Datenschutz im Ehrenamt

Datenschutz allgemein

Datenschutz bedeutet den **Schutz persönlicher Daten** und damit den Schutz der Person zur Wahrung des Persönlichkeitsrechts. Dabei geht es um sogenannte personenbezogene Daten.
Diese personenbezogenen Daten sind alle Informationen über eine bestimmte oder bestimmbare Person, wie z.B. Name, Geburtstag, Adresse, Aussehen, usw. und werden somit fast überall erfasst. Diese Daten müssen mit Vorsicht behandelt werden. Noch sensibler sind die sogenannten besonderen Arten der personenbezogenen Daten. Diese sind noch intimer und deshalb besonders zu schützen. Diese Daten sind Informationen über z.B. den Gesundheitszustand, usw.. Über solche Informationen soll meistens nur ein kleiner, vertraulicher Kreis informiert sein, weshalb sie besonders vorsichtig behandelt werden müssen.

Gesetzliche Grundlagen

Im Jahr 2018 trat in Europa die Datenschutz Grundverordnung (EU-DSGVO) in Kraft. Diese regelt den Datenschutz im weltlichen Bereich. Den Kirchen steht jedoch das Recht zu, eigene Regelungen hierüber zu erlassen. Diese Regelungen finden sich im **Gesetz über den Kirchlichen Datenschutz** (KDG). Das KDG ist hierbei auf alle kirchlichen Rechtsträger nach § 3 KDG anwendbar. Dabei ist das KDG den staatlichen Regelungen nachgebildet und trat am 24.05.2018 in allen Diözesen wortgleich in Kraft.

Das KDG gilt dabei **für alle kirchlichen Einrichtungen und Gruppierungen** und für hauptamtliche, aber auch ehrenamtliche Mitarbeiterinnen und Mitarbeiter.
Beispiele für die betroffenen Institutionen sind etwa kirchliche Einrichtungen wie KiTas und Büchereien, aber auch Gruppierungen wie Chöre oder Messdiener und auch für Krankenpflege- und andere Vereine, die kirchlich anerkannt sind.
Somit ist ganz gleich, wie und wo eine Tätigkeit im kirchlichen Bereich ausgeführt wird, sobald dabei Daten erfasst und verarbeitet werden, gilt das KDG.

Verantwortliche Stelle und Aufsichtsbehörden

Damit der Datenschutz auch umgesetzt wird, muss es Verantwortliche geben, auf die im Zweifel zurückgegriffen werden kann, als auch eine Kontrolle, zur Überwachung der Tätigkeiten. Verantwortlich für den Datenschutz ist grundsätzlich jeder. Das Gesetz definiert als Verantwortlichen denjenigen, der über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.
In Gemeinden ist dies der leitende Pfarrer, gemeinsam mit dem Kirchengemeinderat, bei Vereinen der Vorstand, usw.
Jedoch ist auch die jeweilige Einrichtungs- oder Gruppenleitung selbstverständlich dafür verantwortlich, dass in ihrem Zuständigkeitsbereich der Datenschutz eingehalten wird und die Mitarbeiter oder Mitglieder informiert und verantwortungsbewusst sind.

Damit die Verantwortung jedem bewusst ist, müssen Ehrenamtliche, die mit personenbezogenen Daten arbeiten eine **Verpflichtungserklärung** unterzeichnen, in der sie sich zum rechtmäßigen, verantwortungsbewussten Umgang mit den Daten verpflichten. Diese Erklärung wird dann in der Gemeinde oder bei der entsprechenden Stelle aufbewahrt und ist rechtlich bindend.

Zur Kontrolle der Einhaltung des KDG, aber auch zur Hilfestellung bei Fragen gibt es zudem die **Aufsichtsbehörde**. Diese kontrolliert und überprüft den Datenschutz. Hierfür ist die Aufsicht berechtigt, regelmäßig Kontrollen in den Einrichtungen durchzuführen. Weiterhin dient die Aufsichtsbehörde auch zur Hilfe bei Fragestellungen und als Beschwerdestelle für Betroffene. Möchte ein Betroffener eine Beschwerde einreichen, kann er dies entweder bei der betrieblichen Datenschutzstelle oder bei der diözesanen Datenschutzaufsicht tun.

Der Aufsichtsbehörde müssen auch sogenannte **Datenpannen** gemeldet werden, also jede Verletzung der Datenschutzvorschriften. Diese müssen innerhalb von 72 Stunden bei der Behörde gemeldet werden.

Datenpannen sind:

- Diebstahl oder der Verlust von Daten und Datenträgern mit personenbezogenen Daten (verlorener USB-Stick, Hackerangriff, …)
- Unerlaubte oder ungewollte Veröffentlichungen von personenbezogenen Daten (Versand an die falsche Person, offene Mailverteiler, …)
- Sonstige Verletzungen von Rechten der Betroffenen

Die zuständige Datenschutzaufsicht für die Diözese Rottenburg-Stuttgart ist das

Katholische Datenschutzzentrum Frankfurt/M
Domplatz 3, 60311 Frankfurt
info@kdsz-ffm.de
Tel: 069 – 800 8718 800
Fax: 069 – 800 8718 815
https://www.kath-datenschutzzentrum-ffm.de/

Weiterhin sind Diözesen, Kirchengemeinden und Kirchenstiftungen auch kraft Gesetz dazu verpflichtet einen **betrieblichen Datenschutzbeauftragten** zu bestellen.

