Kirchliches Datenschutzgesetz KDG – Information Nr. 5 – April 2019

Sehr geehrte Damen und Herren,

mit unserer ersten Ausgabe in diesem Jahr möchten wir Sie mit aktuellen Themen und Entwicklungen zum Betrieblichen Datenschutz wieder informieren. Seit der letzten Ausgabe ist nicht nur viel Zeit vergangen, es haben sich auch einige Dinge weiterentwickelt, z.B. durch Inkrafttreten der KDG-DVO.

Wir bitten alle Empfänger, um interne Weiterverteilung dieser Informationen in Ihrem Bereich.

Über folgende Punkte werden wir Sie mit dieser aktuellen KDG-Info informieren:

- Erstkommunion - Hinweise zum Umgang mit dem Datenschutz im Rahmen der Vorbereitung und der Erstkommunionfeier
- Info zum Datenschutzmanagementprojekt - Aktueller Stand zur Erstellung der Verfahrensverzeichnisse
- Aktueller Stand zur Online-Schulung
- Informationsveranstaltungen zum Datenschutz
- KDG-DVO - Informationen zur neuen Durchführungsverordnung

Erstkommunion - Hinweise zum Umgang mit dem Datenschutz im Rahmen der Vorbereitung

Für die Erstkommunionvorbereitung und die anstehenden Erstkommunionfeiern haben wir als Anlage eine Handlungsempfehlung zum Umgang mit Fotos und ein Muster zur Anmeldung inkl. einer Datenschutzerklärung beigefügt.

[s. Anlagen: Erstkommunion Datenschutz_050419 V1.02.docx ; Handlungsempfehlung Kommunionfeier-Fotos_050419 V1.2.pdf]

Datenschutzmanagementprojekt

In Zusammenarbeit mit dem neuen Datenschutzbeauftragten für das Generalvikariat, wird das Thema Betrieblicher Datenschutz im Rahmen eines Projektes weiterentwickelt, mit dem Ziel ein Datenschutzmanagementsystem zu etablieren.

Aktuell wird der **Themenschwerpunkt „Verzeichnis von Verarbeitungstätigkeiten“** ***Kapitel 1, § 1 KDG-DVO*** bearbeitet und auf den Weg gebracht. Hierzu erarbeitet eine Unterarbeitsgruppe unter Beteiligung von Verwaltungsleitungen, ein Pilotverzeichnis für die Kirchengemeinden und Kirchengemeindeverbände. Ziel ist es ein Musterverzeichnis mit den Hauptprozessen zu erstellen, welches im Nachgang durch individuelle Prozesse je Kirchengemeinde / Rechtsträger ergänzt werden kann.

Auch mit dem gesamten Thema der Technischen und Organisatorischen Maßnahmen ***Kapitel 3 KDG-DVO***, wird sich das Projekt zum Datenschutzmanagement und die Arbeitsgruppe zum Datenschutz befassen. Ziel ist es, Sie zu unterstützen und zu beraten.

Weiterer Schwerpunkt wird die Weiterentwicklung von standardisierten Werkzeugen, Prozessen (z.B. Meldeverfahren gemäß § 33 KDG, Dokumenten und Formularen (auch themenbezogen Dokumente zur Firmung, etc.) sein, die den Arbeitsalltag der haupt- und ehrenamtlichen Mitarbeiterinnen und Mitarbeitern erleichtern sollen. In Vorbereitung ist z. B. ein Datenschutzhandbuch, welches die wesentlichen Regelungen zum Umgang mit Daten in allgemeiner Form und im Überblick beinhaltet.

In der Erstellung und kurz vor dem Versand, befindet sich ein Informationsblatt „Datenschutz und Datensicherheit in unseren Einrichtungen und Diensten", welches auf einen Blick die wichtigsten Punkte gemäß dem KDG beinhaltet. Dieses Informationsblatt mit Hinweisen auf das Grundwissen zum Datenschutz, Zuständigkeiten/Verantwortlichkeiten, die Schutzklassen und weiteres, kann sowohl als Aushang, als auch als Schreibtischunterlage in den Pastoralbüros und allen weiteren Einrichtungen genutzt werden. Blockweise mit je 25 Exemplaren wird ein erster Versand an die Gemeindeverbände, Kirchen-/Kirchengemeindeverbände voraussichtlich bis zu den Osterferien erfolgen.

