Evangelische Kirche in Deutschland

DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Was ist bis zum Inkrafttreten des novellierten DSG-EKD zu tun?

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.

Das EKD-Datenschutzgesetz (DSG-EKD) tritt in seiner geänderten Fassung am 24. Mai 2018 in Kraft (§ 56 Satz 2 DSG-EKD). Gleichzeitig gilt das „alte“ DSG-EKD dann nicht mehr und tritt außer Kraft.

Warum war die Novellierung des DSG-EKD notwendig?

Die Anpassungen im DSG-EKD wurden durch den Beschluss der EU-Datenschutz-Grundverordnung (DSGVO) notwendig. Die DSGVO beinhaltet einheitliche Datenschutzregelungen für die gesamte Europäische Union.

Art. 91 Abs. 1 DSGVO erlaubt Kirchen oder religiösen Vereinigungen, die zum Zeitpunkt des Inkrafttretens der DSGVO umfassende gesetzliche Regelungen zum Datenschutz anwenden, dies auch weiterhin zu tun, wenn die Regelungen mit der DSGVO „in Einklang gebracht“ werden.

Auch im Hinblick auf die Datenschutzaufsicht dürfen Kirchen oder religiöse Vereinigungen eine eigene Art der Datenschutzaufsicht vorsehen, wenn die Regelungen im Kapitel VI der DSGVO, in dem die unabhängigen Aufsichtsbehörden geregelt sind, eingehalten werden (Art. 91 Abs. 2 DSGVO)

Was bedeutet das neue DSG-EKD rechtlich und praktisch für kirchliche Stellen als verantwortliche Stellen und Auftragsverarbeiter?

Das neue DSG-EKD beinhaltet einige Neuerungen. Viele Inhalte des alten DSG-EKD haben aber auch völlig unverändert oder in etwas veränderter Form Eingang in das neue DSG-EKD gefunden. Somit muss nicht komplett von vorne begonnen werden.

Vielmehr ist es entscheidend, die in der kirchlichen Stelle schon bestehenden Regelungen (z. B. in Richtlinien, Dienstvereinbarungen) daraufhin zu überprüfen, ob diese den Anforderungen des neuen DSG-EKD (noch) gerecht werden

Weiterhin muss jede kirchliche Stelle prüfen, welche neuen Pflichten das DSG-EKD ihr künftig auferlegt und bis wann diese umgesetzt werden müssen.

Was muss bis zum Inkrafttreten des neuen DSG-EKD rechtlich beachtet werden?

Neue Pflichten im DSG-EKD

Das neue DSG-EKD enthält neue Pflichten für die verantwortliche Stelle.

Diese müssen erkannt und dann in der jeweiligen kirchlichen Stelle praktisch umgesetzt werden.

1) Rechenschaftspflicht (§ 5 Abs. 2 DSG-EKD)

2) Meldepflicht einer „Datenpanne“ an die Aufsichtsbehörde (§ 32 DSG-EKD)

3) Meldepflicht einer „Datenpanne“ an die betroffene Person (§ 33 DSG-EKD)

4) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (§ 28 DSG-EKD)

Datenschutz-Folgenabschätzung anstatt Vorabkontrolle

Die bisher bekannte Vorabkontrolle wird Im neuen DSG-EKD durch eine Datenschutz-Folgenabschätzung ersetzt. Bei der Datenschutz-Folgenabschätzung ist eine Risikoabwägung durchzuführen.

Siehe auch Kurzpapier Nr. 4.

Verzeichnis von Verarbeitungstätigkeiten statt Meldepflichten

Die verantwortliche Stelle und auch der Auftragsverarbeiter muss alle Verarbeitungstätigkeiten, die in seiner Zuständigkeit liegen, in einem Verzeichnis führen (§ 31 DSG-EKD). Dies soll die Dokumentation der Einhaltung des DSG-EKD gegenüber der Aufsichtsbehörde sicherstellen und gewährleisten, dass diese bei eventuellen Prüfungen einen ersten Einblick in den Umgang mit personenbezogenen Daten in der Einrichtung bekommt.

Siehe auch Kurpapier Nr. 1.

Regelung zur Übermittlung an Drittstaaten und internationale Organisationen

Siehe Kurpapier Nr. 3.

Geänderte Begriffsbestimmungen im neuen DSG-EKD

Einige Begriffsbestimmungen im neuen DSG-EKD weichen von den bisherigen Bezeichnungen ab.

Deshalb müssen alle internen Regelungen in der verantwortlichen Stelle sowie die verwendeten Muster und Vorlagen daraufhin überprüft werden, ob sie noch in der bisherigen Form verwendet werden können. Ansonsten sind Anpassungen vorzunehmen.

