Katholisches Datenschutzzentrum

12 Punkte Maßnahmenplan bis Mai 2018

Vorbemerkung

Zum 24. Mai 2018 tritt das Gesetz über den Kirchlichen Datenschutz (KDG) in Kraft. Es wird die bisherige Anordnung über den kirchlichen Datenschutz (KDO) ablösen. In Anlehnung an die Europäische Datenschutzgrundverordnung (DS-GVO) gibt es weitreichende Änderungen, auf die sich kirchliche und caritative Einrichtungen bereits jetzt schon vorbereiten sollten.

1. Bestellung eines betrieblichen Datenschutzbeauftragten

Die Bestellung eines betrieblichen Datenschutzbeauftragten ist in § 36 KDG geregelt. Alle kirchlichen Diözesen, Kirchengemeinden und kirchliche Einrichtungen müssen unabhängig von der Zahl der Mitarbeitenden einen eigenen betrieblichen Datenschutzbeauftragten benennen (§ 36 Abs. 1 KDG). Andere Einrichtungen, wie etwa caritative Wohlfahrtsverbände, müssen einen betrieblichen Datenschutzbeauftragten benennen, wenn ihre Kerntätigkeit die Verarbeitung besonderer Kategorien von personenbezogenen Daten umfasst. Darüber hinaus ist ein betrieblicher Datenschutzbeauftragter zu benennen, wenn mindestens zehn Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind. Dazu zählen insbesondere auch die ehrenamtlichen Helfer.

2. Bestandsaufnahmen

Zur Identifizierung des Änderungsbedarfs ist es notwendig, dass eine Bestandsaufnahme aller Prozesse durchgeführt wird, in denen personenbezogene Daten verarbeitet werden. Nach § 3a KDO ist es bereits Pflicht, ein Verzeichnis aller Verfahren vorzuhalten, in denen automatisiert personenbezogene Daten verarbeitet werden. Dies kann als Grundlage in Kombination mit einem evtl. bestehenden Qualitätsmanagementsystem zur Eruierung der Prozesse herangezogen werden.

3. Überprüfung der Rechtsgrundlage

Der Grundsatz des Verbots mit Erlaubnisvorbehalt ist auch in dem neuen Gesetz verankert. Die Verarbeitung personenbezogener Daten darf nur dann erfolgen, wenn eine kirchliche Rechtsvorschrift oder eine andere gesetzliche Grundlage dieses erlaubt oder anordnet oder die betroffene Person in die Verarbeitung eingewilligt hat. Daher ist für alle Prozesse zu prüfen und zu dokumentieren, auf welcher Grundlage die Verarbeitung erfolgt.

4. Personenbezogene Daten von Kindern unter 16 Jahren

Im KDG sind für den Umgang mit personenbezogenen Daten von Kindern besondere Anforderungen gestellt. In § 8 Abs. 8 KDG werden die Anforderungen an die Einwilligungen bei Kindern beschrieben. Bis zum Inkrafttreten im Mai 2018 sollten alle Vorbereitungen zur Erfüllung der neuen Anforderungen umgesetzt sein.

5. Datenschutz durch Technikgestaltung (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default)

Das KDG stellt bestimmte Rahmenbedingungen auf, wie die Anforderungen einer Umsetzung zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu erfüllen sind. Die bereits genutzten Techniken sind nach diesen Gesichtspunkten zu überprüfen und für den Einsatz neuer Techniken ist sicherzustellen, dass die Anforderungen des Gesetzes berücksichtigt werden.

6. Verträge prüfen

Das KDG sieht Änderungen zu den Anforderungen an eine Auftrags(daten)verarbeitung vor. Die Pflichten des Auftragsgebers sowie des Auftragsnehmers werden erweitert. Bei der Bestandsaufnahme ist daher zu prüfen, ob alle Prozesse mit einer Auftragsverarbeitung vertraglich erfasst sind und ob die bisherigen Regelungen ausreichend sind. Für derzeit schon abgeschlossene Auftragsdatenverarbeitungen gilt gemäß § 57 Abs. 3 KDG eine Übergangsfrist bis zum 31.12.2019 zu der die Altverträge an die neue Rechtslage angepasst werden müssen.

7. Datenschutz-Folgenabschätzung

Die bisherige Vorabkontrolle wird durch die Datenschutz-Folgenabschätzung abgelöst. Im Gesetz (§ 35 KDG) sind konkrete Vorgehensweisen beschrieben. An eine durchgeführte Datenschutz-Folgenabschätzung kann sich eine Konsultation der zuständigen Aufsicht anschließen. Bis zur Inkrafttretung des Gesetzes ist ein Verfahren zu erstellen, wie eine Datenschutz-Folgenabschätzung ausgeführt wird und welche Dokumentationen verpflichtend sind.

8. Meldungen von Datenschutzvorfällen

Das KDG sieht in § 33 KDG vor, dass binnen 72 Stunden nach Bekanntwerden eines datenschutzrechtlichen Vorfalls, der eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt, der zuständigen Aufsicht eine Meldung zu machen ist. Für diese Vorgabe ist in den Einrichtungen ein Verfahren zu erstellen, welches sicherstellt, dass diese Meldung zeitgerecht umgesetzt werden kann.

9. Informations- und Betroffenenrechte umsetzen

Im neuen KDG werden die Informations- und Betroffenenrechte in den Fokus gerückt und gestärkt. Die Betroffenen sind künftig in transparenter Weise über die Verarbeitung ihrer Daten präzise, verständlich und in leicht zugänglicher Form zu informieren (§ 14 Abs. 1 bis 6 KDG). Die Rechte der Betroffenen, wie in den §§ 17 bis 25 KDG beschrieben, sind sicherzustellen. In den Einrichtungen sind daher Verfahren zu erarbeiten, welche die Informations- und Betroffenenrechte ab dem Inkrafttreten des Gesetzes im Mai 2018 gewährleisten.

10. Erweiterte Maßnahmen der Datenschutzaufsicht

Nach der neuen Gesetzgebung verfügt die zuständige Aufsicht über erweiterte Handlungsmöglichkeiten beim Umgang mit Verstößen gegen datenschutzrechtlichen Regelungen (§ 47 KDG). Neben der Beanstandung und Fristsetzung zur Behebung von Mängeln können nun Anordnungen zur Abwehr von Gefahren für personenbezogene Daten erlassen, Verarbeitungen verboten und Geldbußen verhängt werden. Die erweiterten Maßnahmen sind in einer internen Risikoeinschätzung der Einrichtungen zu beachten.

11. Haftung und Schadensersatz

Erstmals ist in § 50 KDG die zivilrechtliche Haftung für das Entstehen materieller und immaterieller Schäden zu Lasten der betroffenen Person geregelt. Die Feststellung einer Aufsichtsbehörde, eine Datenschutzverletzung habe objektiv vorgelegen, ist im Prozess vor Zivilgerichten bindend. Das Haftungs- und Schadensersatzrisiko ist im gesamtunternehmerischen Kontext zu berücksichtigen.

12. Umsetzung von Melde-, Konsultations- und Dokumentationspflichten

Zur Umsetzung der in dem Gesetz vorgegebenen Melde-, Konsultations- und Dokumentationspflichten sind in den Einrichtungen Verfahren zu entwickeln, die sicherstellen, dass die Pflichten umgesetzt und eingehalten werden.