Konferenz der Diözesan-datenschutzbeauftragten der Katholischen Kirche Deutschlands	10.04.2018	**Konferenz der Diözesandaten-schutzbeauftragten**
Vorlage 18/026(neu)	**Für die Sitzung am 17.-18.04.2018**	

TOP 6: Leitfaden elektronische Kommunikation

Sachverhalt

Der Arbeitskreis Technik wurde durch die Konferenz der Diözesandatenschutzbeauftragten am 08.02.2018 beauftragt, den vorgelegten Entwurf abzuklären, so dass dieser anschließend durch die DDSB veröffentlicht werden kann.

Der Entwurf wurde überarbeitet, wobei Begriffe des Risikomanagements in den erläuternden Text und in die tabellarische Darstellung der Fragestellungen aufgenommen wurden. Dadurch soll eine durchgängige Struktur des Leitfadens erreicht und die Verständlichkeit erhöht werden.

Der AK Technik hat den überarbeiteten Entwurf in einer Telefonkonferenz am 11.04.2018 einstimmig verabschiedet.

Entscheidungsvorschlag

Die Konferenz der DDSB beschließt den Leitfaden in der angefügten Fassung.

Vorberatungen zu dem Thema: ---
Verfasser der Vorlage: *Tegethoff/Becker/Gleißner*

Leitfaden „Externe Datenspeicherung und elektronische Kommunikation

Mit diesem Leitfaden soll auf praxisrelevante Fragestellungen und Themen eingegangen werden, die sich beim täglichen Umgang mit elektronischer Kommunikation und der Verwendung externer Speichermöglichkeiten, also z.B. Speicherorten in der „Cloud“ ergeben.

Das Ziel ist, das Bewusstsein für datenschutz- und datensicherheitsbezogene Risiken zu schärfen und jeweils passende Handlungsempfehlungen zu geben, durch deren Befolgen die Risiken deutlich begrenzt werden können.

Datenschutzrechtlich bedeutsam ist bei der Kommunikation und bei der Speicherung im Wesentlichen, ob personenbezogene Daten so gespeichert oder übermittelt werden, dass eine unbefugte Offenlegung gegenüber Dritten nicht mit der erforderlichen Sicherheit ausgeschlossen werden kann. Das ist meist aber keine Frage, die schnell mit einem bloßen Ja oder Nein beantwortet werden kann, sondern eine Gesamtabwägung aller Umstände verlangt. Erfahrungswerte sprechen vielfach dafür, dass kirchliche Dienststellen sich eher Risiko-avers verhalten sollten, d.h. Risiken für die Integrität und Vertraulichkeit der Daten eher vermeiden sollten als diese Risiken zugunsten einer größeren Bequemlichkeit zu akzeptieren.

Es müssen also – auch und gerade im Hinblick auf § 26 Abs. 3 KDG (bisher § 6 KDO) – vor der beabsichtigten Handlung die Prozessschritte des klassischen Risikomanagements durchgeführt werden:

- Risiko-Identifizierung: Welche Risiken für personenbezogene Daten bestehen. Welcher Schaden oder welche Gefährdung kann für den Betroffenen durch eine nicht autorisierte Offenlegung seiner Daten eintreten?
- Risiko-Bewertung: Wie groß wäre der potentielle Schaden und mit welcher Wahrscheinlichkeit wird sich das Risiko realisieren?
- Risiko-Abwehr: Welche Maßnahmen können ergriffen werden, um das Risiko hinsichtlich seiner Wahrscheinlichkeit und/oder seiner Schadenshöhe zu reduzieren oder sogar auszuschließen?

Die Tabelle in diesem Leitfaden soll helfen, die Risiken in ihrer Komplexität zu verstehen und Abhilfe zu schaffen. Dabei wurde auf eine detaillierte Bewertung der Risiko-Wahrscheinlichkeiten verzichtet, weil diese sehr vom Einzelfall abhängt und aufgrund der Schwere der potentiellen Schäden oft auch geringste Eintrittswahrscheinlichkeiten das Risiko schon inakzeptabel machen.