Beispiele:

- Besondere personenbezogene Daten heißen „besondere Kategorien personenbezogener Daten“ (§ 4 Nr. 2 DSG-EKD).
- Sperren heißt „Einschränkung der Verarbeitung“ (§ 4 Nr. 4 DSG-EKD).
- Anstatt Auftragsdatenverarbeitung und Auftragsdatenverarbeiter heißt es Auftragsverarbeitung und Auftragsverarbeiter (§ 4 Nr. 10 DSG-EKD)

Keine Trennung mehr zwischen unterschiedlichen Phasen der Verarbeitung personenbezogener Daten

Bislang wurde im DSG-EKD zwischen den unterschiedlichen Phasen der Datenverarbeitung unterschieden. Somit musste jeweils eine Rechtsgrundlage für das Erheben, Verarbeiten oder Nutzen personenbezogener Daten vorliegen. Im neuen DSG-EKD wird ein einheitlicher Verarbeitungsbegriff verwendet. Es gibt bei der Beurteilung der Zulässigkeit der Verarbeitung personenbezogener Daten keine Unterteilungen mehr. Es muss lediglich eine Rechtsgrundlage für den gesamten Verarbeitungsprozess vorliegen.

Stärkung der Betroffenenrechte im neuen DSG-EKD

Genau wie die DSGVO enthält das neue DSG-EKD Änderungen bei der Ausgestaltung der Betroffenenrechte.

So enthält § 16 DSG-EKD beispielsweise Regelungen im Hinblick auf die praktische Umsetzung der Gewährleistung der Betroffenenrechte. Die verantwortliche Stelle muss hierbei prüfen, ob sie in ihren Richtlinien, Prozessen, Workflows oder Mustern den Regelungen der §§ 16 bis 25 DSG-EKD gerecht werden.

Siehe auch Kurpapiere Nr. 5, 7, 8.

Technische und organisatorische Maßnahmen orientieren sich künftig am Risiko

In § 27 DSG-EKD steht künftig der Risikobegriff im Vordergrund. Bei der Auswahl technischer und organisatorischer Maßnahmen müssen künftig

neben Art, Umfang, Umständen und Zweck der Verarbeitung auch die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten betroffener Personen durch die jeweilige Datenverarbeitung beachtet werden.

Siehe auch Kurpapier 9.

Neue Befugnisse der Aufsichtsbehörden

Künftig werden auch kirchliche Aufsichtsbehörden bei gravierenden Verletzungen des Datenschutzes die Möglichkeit haben die Durchsetzungen des Datenschutzes im Wege von Anordnungen und Bußgeldern zu gewährleisten (§ 44 DSG-EKD).

Siehe auch Kurpapier Nr. 2.

Wie sieht die praktische Umsetzung aus?

1) Information der Leitung und der Fachverantwortlichen über die Änderungen aufgrund des novellierten DSG-EKD. Ggf. Prüfung, ob eine Arbeitsgruppe zur Umsetzung gegründet werden soll.

2) Bestandsaufnahme des Ist-Zustands

   - Welche Prozesse mit Datenschutzbezug gibt es? Dokumentation vorhanden?
   - Welche Rechtsgrundlage habe ich (Rechtsvorschrift, Einwilligung)?
   - Welche Maßnahmen trifft die verantwortliche Stelle zum Schutz personenbezogener Daten?
   - Welche Dienstleistungsbeziehungen (ADV?) gibt es?
   - Welche Dokumentationen gibt es (Vorabkontrollen, Datenschutzkonzept, IT-Sicherheitskonzept)?
   - Welche Dienstvereinbarungen enthalten Regelungen zum Beschäftigtendatenschutz?

3) Handlungsbedarf ermitteln (besondere Beachtung folgender Themen)

   - Welche Rechtsgrundlage (Rechtsvorschrift oder Einwilligung)?
   - Werden die Betroffenenrechte gewährleistet (Verfahren, Fristen, Vorlagen oder Formulare, Transparenz)?
   - Wird der Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen bei der Ausgestaltung von Prozessen und Voreinstellungen beachtet (§ 28 DSG-EKD)?
   - Gibt es eine Übersicht aller Dienstleister (ADV) und entsprechen die ADV-Verträge den Anforderungen in § 30 Abs. 3 DSG-EKD? (Bei Auftragsverarbeitern, die keine kirchliche Stelle sind, Hinweis auf § 30 Abs. 5 DSG-EKD.)
   - Wird der Nachweispflicht gemäß § 5 Abs. 2 DSG-EKD nachgekommen (z. B. Verzeichnis von Verarbeitungstätigkeiten oder Meldepflichten bei Datenpannen)?
   - Wie muss der Prozess der Vorabkontrolle weiterentwickelt werden, um der Datenschutz-Folgenabschätzung gerecht zu werden?
   - Welche Meldepflichten bestehen? Gibt es Prozesse, die Verfahren und Zuständigkeiten regeln?

     z. B. Bestellung von örtlich Beauftragten an die Datenschutzaufsicht und nach dem allgemeinen Recht zuständiger Aufsicht (§ 36 Abs. 5 DSG-EKD)

     z. B. Datenpannen (§§ 32, 33 DSG-EKD)

4) Umsetzung bis zum 24. Mai 2018 bzw. Übergangsfristen beachten