Kurzinformation zum Thema KDG-DVO

Am 1. März 2019 ist die Durchführungsverordnung zum Gesetz über den kirchlichen Datenschutz (KDG-DVO) in Kraft getreten und löst somit die bisherige Durchführungsverordnung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) ab. Die KDG-DVO enthält dabei Konkretisierungen zum Gesetz über den kirchlichen Datenschutz (KDG) und befasst sich mit folgenden Themen:

- Verarbeitungstätigkeiten (§ 1)
- Datengeheimnis (§§ 2 - 3)
- Technische und organisatorische Maßnahmen (§§ 4 - 14)
- Maßnahmen des Verantwortlichen und des Mitarbeiters (§§ 15 - 17)
- Besondere Gefahrenlagen (§§ 18 - 26)

Ein inhaltlicher Schwerpunkt liegt dabei sicherlich auf den technischen und organisatorischen Maßnahmen (sog. TOM), die von den Verantwortlichen ergriffen und vollumfänglich dokumentiert werden müssen, um personenbezogene Daten in geeigneter Weise zu schützen. Die in § 6 Abs. 2 KDG-DVO genannten Kontrollbegriffe und Erläuterungen sind dabei durchaus hilfreich:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Transportkontrolle
- Speicherkontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

Im Unterschied zur bisher gültigen KDO-DVO schreibt die KDG-DVO eine regelmäßige Überprüfung der TOM auf ihre Wirksamkeit im Abstand von mindestens zwei Jahren vor. Der Abstand dieser Überprüfungen sollte dem Risiko für den Betroffenen, welches sich aus der Durchführung der Verarbeitung ergibt, angepasst sein. Verarbeitungen mit höheren Risiken sollten häufiger geprüft werden.

Anders als bisher wird in der neuen Regelung bereits für Daten der Datenschutzklasse II höhere Anforderungen an die Authentifizierung der Benutzer gestellt, sowie eine verschlüsselte Übertragung gefordert.
Die Nutzung privater IT-Systeme zu dienstlichen Zwecken ist grundsätzlich unzulässig, kann jedoch, bei Einhaltung genau definierter Mindestvoraussetzungen, im Einzelfall schriftlich genehmigt werden. Die neuen Regelungen der KDG-DVO sind unverzüglich, spätestens jedoch bis zum 31.12.2019, umzusetzen.

Zusammenfassung der wichtigsten Punkte zum Thema KDG-DVO

Verarbeitungstätigkeiten (§ 1)

Bevor eine Verarbeitung von personenbezogenen Daten aufgenommen werden kann, ist es notwendig, diese Tätigkeit in das Verzeichnis für Verarbeitungstätigkeiten einzutragen.
Das Verarbeitungsverzeichnis ist in regelmäßigen Abständen von höchstens zwei Jahren auf Vollständigkeit und Aktualität zu überprüfen. Das Verzeichnis für Verarbeitungstätigkeiten muss auf Anfrage der Datenschutzaufsicht zur Einsichtnahme unverzüglich zur Verfügung stehen.

Datengeheimnis (§§ 2 - 3)

Sämtliche Mitarbeiter sind durch geeignete Maßnahmen mit den Vorschriften des KDG sowie den anderen für ihre Tätigkeit geltenden Datenschutzvorschriften vertraut zu machen. Das Kirchliche Datenschutzgesetz muss jedem Mitarbeiter zur Einsichtnahme zur Verfügung stehen. Zusätzlich müssen die Mitarbeiter über die rechtlichen Folgen eines Verstoßes informiert werden und darüber, dass das Datengeheimnis nach Beendigung ihrer Tätigkeit weiter fortbesteht. Die Verpflichtungserklärung ist schriftlich zu unterschreiben und anschließend in der Personalakte zu Nachweiszwecken vorzuhalten.