Die empfohlenen Maßnahmen sind aus unserer Sicht verhältnismäßig im Hinblick auf Ihre Implementierungskosten und den zu tragenden organisatorischen Aufwand und entsprechen dem Stand der Technik. Demnach erfüllen sie die Vorgaben des § 26 Abs. 3 KDG.

Ein Verzichten auf diese Maßnahmen mit Berufung auf eine vorliegende Einwilligung des Betroffenen in einen „unsicheren“ Umgang mit seinen personenbezogenen Daten halten wir nur in wenigen Ausnahmefällen für angebracht, da ein solches Vorgehen dem Selbstverständnis von kirchlichen Einrichtungen in diesen elementaren Fragen des Daten- und Vertrauensschutzes widerspricht.

Anlage

Elektronische Kommunikation

Thema / Subject	*Risikobeschreibung*	*Relevante Rechtliche Bestimmungen oder Grundsätze*	*Maßnahme zur Erreichung der Konformität oder Risikominderung*
Festnetztelefonie	Herkömmliche analoge Telefonie sowie Router-gebundenes VOIP bei etabliertem Anbieter ist risikoarm, weil zeitgemäße Verschlüsselungstechniken verwendet werden	TKG, DSGVO,	
Mobiltelefonie, mobile Datenverbindung	Telefonate und UMTS- bzw. LTE- Datenverbindungen eher unproblematisch, aber Nutzung (z.B. von VOIP) in öffentlichen WLAN sehr risikobehaftet (unbefugtes Mithören/Mitlesen, z.T. selbst bei verschlüsselten Netzen durch Sicherheitslücke während des Verbindungsaufbaus.	§§ 26, 27 KDG	VPN-Tunnel bei der Nutzung öffentlicher Netze. Ansonsten öffentliche WLAN möglichst vermeiden.
SMS / MMS	Basiert auf mobiler Telefonie, deshalb relativ sicher		
Telefax	Historisch ein sicheres und zugelassenes Medium, solange die Übertragung auf der klassischen analogen Telefonie basierte. Wegen der immer weiter verbreiteten (und für den Anwender transparenten) Verbreitung der digitalen Übertragung (IP) ähnelt das Telefax in Datenschutz-Hinsicht inzwischen der E-Mail. Durch Integration in Kombi-Geräte (Gemeinschaftsdrucker) kann die	Vertraulichkeit	Faxgeräte nur als Einzelgeräte einrichten oder vertraulichen Druck als Voreinstellung vorgeben. Wenn analoge Übertragung nicht garantiert werden kann, besser vermeiden (und stattdessen verschlüsselte E-Mail nutzen)

	Vertraulichkeit zusätzlich kompromittiert werden.		
Soziale Netzwerke und deren verbundene Messenger-Dienste	Unkontrollierbare Übertragung und Verwertung der Daten und Metadaten, auch in Drittstaaten, auch von Unbeteiligten durch Auslesen von Adressbüchern	§§ 39-41 KDG bzw. ein möglicher Verstoß gegen diese Drittlandsbestimmungen	Strikte Trennung zwischen privaten und dienstlichen Daten per Technik und Dienstanweisung. I.d.R. keine dienstliche Nutzung
Andere Messenger-Dienste	Eventuell fehlende Datenschutz-Konformität	KDG	Datenschutz-Faktoren wie Verschlüsselung, Vertraulichkeit, Speicherort sind streng zu prüfen. Dienstliche und private Nutzung sind streng zu trennen, d.h. separate Geräte, kein „Bring your own device“
FTP (File transfer protocol)	Unverschlüsselte Datei-Übertragung, dadurch Möglichkeit des Mitlesens und der Verfälschung	§§ 26, 27 KDG Vertraulichkeit, Integrität	Entweder Dateien vor dem Übertragen verschlüsseln, oder nur per VPN-Tunnel übertragen oder SFTP (Secure file transfer protocol) verwenden, welches eine Transportverschlüsselung einschließt.
E-Mail	Möglichkeit des Mitlesens in jedem Vermittlungsknoten („Elektronische Postkarte“). Möglichkeit der Fälschung von Absenderangaben. Auch beste Absicherungen (siehe rechte Spalte) auf nur einer der beiden Seiten (Sender oder Empfänger) können durch Schwachstellen auf der jeweils anderen Seite unwirksam gemacht werden.	Vertraulichkeit, Integrität, Authentizität	E-Mail verschlüsseln und signieren. (Beispiel: S/MIME oder PGP) Ansonsten nur unkritische Inhalte per offener E-Mail übertragen. Bei Inhalten mit personenbezogenen Daten zuvor die Einwilligung des Betroffenen zur Übertragung einholen. Risiko-Reduzierung durch - Nutzung seriöser inländischer, bestenfalls kirchlicher Provider - Nutzung virtueller privater Netzwerke (VPN) für die Übermittlung vom/zum Provider **Die beiden vorstehend genannten Maßnahmen sind nur dann voll wirksam, wenn sie sowohl auf Sender- als auch auf Empfängerseite beachtet werden!**

