Evangelische Kirche in Deutschland

DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Datenschutz-Folgenabschätzung

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.

Hintergrund

Mit dem Inkrafttreten des neuen EKD-Datenschutzgesetzes (DSG-EKD) entfällt die Pflicht verantwortlicher Stellen zur Durchführung einer Vorabkontrolle automatisierter Verarbeitungen. Gleichwohl gilt es, eine Beeinträchtigung der Rechte und Freiheiten betroffener Personen durch einen unreflektierten und unangepassten Einsatz neuer Verarbeitungsformen zu verhindern. Dies ist einer der Hauptzwecke der in § 34 DSG-EKD normierten Datenschutz-Folgenabschätzung (im Folgenden als „DSFA“ bezeichnet), die sich als spezielles Instrument des Datenschutzes nicht nur mit der Identifikation von Risiken für die Rechte natürlicher Personen, sondern auch mit geeigneten Abhilfemaßnahmen befasst.

Im Rahmen der DSFA sind verantwortliche Stellen gehalten, die aus einzelnen Verarbeitungsvorgängen resultierenden Datenschutz-Risiken systematisch zu ermitteln und zu bewerten. Hierbei ist der Rat der örtlich Beauftragten einzuholen, sofern solche bestellt wurden.

Das Anknüpfungsmerkmal „Verarbeitungsvorgang“

Gegenstand der DSFA sind einzelne, konkrete „Verarbeitungsvorgänge“. Dieser Begriff ist weit zu verstehen und umfasst grundsätzlich die Verarbeitung sämtlicher Kategorien personenbezogener Daten. Außerdem sind sowohl Hardware, als auch Software-Systeme sowie sämtliche anderen denkbaren Prozesse zu betrachten. § 4 Nr. 3 DSG-EKD definiert, was unter einer „Verarbeitung“ zu verstehen ist.

Das Gesetz gestattet es verantwortlichen Stellen, für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken eine einzige DSFA vorzunehmen. Aus einer solchen Zusammenfassung mehrerer Verarbeitungsvorgänge können sich für die Erstellung der DSFA Besonderheiten ergeben, die möglicherweise eine Abweichung vom hier Vorgehen erforderlich machen.

Voraussetzungen zur Durchführung einer DSFA

Vor Durchführung der in § 34 Abs. 1 bis 4 DSG-EKD beschriebenen Prüfungsschritte einer DSFA sollte die verantwortliche Stelle stets prüfen, ob die Voraussetzungen des § 34 Abs. 7 DSG-EKD vorliegen, da in diesem Fall keine DSFA durchgeführt werden muss.

In allen anderen Fällen ist eine DSFA immer dann durchzuführen, wenn eine Form der Verarbeitung – insbesondere bei Verwendung neuer Technologien – aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge hat.

Zum Begriff des „Risikos“, der im neuen DSG-EKD nicht nur im Bereich der DSFA eine wichtige Rolle spielt, wird eine eigene Kurzinformation veröffentlicht.

Die gesetzliche Formulierung, wonach zu prüfen ist, ob „*voraussichtlich* ein hohes Risiko“ besteht, verdeutlicht, dass die Durchführung einer DSFA auf Grundlage einer Prognose stattfindet. Diese Prognose-Entscheidung ist entbehrlich, sofern eine der in § 34 Abs. 3 Nr. 1 bis 3 DSG-EKD beispielhaft aufgelisteten risikobehafteten Verarbeitungsformen vorliegt. Nach dieser Liste ist eine DSFA unter anderem dann stets erforderlich, wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche stattfinden soll.

Aus diesen gesetzlichen Anforderungen folgt für die Praxis, dass grundsätzlich *jeder* Verarbeitungsvorgang vor seiner Umsetzung von der verantwortlichen Stelle zunächst daraufhin zu untersuchen ist, ob ihm voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen innewohnt. Erst anhand dieser auch als „Schwellwertanalyse“ bezeichneten Vorprüfung lässt sich beurteilen, ob eine DSFA durchgeführt werden muss.

Zeitpunkt der Durchführung und Fortschreibung

Für die Vornahme einer DSFA ergeben sich aus dem Gesetz zwei zeitliche „Meilensteine“. Zum einen ist sie nach § 34 Abs. 1 Satz 1 DSG-EKD „vorab“, das heißt vor der praktischen Umsetzung der von der verantwortlichen Stelle geplanten Verarbeitungsvorgänge, durchzuführen.

Zum anderen sieht § 34 Abs. 8 DSG-EKD vor, dass die verantwortliche Stelle eine Überprüfung der DSFA durchführt, solange die relevanten Verarbeitungsvorgänge fortdauern. Hierdurch soll bewertet werden, ob die Verarbeitung gemäß der DSFA durchgeführt wird oder ob Anpassungen des Prüfergebnisses erforderlich sind. Eine Überprüfung muss insbesondere erfolgen, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind. Hierbei kommen grundsätzlich sämtliche in der DSFA bisher nicht berücksichtigte Faktoren wie zum Beispiel neu hinzutretende Risikoquellen, neue Erkenntnisse zu den Risiken einer eingesetzten Technologie sowie Änderungen im Verfahren in Betracht.

