeholt, wird in diesem Rahmen über die Modalitäten der Datenverarbeitung informiert.

Die rechtliche Einordnung kann im Einzelfall schwierig sein. Wenden Sie sich bitte in jedem Fall an Ihren zuständigen betrieblichen Datenschutzbeauftragten.

17. Frage: Ich möchte eine Videoüberwachung durchführen – darf ich das?

- ☐ Datenschutzbeauftragter ist einbezogen.

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie a) zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder b) zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. (§ 52 Abs. 1 KDG)

Die rechtliche Einordnung kann im Einzelfall schwierig sein. Wenden Sie sich bitte in jedem Fall an Ihren zuständigen betrieblichen Datenschutzbeauftragten.

18. Frage: Ich habe gehört, dass WhatsApp im dienstlichen Kontext nicht mehr genutzt werden darf – warum ist das so?

- ☐ WhatsApp ist auf dienstlichen Endgeräten nicht installiert.
- ☐ WhatsApp auf privaten Smartphones o.ä. wird nicht zur dienstlichen Kommunikation genutzt.

WhatsApp verfügt über eine nicht datenschutzgerechte Anbindung an Facebook. Darüber hinaus findet die Speicherung der Verbindungsdaten außerhalb des Bereichs der EU bzw. des Europäischen Wirtschaftsraumes (EWR) statt, was datenschutzrechtlich nur unter ganz engen Voraussetzungen zulässig ist. Facebook wiederum steht im Verdacht, die von seinen Nutzern übermittelten Daten in einer Weise zu vermarkten, wie sie von den Nutzern nicht gewünscht wird. Der Diözesandatenschutzbeauftragte für die bayerischen (Erz-)Diözesen hat daher entschieden, dass die Verwendung eines Messangerdienstes auf dienstlichen Endgeräten untersagt ist, soweit eine physikalische Datenspeicherung außerhalb des Gebiets des EWR und der Schweiz stattfindet oder keine Punkt-zu-Punkt-Verschlüsselung genutzt wird.

Diese Voraussetzungen erfüllt WhatsApp nicht. Daher darf WhatsApp nicht im dienstlichen Kontext verwendet werden.

Was ist zu tun:

- Sofern Sie WhatsApp auf einem dienstlichen Endgerät nutzen, müssen Sie die App löschen.
- Sofern Sie WhatsApp auf Ihrem privaten Smartphone o.ä. nutzen, dürfen Sie WhatsApp nicht für dienstliche Kommunikation nutzen.

Andere Messangerdienste können u. U. genutzt werden, sofern die vorgenannten Vorgaben eingehalten werden. Bei Fragen hierzu wenden Sie sich bitte an Ihren betrieblichen Datenschutzbeauftragten.

19. Frage: Müssen bestimmte Datenschutzverletzungen / Vorfälle gemeldet werden?

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z.B. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Daten) so bestehen, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt, gesetzliche Meldepflichten binnen 72 Stunden. (§ 33 KDG)

Was ist zu tun:

Solange noch kein einheitlicher Meldeprozess vorliegt, wenden Sie sich bitte bei derartigen Vorfällen – auch wenn Sie ggf. über die Notwendigkeit der Meldung im Unklaren sind – unverzüglich an Ihren zuständigen betrieblichen Datenschutzbeauftragten.

Ich habe noch weitere Fragen – an wen kann ich mich wenden?

Sofern anhand dieser Checkliste aufkommende Fragestellungen nicht erschöpfend beantwortet werden können oder wenn darüber hinausgehende Fragestellungen bestehen, wenden Sie sich bitte an Ihren zuständigen betrieblichen Datenschutzbeauftragten.

Wenn Sie nach Durchsicht der Checkliste feststellen, dass für bestimmte Datenverarbeitung ein Anpassungsbedarf besteht, wenden Sie sich auch dann bitte gerne an Ihren zuständigen betrieblichen Datenschutzbeauftragten. Dieser berät Sie gerne.

Wenn Sie nicht wissen, wer der für Sie zuständige betriebliche Datenschutzbeauftragte ist, wenden Sie sich an Ihren Dienststellenleiter oder an die Datenschutzaufsicht. Die Datenschutzaufsicht hält eine Liste aller betrieblichen Datenschutzbeauftragten vor. Sie erreichen die Datenschutzaufsicht unter folgenden Kontaktdaten:

Datenschutzstelle der Erzdiözese München und Freising
Der Diözesandatenschutzbeauftragte Herr Jupp Joachimski
Kapellenstr. 4
80333 München
Telefon: 089 2137-1796
JJoachimski@eomuc.de

Vertiefende Informationen zum kirchlichen Datenschutz, insbesondere KDG-Praxishilfen und weiteren Praxishilfen zu Ihrer Unterstützung können Sie folgendem Link entnehmen:
https://www.erzbistum-muenchen.de/ordinariat/generalvikar/datenschutzstelle