Evangelische Kirche in Deutschland

DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Verzeichnis von Verarbeitungstätigkeiten

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.

Nach der Novellierung des EKD-Datenschutzgesetzes (DSG-EKD) ist gemäß § 31 DSG-EKD ein Verzeichnis von Verfahrenstätigkeiten zu führen.

Ein „Verfahrensverzeichnis“ war schon bis Ende 2012 im DSG-EKD vorgesehen. Bei der letzten Novellierung des DSG-EKD wurde auf das Verfahrensverzeichnis verzichtet. Die bestehenden Meldepflichten der verantwortlichen Stelle wurden als ausreichend erachtet.

Um den europarechtlichen Vorgaben gerecht zu werden, wurde das Verzeichnis von Verarbeitungstätigkeiten wieder in das DSG-EKD aufgenommen.

Was ist der Sinn und Zweck eines solchen Verzeichnisses von Verarbeitungstätigkeiten?

Mit Hilfe des Verzeichnisses von Verarbeitungstätigkeiten wird der verantwortlichen Stelle eine Dokumentationspflicht gegenüber der Aufsichtsbehörde auferlegt. Sie erbringt durch das Verzeichnis den Nachweis, dass sie die Regelungen über den Datenschutz einhält. Dies ist dem Erwägungsgrund 82 der EU-Datenschutz-Grundverordnung (DSGVO) zu entnehmen.

Wer darf Einsicht in das Verzeichnis nehmen?

Das Verzeichnis darf lediglich von der Aufsichtsbehörde eingesehen werden und muss dieser zur Verfügung gestellt werden (§ 31 Abs. 4 DSG-EKD). Eine Einsichtnahme von Dritten ist nicht vorgesehen.

Wer muss ein solches Verzeichnis führen?

Ein Verzeichnis der Verarbeitungstätigkeiten muss von der verantwortlichen Stelle sowie dem Auftragsverarbeiter (§ 31 Abs. 1 und 2 DSG-EKD) geführt werden.

Verantwortliche Stelle ist nach der Legaldefinition in § 4 Nr. 9 DSG-EKD „die natürliche oder juristische Person, kirchliche Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten entscheidet.

Auftragsverarbeiter ist gemäß Legaldefinition in § 4 Nr. 10 DSG-EKD eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, die personenbezogene Daten im Auftrag der verantwortlichen Stelle verarbeitet.

Ist die kirchliche Stelle sowohl verantwortliche Stelle als auch Auftragsverarbeiter, dann bietet es sich an, zwei Vorlagen und zwei unterschiedliche Formulare zu verwenden.

In welchen Fällen muss kein Verzeichnis von Verarbeitungstätigkeiten geführt werden?

Ein Verzeichnis aller Verarbeitungstätigkeiten muss - wie nach den Regelungen der DSGVO - nicht geführt werden, wenn eine verantwortliche Stelle weniger als 250 Beschäftigten hat. In § 31 Abs. 5 Satz 1 DSG-EKD ist diese Ausnahme geregelt. Wer als Beschäftigter zu sehen ist, kann § 4 Nr. 20 DSG-EKD entnommen werden.

Zielsetzung des Gesetzgebers ist hierbei die Entlastung kleiner und mittlerer Einrichtungen von Dokumentationspflichten, die als bürokratisch empfunden werden könnten.

Anders als in der DSGVO und dem Gesetz über den Kirchlichen Datenschutz (KDG) der katholischen Kirche enthält das DSG-EKD dem Wortlaut nach in § 31 Abs. 5 Satz 2 DSG-EKD keine generelle Gegenausnahme, die dazu führt, dass auch kleine und mittlere Einrichtungen wieder verpflichtet sind ein Verfahrensverzeichnis zu führen, wenn einer der folgenden Fälle vorliegt: Die Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung ist nicht nur gelegentlich sowie besondere Kategorien personenbezogener Daten bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten werden durchgeführt.

Dem Wortlaut nach müssen kirchliche Stellen, die weniger als 250 Beschäftigte haben, gemäß § 31 Abs. 5 Satz 2 DSG-EKD ein Verzeichnis vielmehr nur in Bezug auf die einzelnen Verfahren führen, in denen besondere Kategorien personenbezogener Daten (§ 4 Nr. 2 DSG-EKD) verarbeitet werden.

Wie diese Einschränkung dem Ziel der Vorschrift gerecht wird, wird die zukünftige Praxis zeigen.

In welcher Form muss das Verzeichnis geführt werden?