Der Pflicht zur Vornahme einer DSFA kann daher in der Regel nur im Wege eines fortlaufenden, dynamischen und iterativen Prozesses, der sich aus einer Erstprüfung und deren kontinuierlicher Fortschreibung ergibt, entsprochen werden.

Zwingender Inhalt

Das Gesetz macht keine abschließenden Vorgaben zur inhaltlichen Gestaltung der DSFA. In § 34 Abs. 4 Nr. 1 bis 4 DSG-EKD werden jedoch als Mindestanforderungen die folgenden Angaben benannt:

1) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von der verantwortlichen Stelle verfolgten berechtigten Interessen;

2) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

3) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

4) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die datenschutzrechtlichen Regelungen eingehalten werden.

Form und Dokumentation

§ 34 DSG-EKD enthält keine Vorgabe zur Form der DSFA. Die gesetzlichen Mindestanforderungen an ihren Inhalt, vor allem die Forderung einer „systematischen Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung“ (§ 34 Abs. 4 DSG-EKD) gebieten jedoch eine Anfertigung in Textform. Hinzu kommt, dass der DSFA-Bericht einen Baustein der umfassenden Dokumentation zur Umsetzung der in § 5 Abs. 2 DSG-EKD normierten Rechenschaftspflicht der verantwortlichen Stelle darstellt.

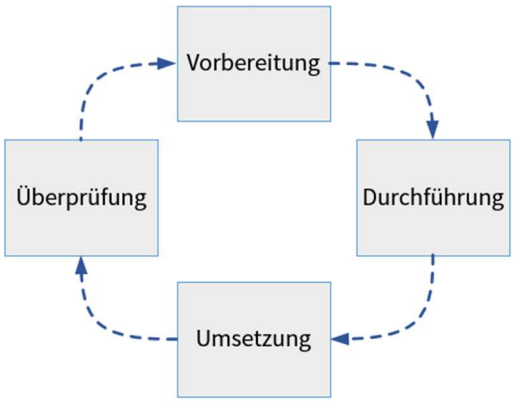
Konsultation der Aufsichtsbehörde

Ergibt eine DSFA, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss nach § 34 Abs. 9

DSG-EKD die verantwortliche Stelle die Aufsichtsbehörde vor Beginn der Verarbeitung konsultieren.

Empfehlungen zur praktischen Prozessgestaltung

Innerhalb der Grenzen der gesetzlichen Regelungen verfügen die verantwortliche Stellen über Gestaltungsspielräume hinsichtlich der Art und Weise der praktischen Durchführung der DSFA.



Hierzu sollen den verantwortlichen Stellen im Folgenden unverbindliche Empfehlungen an die Hand gegeben werden. Die praktische Umsetzung dieser Empfehlungen muss im Einzelfall stets unter Einhaltung der vorrangigen gesetzlichen Vorgaben erfolgen.

Die DSFA kann nach positiver Beantwortung der Vorfrage, ob die betrachtete Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge haben wird, in vier Hauptprozessschritte unterteilt werden: 1. Vorbereitung, 2. Durchführung, 3. Umsetzung, 4. Überprüfung.

Im Zuge der vorstehend erläuterten kontinuierlichen Fortschreibung kann es erforderlich sein, diese Prozesskette wiederholt zu durchlaufen. Die Umsetzung und Überprüfung der DSFA dienen der Implementierung der Abhilfemaßnahmen und sollten nicht lediglich linear durchlaufen werden, sondern eine Rückkopplung der jeweiligen Ergebnisse im Sinne eines iterativen Vorgehens ermöglichen. Beispielsweise können durch eine Maßnahme weitere Verarbeitungsvorgänge nötig werden, für die wiederum etwaige Risiken zu betrachten sind.

Vorbereitung

1) Zusammenstellung eines DSFA-Teams

   Die Durchführung einer DSFA wird in vielen Fällen ein interdisziplinäres Team erfordern. Regelmäßig werden Kompetenzen in den Bereichen Datenschutzrecht, IT, Risikoermittlung sowie Kompetenzen in den im Einzelfall relevanten Fachprozessen benötigt. Der oder die örtlich Beauftragte steht diesem Team während des gesamten Prozesses beratend zur Seite. Es kann außerdem sinnvoll oder notwendig sein, Externe wie zum Beispiel Auftragsverarbeiter oder Hersteller von IT-Systemen ebenfalls mit einzubeziehen.

2) Prüfplanung

   Da eine DSFA in den meisten Fällen ein komplexer Prozess ist, der viele Mitwirkende umfasst, ist eine Prüfplanung (zum Beispiel mit Methoden des Projektmanagements) empfehlenswert.