[s. Anlage: Schreibtischunterlage-A2-SVBM-KDG_R.pdf]

Aktueller Stand der Online-Schulung zum Datenschutz

Passend zur neuen Durchführungsverordnung (DVO) zum Katholischen Datenschutzgesetz (KDG) ist die schon im letzten Jahr angekündigte Online-Schulung fertiggestellt worden.

Hinweise:

1. Diese Schulung darf derzeit ausschließlich von ehrenamtlichen Gremienmitgliedern und Mitarbeitenden genutzt werden, für die **keine** MAV zuständig ist (z.B. Leitende Mitarbeitende, Pfarrer, Kapläne, Diakone). Die notwendige MAV-Beteiligung für die übrigen Mitarbeitenden wird in Kürze eingeleitet.
2. Am Ende der Schulung können Sie sich ein Zertifikat erstellen und ausdrucken. Bitte bewahren Sie dieses Zertifikat zunächst noch selber auf. Noch haben wir nicht abschließend geklärt, wo diese Zertifikate auf Dauer aufbewahrt werden sollen.

Eine Anleitung und die entsprechenden Anmeldedaten zur persönlichen Registrierung und Durchführung der Schulung wird Ihnen schon mit dieser KDG-Info vorab zur Verfügung gestellt.

Der Link:	https://datenschutz.erzbistum-koeln.de/
Die Kennung:	datenschutz
Das Passwort:	FwDwF45xFY3
Anleitung:	https://www.erzbistum-koeln.de/presse_und_medien/internet/administration/datenschutzkurs/index.html

Informationsveranstaltungen zum Datenschutz

Gemeinsam mit dem betrieblichen Datenschutzbeauftragten des EGV, dem Sachverständigenbüro Mülot GmbH, werden noch in diesem Jahr Informationsveranstaltungen, ergänzend zu der Online-Schulung angeboten. Analog zu dem Format der aktuellen Veranstaltungen zur umsatzsteuerlichen Neuregelung des §2b UstG, werden wir an zentralen Standorten die Informationsveranstaltungen durchführen.

Termine und Veranstaltungsorte befinden sich in der Planung und Abstimmung. Sobald dieser Vorgang abgeschlossen ist, werden entsprechende Informationen umgehend veröffentlicht, so dass eine Anmeldung zur Teilnahme erfolgen kann.

KDG-DVO – Informationen zur neuen Durchführungsverordnung

Am 01.03.2019 ist die neue KDG-Durchführungsverordnung in Kraft getreten und wurde veröffentlicht. Die DVO enthält Konkretisierungen zum Katholischen Datenschutzgesetz (KDG).

Als Anlage haben wir Ihnen erneut die **KDG-DVO** und zusätzlich eine **Kurzinformation beigefügt**, die wir in Zusammenarbeit mit dem betrieblichen Datenschutzbeauftragten des EGV erstellt haben. Diese soll Ihnen unterstützend einen Überblick über die DVO verschaffen.

[s. Anlagen: KDG-DVO.pdf ; KDG-DVO Kurzinformation_080319 V1.0.pdf]

Ergänzend möchten wir noch folgende Begriffe näher erläutern. Sie werden feststellen, dass die einzelnen Kontrollen und Maßnahmen eng ineinandergreifen:

- **Zutrittskontrolle**

  Eine Zutrittskontrolle steuert den Zutritt von berechtigten Personen zu den für sie freigegebenen Bereichen in Gebäuden und Einrichtungen. Hierbei geht aus Sicht des Datenschutzes um Bereiche, die Datenverarbeitungsanlagen (Computer, Server, Festplatten, etc.) enthalten. Die Identitätsprüfung kann über Mitarbeiter, einen Sicherheitsdient oder über technische Kontrollsysteme (Chipkartensystem, Alarmanlagen, Absicherungen von Fenstern und Türen, etc.) erfolgen.
- **Zugangskontrolle**

  Die Zugangskontrolle verhindert die Nutzung der vorhandenen Datenverarbeitungsanlagen durch unbefugte Personen und verhindert die Nutzung des elektronischen Systems. Zur Sicherung gehören u.a. Passwortschutz (Benutzername und Passwort), PIN-Verfahren, SPAM-Filter und Virenscanner.
- **Zugriffskontrolle**

  Die Zugriffskontrolle regelt, dass ausschließlich befugte Personen Zugriff auf personenbezogene Daten, Programme und Dokumente erhalten und nutzen. Maßnahmen hierzu sind Regelungen, Richtlinien, Berechtigungskonzepte, sowohl organisatorische als auch technische Maßnahmen (Administratorenrechte, Schreib- und Leserechte), datenschutzkonforme Vernichtung von Daten (z. B. Löschung, Schreddern).
- **Transportkontrolle**

Unter dem Punkt Transportkontrolle versteht man die Gewährleistung und Sicherstellung einer sicheren Übertragung von personenbezogenen Daten, sowie beim Transport entsprechender Datenträger, dass unbefugte Personen nicht lesen, verändern und löschen können. Maßnahmen hierzu sind z. B. verschlüsselte Datenübermittlung, verschließbare Aufbewahrungsbehälter, Versand von Datenträger als Wertsendung.