Das Verzeichnis muss schriftlich in analoger oder elektronischer Form geführt werden (§ 31 Abs. 3 DSG-EKD). Zur Vorlage an die Aufsichtsbehörde muss das Verzeichnis in beiden Formen exportierbar sein.

Was muss das Verzeichnis konkret enthalten?

Inhaltlich muss das Verzeichnis alle Verarbeitungstätigkeiten personenbezogener Daten enthalten, für die die verantwortliche Stelle oder der Auftragsverarbeiter zuständig ist (§ 31 Abs. 1 Satz 1 DSG-EKD). Im Hinblick auf den Verfahrensbegriff ist nach wie vor von „einem Bündel von Verfahrensschritten“ auszugehen (§ 18 Abs. 1 RL 95/46/EG). Dies ergibt sich schon aus der Zielsetzung nicht einzelne Verarbeitungen, sondern eine prozessorientierte Darstellung der Verarbeitungstätigkeiten im Verzeichnis aufzunehmen.

Konkret sind die einzelnen Angaben, die das Verzeichnis enthalten muss, in § 31 Abs. 1 Nr. 1 bis 8 DSG-EKD für die verantwortliche Stelle und in § 31 Abs. 2 Nr. 1 bis 4 DSG-EKD für den Auftragsverarbeiter einzeln benannt.

Im Einzelnen trifft die verantwortliche Stelle die Dokumentationspflicht in einem Verzeichnis hinsichtlich folgender Punkte

1) Namen und Kontaktdaten der verantwortlichen Stelle, bei gemeinsamer Verantwortlichkeit Namen und Kontaktdaten aller verantwortlicher Stellen sowie ggf. der Name der oder des örtlich Beauftragten

2) Verarbeitungszweck

   Hier wird der Tatsache Rechnung getragen, dass der Zweck der Verarbeitung Auswirkungen auf das Risiko für Rechte der betroffenen Personen hat. Personenbezogene Daten, die zur Abwicklung eines Vertrages verarbeitet werden, bergen in sich weniger Gefahren, als etwa eine gezielte Profilbildung anhand der Daten.

3) Personen- und Datenkategorien

   Personenkategorien sind beispielsweise Kunden, Mitarbeitende oder Patienten, also die betroffenen Personengruppen.

   Bei Datenkategorien kann insbesondere zwischen personenbezogenen Daten und besonderen Kategorien gemäß § 4 Nr. 2 DSG-EKD unterschieden werden.

4) ggf. Profiling (wenn dies durchgeführt wird)

5) Empfängerkategorien

   Der Begriff Empfänger ist in § 4 Nr. 11 DSG-EKD legal definiert. Es handelt sich um „eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, der personenbezogene Daten offengelegt werden“. Bei internen

Empfängern wird die Funktionsbezeichnung (z. B. Personalabteilung) ausreichen.

6) Übermittlung an ein Drittland

Mitteilungen zu einem Angemessenheitsbeschluss oder einer sonstigen Rechtsgrundlage gemäß § 10 DSG-EKD

7) (wenn möglich) Löschfristen

Die Löschfristen der einzelnen Datenkategorien müssen auch im Rahmen eines Löschkonzepts im IT-Sicherheitskonzept enthalten und sollten Teil des Datenschutzkonzepts der Einrichtung sein. Mit der Aufnahme in das Verfahrensverzeichnis wird gleichzeitig der Nachweispflicht gemäß § 5 Abs. 2 DSG-EKD nachgekommen.

8) (wenn möglich) eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 27 DSG-EKD

Eine eher kurzgehaltene und skizzenhafte Darstellung reicht aus. Eine umfassende Darstellung muss aufgrund der Rechenschaftspflicht in § 5 Abs. 2 DSG-EKD aber im Datenschutzkonzept enthalten sein. Mit der Aufnahme in das Verfahrensverzeichnis wird ebenfalls der Nachweispflicht gemäß § 5 Abs. 2 DSG-EKD nachgekommen.

Welche Besonderheiten gelten, wenn es sich um einheitliche Verfahren handelt?

9) Gemäß § 31 Abs. 6 DSG-EKD können sowohl die EKD als auch die Gliedkirchen oder die gliedkirchlichen Zusammenschlüsse rechtliche Regelungen treffen, wonach bei einheitlichen Verfahren das Verzeichnis zentral geführt werden kann. Mit dieser Möglichkeit soll eine unverhältnismäßige Bürokratisierung durch das Verzeichnis von Verarbeitungstätigkeiten vermieden werden.