Evangelische Kirche in Deutschland

DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Technische und organisatorische Maßnahmen, IT-Sicherheit

Die Kurzpapiere des Beauftragten für den Datenschutz der EKD (BfD EKD) dienen als erste Orientierung für die praktische Anwendung des novellierten EKD-Datenschutzgesetzes (DSG-EKD). Die in den Kurzpapieren vertretene Auffassung des BfD EKD steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung, die sich im praktischen Vollzug des DSG-EKD entwickeln kann.

Einleitende Überlegungen

Die Begriffe Datensicherheit, IT-Sicherheit und technischer Datenschutz werden im Bereich Datenschutz zwar häufig verwendet, aber leider immer wieder miteinander vermischt oder auch verwechselt. Es besteht deshalb ein nicht unwesentlicher Interpretationsspielraum, welche technischen Sicherheitsmaßnahmen auch aus Datenschutzgesichtspunkten erforderlich sind.

Der früher relevante § 9 DSG-EKD zu den technischen und organisatorischen Maßnahmen blieb – trotz Anlage – eher allgemein, wenn es darum ging, geeignete Maßnahmen nach festen Kriterien zu bestimmen. § 9 Abs. 2 DSG-EKD mit der IT-Sicherheitsverordnung (ITSVO) machten hingegen klar, dass IT-Sicherheit angelehnt an den BSI-Grundschutz umgesetzt werden sollte. Im neuen DSG-EKD sind nun neue Regelungen zur Informationssicherheit getroffen worden und es stellt sich die Frage, wie diese zu verstehen sind.

Besondere Bedeutung hat § 27 DSG-EKD. In diesem Paragraphen wird vergleichsweise ausführlich beschrieben, nach welchen Kriterien technische und organisatorische Maßnahmen zu wählen sind, um ein angemessenes Schutzniveau zu gewährleisten.

Auch an vielen anderen Stellen des DSG-EKD werden entsprechende Fachbegriffe zur IT-Sicherheit aus § 27 DSG-EKD erwähnt. Nachfolgend werden deshalb grundlegende Begriffe, die nach Einschätzung des BfD EKD eine bedeutsame Rolle spielen, näher dargestellt und eingeordnet.

Schutzbedarf personenbezogener Daten

Um beurteilen zu können, was ein angemessenes Schutzniveau nach § 27 Abs. 1 DSG-EKD ist, muss im Vorfeld für Verantwortliche klar sein, welchen Schutzbedarf die relevanten personenbezogenen Daten besitzen. Hierbei existieren in der Praxis bereits heute verschiedene Ansätze, die in der Regel auf das Schadenspotential abzielen. Berücksichtigt man § 27 Abs. 6 DSG-EKD und die ITSVO, so wird man in Kategorien des Schutzbedarfs nach BSI Grundschutz (normal, hoch und sehr hoch) sprechen und handeln können. Die Schutzbedarfsfeststellung ist als ein erster Schritt essentiell, wenn es später darum geht, geeignete technische und organisatorische Maßnahmen auszuwählen.

Risikobewertung

Der Begriff des Risikos wird mehrfach im DSG-EKD verwendet. Die Maßnahmen, die zum Schutz von personenbezogenen Daten getroffen werden sollen, müssen künftig unter Berücksichtigung des Risikos ausgewählt werden. Hierbei besteht die Herausforderung, objektive Kriterien für Eintrittswahrscheinlichkeit und Schwere eines Risikos für die Rechte und Freiheiten natürlicher Personen festzulegen. Während durch die Umsetzung der

ITSVO heute bereits einige kirchliche Stellen verschiedene Risikobewertungsansätze etabliert haben, gilt es künftig, nicht nur die verantwortliche kirchliche Stelle, sondern im Sinne des Datenschutzes auch die betroffenen Personen in den Fokus der Risikobewertung zu setzen. Zum Risikobegriff wird auch auf das Kurzpapier Nummer 9 verwiesen.

Technische und organisatorische Maßnahmen

In § 27 DSG-EKD wird von geeigneten technischen und organisatorischen Maßnahmen, die die verantwortliche Stelle unter Berücksichtigung u. a. des Stands der Technik und der Implementierungskosten zu treffen hat, gesprochen. Folglich wird einerseits stets zu prüfen bleiben, was beim jeweiligen Verfahren als Stand der Technik angesehen wird. Anderseits ist auch die Verhältnismäßigkeit einer Maßnahme hinsichtlich des Aufwands zu diskutieren (§ 27 Abs. 3 DSG-EKD).

Generell gelten aber folgende Anforderungen an die technischen und organisatorischen Maßnahmen:

1. Sie sind nachweisfähig.
2. Sie berücksichtigen den Kontext.
3. Sie entsprechen dem Stand der Technik.
4. Sie werden regelmäßig geprüft/aktualisiert.
5. Sie basieren auf einer Risikobetrachtung.

Technische Aspekte der Datenverarbeitung, die bislang eher unter „IT-Sicherheit“ fielen, bekommen durch das neue DSG-EKD eine höhere Bedeutung für die verantwortliche kirchliche Stelle als es bislang durch das DSG-EKD abgebildet wurde. In den nächsten Jahren müssen hierfür jedoch objektive Kriterien und Methoden festgelegt werden, um künftig geeignete Maßnahmen auszuwählen. Der BfD EKD ist aber weiterhin der Auffassung, dass eine erste Quelle der BSI-Grundschutz sein kann. Darüber hinaus befasst sich eine ökumenische Arbeitsgruppe gegenwärtig damit, das im staatlichen Datenschutz entwickelte Standard-Datenschutzmodell (SDM), das ebenfalls geeignete Maßnahmen aufzeigt, für den kirchlichen Bereich anwendbar zu machen. Es wird ein kirchliches Standard-Datenschutzmodell (KDM) erarbeitet, welches sich direkt auf die kirchlichen Datenschutzgesetze (DSG-EKD und KDG) beziehen wird.

Nachweis der Konformität

Inwieweit eine verantwortliche kirchliche Stelle sich an die Verarbeitungsgrundsätze des DSG-EKD hält und die Sicherheit der Verarbeitung gewährleistet, wird auch im Rahmen einer Nachweiserbringung relevant werden (siehe Rechenschaftspflicht nach § 5 Abs. 2 DSG-EKD). Die verantwortliche kirchliche Stelle muss im Ergebnis eine Fülle an technischen und organisatorischen Maßnahmen (risikobasiert) definieren, umsetzen, dokumentieren und kontrollieren. Angesichts der Fülle von Anforderungen einerseits und der Rechenschafts- und Nachweispflicht aus dem DSG-EKD andererseits wird sie dabei um ein geordnetes System nicht herumkommen. So ist die Einführung eines Datenschutzmanagements wohl zwingend. Darüber hinaus werden genehmigte Verhaltensregeln ebenso wie Zertifizierungen an Bedeutung gewinnen.

PDCA-Zyklus

Das DSG-EKD greift etablierte Prinzipien aus Management-Systemen anderer Disziplinen wie etwa der Informationssicherheit oder des Risikomanagements auf. Nach § 27 DSG-EKD muss die verantwortliche Person unter Berücksichtigung des Kontexts und des Risikos Maßnahmen planen, umsetzen, dokumentieren, prüfen und bei Bedarf verbessern. Nichts anderes besagt im Kern der P(lan)-D(o)-C(heck)-A(ct)-Zyklus als Prinzip eines jeden Management-Systems. Somit ist der PDCA-Zyklus auch geeignet, um die Anforderungen an technische und organisatorische Maßnahmen zu dokumentieren und geordnet zu planen und umzusetzen.