- **Speicherkontrolle**

  Bei diesem Punkt geht es um die Verhinderung, unbefugten Personen die Dateneingabe, Kenntnisnahme, Veränderung oder Löschung von personenbezogenen Daten möglich zu machen. Auch hier geht es um personifizierten Zugriffsschutz u.a. bei zentralen und dezentralen Rechnern, Berechtigungskonzepte.

- **Weitergabekontrolle**

  Unter Weitergabekontrolle versteht man die technischen und organisatorischen Maßnahmen die verhindern, dass während des Transportes oder der Speicherung von personenbezogenen Daten auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden kann. In der Praxis betrifft das insbesondere Daten, die über Netzwerke fließen und per Email versandt werden, d.h. Protokollierung des Versands, Transportsicherungen, Verschlüsselung der Daten, Versand per Einschreiben und/oder Wertsicherung, getrennte Mitteilung des Kennworts zur Nutzung der Daten, usw.

- **Eingabekontrolle**

  Die Eingabekontrolle regelt, dass im Nachgang überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungsanlagen eingegeben, verändert oder gelöscht worden sind. Dies erfolgt durch automatische Protokollierung der Eingaben, die den bearbeiteten Datensatz, die Tätigkeit (Neuanlage, Veränderung, Löschung), Zeitpunkt und den Benutzer. Maßnahmen können sein, Unterweisungen an die berechtigten Personen, differenzierte Berechtigungen und Benutzerrechte, Einsatz von Softwareanwendungen mit Rollenkonzepten und/oder differenzierten Rechten.

- **Auftragskontrolle**

  Ein Auftrag liegt vor, wenn personenbezogene Daten durch Dritte verarbeitet werden (externe Dienstleister, externe Datenvernichtung, externe Mitarbeiter). In diesen Fällen ist darauf zu achten und sicherzustellen, dass personenbezogene Daten nur gemäß den Weisungen des Auftraggebers verarbeitet werden können. Dies vorgeschriebene Datenverarbeitung muss kontrolliert werden, dies ist über organisatorische und technische Maßnahmen sicherzustellen (Unterweisungen, vertragliche Regelungen, Verpflichtungserklärungen, Festlegung des Zugriffs, Einfordern von Nachweisen wie Datenschutz-/IT-Sicherheits-Zertifikate, etc.).

- **Verfügbarkeitskontrolle**

  Unter der Verfügbarkeitskontrolle versteht man den Schutz vor Zerstörung und Verlust von personenbezogenen Daten. Dies kann durch regelmäßige Datensicherungen, Virenschutz, Notfallkonzepte, Regelungen zum Umgang z.B. beim Emailversand.

- **Trennungsgebot**

  Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann durch logische oder physikalische Maßnahmen erfolgen.

Zum Tragen kommen hier Zweckbindungen/-formulierungen die im Verfahrensverzeichnis genau beschrieben werden, z. B. Zugriffsberechtigungen, Unterweisungen der Mitarbeiter zu diesen Sachverhalten, Funktionstrennungen (Verantwortung/Ausführung), Regelungen zu Datenübermittlungen.

Bei weiteren Fragestellungen senden Sie uns bitte eine Mail an: betrieblicher-datenschutz@erzbistum-koeln.de.

Freundliche Grüße

Ihre Abteilung Gemeindeverbände, Rendanturen und Service Kirchengemeinden

Im Auftrag
Lukas Karcz

Erzbistum Köln | Generalvikariat
Hauptabteilung Seelsorgebereiche
Abteilung Gemeindeverbände, Rendanturen und Service Kirchengemeinden
Betrieblicher Datenschutz für Kirchengemeindliche Rechtsträger

Marzellenstr. 32 | 50668 Köln
Postanschrift:
Erzbistum Köln | 50606 Köln

Telefon 0221 1642 1640

betrieblicher-datenschutz@erzbistum-koeln.de
www.erzbistum-koeln.de