KDG-Praxishilfe 08

Datenübermittlung in Drittländer

nach dem neuen Gesetz über den Kirchlichen Datenschutz (KDG)

Stand 11/2017

Konferenz der Diözesandatenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 8

Datenübermittlung in Drittländer nach dem KDG

Herausgegeben von
der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands

So erreichen Sie uns:
Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund
Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Autor dieser Praxishilfe:
Der Diözesandatenschutzbeauftragte für die bayerischen (Erz-)Bistümer

Diese Praxishilfe der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands dient als erste Orientierung, wie nach Auffassung der Diözesandatenschutzbeauftragten das neue Gesetz über den kirchlichen Datenschutz (KDG) im praktischen Vollzug angewendet werden sollte. Sie kann noch keine verbindliche Auslegung bieten, sondern stellt die gegenwärtige Interpretation der neuen Vorschriften durch die Diözesandatenschutzbeauftragten dar.

Revision 1.0/22.12.2017

Datenübermittlung in Drittländer nach dem Kirchlichen Datenschutzgesetz (KDG)

Übermittlungen personenbezogener Daten an und in Drittländer oder an internationale Organisationen

Bedeutung der Vorschriften für die katholische Kirche

Die Anordnung über den kirchlichen Datenschutz (KDO) hatte keine entsprechende Regelung. Auf den ersten Blick möchte man nun annehmen, dass nur in relativ wenigen Fällen überhaupt personenbezogene Daten durch kirchliche Dienststellen in das Ausland übermittelt werden und daher kein wirkliches Bedürfnis für die neue Kodifizierung besteht. Das ist so aber nicht richtig, wie die folgenden Beispiele zeigen mögen:

Beispiel 1
In einer Einrichtung wird ein Softwareprogramm zur Unterstützung der Kernprozesse eingesetzt. Diese Software wird über einen deutschen Anbieter vertrieben, jedoch durch ein internationales Team gewartet. Die Wartungszugriffe erfolgen jederzeit von überall aus der Welt (Service Follow the Sun); das Entwicklungsteam der Software hat seinen Hauptsitz in Indien. Im Rahmen des bestehenden Vertrages zur Auftragsdatenverarbeitung soll nun der Zugriff der Techniker aus einem Drittland zugelassen werden. Darf die Einrichtung dieser Vereinbarung zustimmen?
Beispiel 2
Eine Ordensgemeinschaft hat zwar ihren Sitz in Deutschland, aber in zahllosen Ländern Missionsstationen. Dürfen die personenbezogenen Daten der Missionare dorthin übermittelt werden?

Der Auslandsbezug zwingt deswegen, weil der Datenschutz nicht überall auf der Welt gleich ausgestaltet ist, die übermittelnde kirchliche Dienststelle zu einer sorgfältigen Zulässigkeitsprüfung. Dabei muss klargestellt werden, dass es sich um eine zusätzliche Prüfung der Zulässigkeit handelt, die allgemeinen Übermittlungsvoraussetzungen also bereits gegeben sein müssen, bevor überhaupt in diese Prüfung eingetreten wird. Um bei einem der obigen Beispiele zu bleiben: Ist der Einrichtung bekannt, dass das Datenschutzniveau in dem Drittland den Anforderungen der Europäischen Datenschutzgrundverordnung entspricht oder ob es Vereinbarungen gibt, die ein ähnliches Datenschutzniveau garantieren (sog. Binding Corporate Rules).

Für den gesamten Bereich des Auslandsbezuges muss der übermittelnden Dienststelle auch klar sein, dass sie als Behörde des öffentlichen Rechts tätig wird. Soweit sich Ausnahmen für die Übermittlungsbefugnis aus zwischenstaatlichen handelsrechtlichen Verträgen ergeben, reicht dies normalerweise noch nicht für eine Mitteilung durch eine Behörde, sofern die übrigen Voraussetzungen des § 40 KDG nicht gegeben sind.

Die Prüfungsgrundsätze

Übermittlung in Länder der Europäischen Union (EU) oder des Europäischen Wirtschaftsraumes

Solange die Datenübermittlung als Ziel ein Land oder eine Organisation innerhalb des Bereichs der Europäischen Union oder des europäischen Wirtschaftsraumes hat, ist sie unproblematisch, jedenfalls solange nicht Landbereiche betroffen sind, die ausdrücklich aus den genannten Gebieten ausgegliedert sind, wie Helgoland, Andorra, Grönland, San Marino etc.

Übermittlung in andere Länder der Welt

Sichere Drittländer sind solche, die über ein angemessenes Datenschutzniveau verfügen, welches dem EU-Recht hinreichend vergleichbar ist. Dazu gehören u. a. die Schweiz, Kanada, Argentinien, Andorra, Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland und Uruguay.

Unsichere Drittländer sind solche, die nicht zur EU oder zum europäischen Wirtschaftsraum gehören und über keinen Angemessenheitssbeschluß verfügen (§ 40 Abs. 2 KDG).

Darüber hinaus eröffnet § 41 KDG noch **Ausnahmen**, unter denen eine Übermittlung in ein Drittland auch dann zulässig sein kann, wenn kein angemessenes Datenschutzniveau herrscht. Dazu zählen z. B. die Einwilligung des Betroffenen, die Erfüllung eines Vertrages oder die Wahrung lebenswichtiger Interessen des Betroffenen.

Weitere Praxishilfen:

01 Wichtige Schritte bis zum In-Kraft-Treten des KDG

02 Der betriebliche Datenschutzbeauftragte nach dem KDG

03 Verantwortlichkeiten nach dem KDG

04 Auftragsverarbeitung nach dem KDG

05 Verzeichnis der Verarbeitungstätigkeiten nach dem KDG

06 Betroffenenrechte nach dem KDG

07 Transparenz- und Dokumentationspflichten nach dem KDG

09 Befugnisse und Sanktionsmöglichkeiten der Aufsicht nach dem KDG

10 Umgang mit Datenpannen nach dem KDG

11 Datenschutzfolgeabschätzung nach dem KDG

12 Neue Anforderungen an die IT-Sicherheit nach dem KDG

13 Datenschutzorganisation und -managementsysteme nach dem KDG

14 Der Rechtsweg nach der KDSGO

15 Technischer Datenschutz nach dem KDG

16 Begriffe im neuen KDG

17 Rechtmäßigkeit der Verarbeitung/Einwilligung

18 Nutzung der Daten für Werbezwecke

Diese Schriftenreihe wird gemeinsam herausgegeben von

Diözesandatenschutz-
beauftragter für die nord-
deutschen (Erz-)Diözesen

Diözesandatenschutz-
beauftragter für die ost-
deutschen (Erz-)Diözesen

Diözesandatenschutzbeauftragter für die
nordrhein-westfälischen (Erz-)Diözesen

Diözesandatenschutzbeauftragter
für die bayerischen (Erz-)Diözesen

Gemeinsame Datenschutzstelle der (Erz-)Diözesen
Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stutt-
gart, Speyer und Trier