In der Diözese Rottenburg-Stuttgart ist dies die

Stabsstelle Datenschutz
Bischöfliches Ordinariat, Postfach 9
72101 Rottenburg
Tel: 07472 169-890
Fax: 07472 169-83890
E-Mail: datenschutz@bo.drs.de

Diese Datenschutzstelle steht den Gemeinden und Einrichtungen, aber auch dem Einzelnen unterstützend zur Seite und hilft bei Fragen und Datenpannen.

Verarbeitung personenbezogener Daten

Eigentlich dürfen personenbezogene Daten nach dem Gesetz gar nicht verarbeitet werden. Die Verarbeitung ist nur dann erlaubt, wenn das **Gesetz eine Erlaubnis** erteilt oder der **Betroffene eingewilligt** hat.

Gesetzlich erlaubt ist die Verarbeitung dann, wenn ein Vertrag zwischen den Betroffenen und den Verantwortlichen entsteht, wie etwa ein Arbeitsvertrag, bei verbindlichen Anmeldungen zu Veranstaltungen, dem Beitritt zu Vereinen oder bei Meldungen zum Schutz der Allgemeinheit an Behörden wie beispielsweise an das Gesundheitsamt.

Dabei dürfen aber nur die jeweils für einen **eindeutig festgelegten Zweck** notwendigen Daten erhoben werden. Dass nur die **erforderlichen Daten** erhoben werden dürfen und unnötige Daten vernichtet werden müssen, ist der Grundsatz der **Datensparsamkeit**. Auch muss bei der Vernichtung von Daten darauf geachtet werden, dass diese unkenntlich gemacht werden und nicht mehr wiederhergestellt werden können. Dies bedeutet Papierdaten müssen vor dem Entsorgen geschwärzt oder geschreddert werden und digitale Daten endgültig vernichtet.

Einwilligung

Wie oben bereits genannt, kann auch eine Einwilligung des Betroffenen die Datenverarbeitung legitimieren.

Die Einwilligung muss hierbei bestimmte Kriterien erfüllen. Sie muss

- den **Zweck der Verarbeitung** erhalten,
- **freiwillig** erklärt werden
- auf nachvollziehbare Art und Weise erklärt werden (**Schriftform**)
- den deutlichen **Hinweis auf** das jederzeitige **Widerrufsrecht** enthalten.

Wenn diese Kriterien erfüllt sind und die Einwilligung nicht widerrufen wird, ist sie unbegrenzt gültig. Jedoch dürfen die Daten nur zu den formulierten Zwecken verwendet werden und nicht darüber hinaus.

Wird ein Widerruf abgegeben, dann betrifft dies nur die Verarbeitung in der Zukunft. Bereits veröffentlichte und nicht rückholbare Daten sind davon nicht betroffen, jedoch müssen veränderbare Medien, wie etwa der Internetauftritt angepasst und die Daten dort entfernt werden. Der Widerruf sollte dabei, aus Gründen der Dokumentation, ebenfalls immer schriftlich erfolgen.

Bei minderjährigen Personen unter sechzehn Jahren ist die Einwilligung der Eltern bzw. des Erziehungsberechtigten erforderlich.

Datensicherheit

Wichtiger Bestandteil des Datenschutzes ist die Sicherheit der personenbezogenen Daten. Dies bezieht sich vor allem auch auf die technischen Maßnahmen, die bei der Aufbewahrung und bei der Übermittlung getroffen werden müssen.
Papierdaten sollten grundsätzlich so aufbewahrt werden, dass sie vor dem Zugriff Unbefugter sicher sind, also möglichst in **verschließbaren Schränken**. Auch sollten Dokumente niemals offen und unbeaufsichtigt liegen gelassen werden.

Selbiges gilt für Daten in digitaler Form. **Geräte** und Speichermedien sollten immer mit einem **Passwort gesichert** sein und bestenfalls werden auch die einzelnen Dokumente und Ordner mit Passwörtern versehen. Dies ist insbesondere dann notwendig, wenn auf private PCs, die für ehrenamtliche Tätigkeiten genutzt werden, auch andere Personen, wie etwa Familienmitglieder, Zugriff haben.
Wichtig ist auch ein ausreichender Virenschutz, sowohl auf dem Computer selbst, als auch beispielsweise auf USB-Sticks und auch die Software von Geräten sollte immer auf dem aktuellsten Stand gehalten werden.

Bei der Speicherung von Daten in einer **digitalen Cloud** muss darauf geachtet werden, dass diese von einem **datenschutzkonformen Anbieter** ist. Relevant ist hierbei sowohl die Sicherheit, als auch der Sitz der Firma, dieser muss sich innerhalb Europas befinden.