			- Dateitransfer per gesichertem Download/Upload von der Website (wie z.B. bei Kontoauszügen) - Bereitstellen von Kontaktformularen auf der (verschlüsselten) Website

Anlage

Externe digitale Datenspeicherung

Thema / Subject	*Risikobeschreibung*	*Relevante Rechtliche Bestimmungen oder Grundsätze*	*Maßnahme zur Erreichung der Konformität oder Risikominderung*
Fernwartung einer EDV-Anlage mit gespeicherten personenbezogenen Daten.	Während der Fernwartung kann es zu unbeabsichtigten und unkontrollierten Offenlegungen gegenüber dem Servicetechniker kommen. Der Tatbestand der Auftragsverarbeitung wird nicht erkannt. Notwendige vertragliche Regelungen unterbleiben	§§ 10,29 KDG	§ 29 Abs. 12 KDG definiert die Fernwartung als besondere Art der Auftragsverarbeitung. Demnach ist ein Auftragsverarbeitungsvertrag mit dem Erbringer der Fernwartung abzuschließen, der alle Anforderungen des § 29 KDG erfüllt.
Nutzung einer Cloud mit physikalischer Datenspeicherung im Ausland, (z.B. MS One Drive, Dropbox, Google) oder mit nicht definiertem oder unklarem physikalischem Speicherort	Bei physikalischer Speicherung der Daten in einem Drittland ist u.U. kein mit der Eu-DSGVO und dem KDG vergleichbares Datenschutzniveau gewährleistet. Möglicher Verstoß gegen Drittlandsbestimmungen.	§§ 39-41 KDG	Verwendung einer Cloud mit physikalischer Speicherung innerhalb der EU oder in Ländern mit durch die EU anerkanntem Datenschutzniveau (Angemessenheitsbeschluss). In Ausnahmefällen: Dokumentation der Abwägung der Ausnahmebedingungen nach § 41 KDG.
Auftragsverarbeitung von Daten, die in § 203 StGB genannt sind (Amts- und Berufsgeheinisse, v. a. medizinische Daten).	Erhöhtes Risiko der unzulässigen Offenlegung durch Verlängerung der Verarbeitungskette. Nicht ausreichende oder fehlerhafte Vertragsgestaltung kann auch strafrechtlich relevant werden	§ 203 StGB, § 29 KDG	Prinzipiell ist die Auftragsverarbeitung von personenbezogener Daten im Zusammenhang mit Amts- und Berufsgeheimnissen zulässig, wenn verschärfte Anforderungen an • die Gestaltung des Auftragsverarbeitungsvertrages • die Einbindung der Mitarbeiter des Auftragsverarbeiters (Verschwiegenheitserklärung) • die Einhaltung der Drittlandsbestimmungen beachtet werden.