Technische und organisatorische Maßnahmen (§§ 4 - 14)

Die Begriffsbestimmungen für IT-Systeme befindet sich in §5 KDG-DVO. Unter anderem werden Smartphones und Tablet Computer als IT-System definiert. Personenbezogene Daten dürfen erst auf IT-Systemen verarbeitet werden, wenn diese durch technische und organisatorische Maßnahmen angemessen geschützt sind (§5-6 KDG-DVO). Die technischen und organisatorischen Maßnahmen müssen spätestens alle zwei Jahre durch ein selbst entwickeltes Verfahren auf Sicherheit und Aktualität geprüft werden. Die Überprüfung muss schriftlich protokoliert werden (§7 KDG-DVO). Es darf nur Software installiert werden, welche von der verantwortlichen Stelle für Datenschutz geprüft und autorisiert wurden (§18 KDG-DVO).
Das automatische Weiterleiten von dienstlichen E-Mails auf private E-Mail-Konten ist grundsätzlich nicht gestattet (§20 KDG-DVO). Alle nicht zurücksetzbaren Passwörter sind gesichert aufzubewahren (§23 KDG-DVO).

Datenschutzklassen

- Personenbezogene Daten werden in drei verschiedene Datenschutzklassen unterteilt.
- Je höher die Schutzklasse, desto strenger sind die Regelungen der sicheren Aufbewahrung der personenbezogenen Daten.
- Die Schutzklasse ist vom Verantwortlichen für Datenschutz durch eine Risikoanalyse festzustellen (§9-10 KDG-DVO).

Maßnahmen des Verantwortlichen und des Mitarbeiters (§§ 15 - 17)

Verantwortlicher ist gemäß § 4 Nr. 9. KDG die natürliche oder juristische Person die, über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Erfolgt die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter, so ist der Verantwortliche verpflichtet, die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters regelmäßig, mindestens jedoch im Abstand von jeweils zwei Jahren auf ihre Wirksamkeit zu überprüfen und dies zu dokumentieren. Bei Vorlage eines anerkannten Zertifikats durch den Auftragsverarbeiter gemäß § 29 Absatz 6 KDG kann auf eine Prüfung verzichtet werden. Der Verantwortliche kann, unbeschadet seiner Verantwortlichkeit, seine Aufgaben und Befugnisse nach dieser Verordnung durch schriftliche Anordnung auf geeignete Mitarbeiter übertragen. Eine Übertragung auf den betrieblichen Datenschutzbeauftragten ist ausgeschlossen. Der Verantwortliche hat ein Datensicherungskonzept zu erstellen und entsprechend umzusetzen. Dabei ist die langfristige Lesbarkeit der zu speichernden Daten in der Datensicherung sicherzustellen.

Unbeschadet der Aufgaben des Verantwortlichen im Sinne des § 4 Ziffer 9. KDG trägt jeder Mitarbeiter nach KDG-DVO die Verantwortung für die datenschutzkonforme Ausübung seiner Tätigkeit.

Besondere Gefahrenlagen (§§ 18 - 26)

Die Nutzung privater IT-Systeme zu dienstlichen Zwecken ist grundsätzlich unzulässig, kann jedoch, bei Einhaltung genau definierter Mindestvoraussetzungen, im Einzelfall schriftlich genehmigt werden. Der Zugriff auf personenbezogene Daten von Dritten darf nur aufgrund einer vertraglichen Vereinbarung erfolgen. Die Vereinbarung muss neben der DSGVO auch die Anwendung des KDG beinhalten. Es muss sichergestellt werden, dass es für Externe nicht möglich ist, Sicherheitskopien von personenbezogenen Datenbeständen zu erstellen. Die Wartung von IT-Systemen mit Daten der Datenschutzklasse III darf nur in den eigenen Räumen erfolgen, außer es ist technisch nicht möglich, die Wartung in den eigenen Räumen durchführen zu lassen.

Wichtiger Hinweis: Die obige Darstellung dient nur der Übersicht. Ein Blick ins Gesetz erleichtert immer noch die Rechtsfindung.