Beim Versand von Daten oder der Kommunikation per E-Mail ist es notwendig einen verschlüsselten Anbieter zu nutzen der datenschutzkonform ist.
Bei der Kommunikation per E-Mail ist zudem zum Schutz der E-Mail Adressen erforderlich, dass E-Mails an mehrere Empfänger nie als offene **Verteiler** genutzt werden, sondern E-Mails immer **als Blindkopie** (BCC) versendet werden.
Gerade bei der Kommunikation per E-Mail ergibt sich eine weitere Gefahr durch SPAM-Mails. Mails von unbekannten Empfängern oder mit fragwürdigem Inhalt sollten sofort gelöscht werden, enthaltene Anhänge oder Links dürfen bei SPAM-Verdacht niemals geöffnet werden. Ist es unsicher, ob die Mail vom entsprechenden Absender kommt und der Inhalt evtl. doch relevant ist, sollte im Zweifel immer Rücksprache mit dem vermeintlichen Absender gehalten werden.

Grundstein zum Schutz von personenbezogenen Daten in digitaler Form ist immer ein sicheres Passwort. Passwörter sollten deshalb nicht personalisiert sein und keine zusammenhängende Kombination darstellen. Ein **sicheres Passwort** besteht nach heutigem Stand aus **mind. 12 unzusammenhängenden Zeichen** (Groß- und Kleinschreibung, Zahlen und Sonderzeichen). Passwörter sollten zudem regelmäßig erneuert werden.

Veröffentlichung von Daten

Die Veröffentlichung von personenbezogenen Daten ist nur mit der **Einwilligung der Betroffenen** zulässig. Gerade Internet und Social-Media Auftritte sind ein großes Datenloch, denn einmal ins Internet gestellt, ist es heutzutage beinahe unmöglich, Beiträge und alle deren Verknüpfungen und Verlinkungen wieder zu löschen. Und auch im Printbereich lassen sich einmal veröffentlichte Zeitungsartikel oder verteilte Flyer nicht mehr zurückholen. Es sollten deshalb **so wenig personenbezogene Daten veröffentlicht** werden **wie möglich**. Soll dies z.B. zu Werbezwecken doch geschehen, so muss die Einwilligung der Betroffenen vorliegen. Gerade bei Bildern sollten außerdem nie unvorteilhafte Aufnahmen veröffentlicht, sondern immer mit Bedacht gewählt werden.

Messenger-Dienste

Messenger-Dienste sind mittlerweile ein beliebtes Kommunikationsmittel. Leider sind gerade die bekannten Anbieter wie **WhatsApp** datenschutzrechtlich mangelhaft und deshalb zur Nutzung für **dienstliche Zwecke nicht zulässig**. Privates darf hierüber geklärt, nicht aber Informationen über das Ehrenamt ausgetauscht oder gar Daten verschickt werden.

Alternativen sind Anbieter die ihren Sitz in Europa haben und verschlüsselte Kommunikation anbieten. Außerdem ist erforderlich, dass diese so wenig Berechtigungen wir möglich über Zugriffe auf die Kontakt- oder Bilddaten des Telefons haben.

Empfehlungen für die Umsetzung

Datenschutzerklärung für die Homepage

Neben der Pflicht eines Impressums ist auch erforderlich, dass auf Internetseiten eine Datenschutzerklärung vorhanden ist. Ein Vergleich finden Sie auf der Homepage der Diözese Rottenburg-Stuttgart.

Verzeichnis über Verarbeitungstätigkeiten

Über die Verarbeitung von personenbezogenen Daten muss ein Verzeichnis angelegt werden. Dieses dient im Falle der Auskunftsanforderung eines Betroffenen als Nachweis. Entsprechende Muster erhalten Sie von der Stabsstelle Datenschutz.

Auskunftsrecht

Betroffene haben das Recht Auskunft über die Verarbeitung ihrer Daten zu verlangen. Diese muss mit einer Rückmeldefrist von vier Wochen erfolgen und jede Information, Verarbeitung sowie Aufbewahrungsfristen beinhalten.

Dokumentation der Datenschutzmaßnahmen

Sowohl Verpflichtungserklärungen als auch Einwilligungen, sowie interne Absprachen und Regelungen zum Datenschutz sollten schriftlich dokumentiert und aufbewahrt werden. Intern sollte zudem überprüft werden, wer Zugang zu welchen Daten hat und ob dies notwendig ist. Außerdem sollten regelmäßig die Aufbewahrungsfristen kontrolliert und gegebenenfalls Daten gelöscht werden.

Weitere Informationen

Weitere Informationen finden Sie unter:

- https://www.dbk.de/themen/kirche-staat-und-recht/datenschutz-faq/
- https://www.datenschutz-kirche.de/
- https://www.kath-datenschutzzentrum-ffm.de/
- Mitarbeiterportal der Diözese („Gruppe Stabsstelle Datenschutz“)