3) Festlegung des Beurteilungsumfangs (Scope)

   Die betrachteten Verarbeitungsvorgänge sind von anderen Prozessen im Verantwortungsbereich der verantwortlichen Stelle abzugrenzen und ausführlich sowie abschließend mit allen Datenflüssen zu beschreiben. Wesentlich ist es, die beabsichtigten Zwecke der Verarbeitungsvorgänge festzuhalten. Vergleiche hierzu § 34 Abs. 4 Nr. 1 DSG-EKD.

4) Identifikation und Einbindung von Akteuren und betroffenen Personen

   Die relevanten Akteure und betroffenen Personen sind zu identifizieren. Bei der Durchführung der DSFA zieht die verantwortliche Stelle die oder den örtlich Beauftragte/n zurate (§ 34 Abs. 2 DSG-EKD). Des Weiteren kann eine Einbindung von Gremien der Mitbestimmung wie zum Beispiel der Mitarbeitervertretung erforderlich sein.

5) Bewertung der Notwendigkeit/Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf ihren Zweck

Die im vorherigen Schritt beschriebenen Verarbeitungsvorgänge werden ausgehend von den mit ihnen verfolgten Zwecken daraufhin bewertet, ob der durch sie bewirkte Eingriff in die Rechte und Freiheiten der betroffenen Personen im Verhältnis zu dem angestrebten Zweck steht, ob sie zum Erreichen der Zwecke tatsächlich notwendig sind oder ob alternative Vorgehensweisen zur Verfügung stehen, die in die Rechte und Freiheiten der betroffenen Personen weniger stark eingreifen. Vergleiche hierzu § 34 Abs. 4 Nr. 2 DSG-EKD. Erforderlichenfalls nimmt die verantwortliche Stelle eine Anpassung der Verarbeitungsvorgänge vor, zum Beispiel durch Beschränkung der zu verarbeitenden Daten oder durch Änderung der beteiligten Akteure oder eingesetzten Technologien.

6) Identifikation der Rechtsgrundlagen

Aufbauend auf dem vorherigen Schritt können sodann die Rechtsgrundlagen für die zu bewertenden Verarbeitungsvorgänge bestimmt und dokumentiert werden.

Durchführung

7) Modellierung der Risikoquellen

Die Quellen des Risikos für die Rechte und Freiheiten natürlicher Personen müssen identifiziert werden. Insbesondere ist zu bestimmen, welche Personen motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen, und welches ihre Beweggründe und möglichen Ziele sein können. Anhand dessen können die damit zusammenhängenden Eintrittswahrscheinlichkeiten ermittelt werden.

8) Risikobeurteilung

Aufbauend auf den vorherigen Schritten wird bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Vergleiche hierzu § 34 Abs. 4 Nr. 3 DSG-EKD. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Ihre Schwere sowie ihre jeweilige Eintrittswahrscheinlichkeit sind zu berücksichtigen.

9) Auswahl geeigneter Abhilfemaßnahmen

Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen (insbesondere durch technische und organisatorische Maßnahmen (TOMs)) eingedämmt werden. Eine Auswahl sowie Planung der Umsetzung der Maßnahmen findet statt. Dabei wird den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen. Verbleibende Restrisiken werden ermittelt und dokumentiert.

10) Erstellung des DSFA-Berichts

Der DSFA-Bericht muss mindestens die in § 34 Abs. 4 Nr. 1 bis 4 DSG-EKD geforderten Inhalte umfassen. Er kann sich dabei an den hier dargestellten Phasen orientieren.

Umsetzung

11) Umsetzung der Abhilfemaßnahmen

Bevor mit der geplanten Datenverarbeitung begonnen wird, müssen die für die Eindämmung des Risikos geeigneten Abhilfemaßnahmen (insbesondere TOMs) umgesetzt sein. Vorher darf die Verarbeitung personenbezogener Daten nicht stattfinden. Sofern sich bei der Umsetzung herausstellt, dass geplante Maßnahmen nicht (wirksam) realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt, die Restrisikobewertung angepasst oder die Verarbeitungsvorgänge insgesamt angepasst werden, so dass sie den gesetzlichen Anforderungen genügen.

12) Test der Abhilfemaßnahmen

Nachdem Abhilfemaßnahmen umgesetzt wurden, müssen sie auf ihre Wirksamkeit getestet werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

13) Dokumentation der DSFA

Gemäß § 5 Abs. 2 Datenschutz-Grundverordnung (DSGVO) hat die verantwortliche Stelle eine umfassende Dokumentations- und Rechenschaftspflicht, durch welche die Einhaltung der Grundsätze des DSG-EKD insgesamt nachgewiesen werden soll. Der DSFA-Bericht und eine Bestätigung der Wirksamkeit der umgesetzten Maßnahmen dienen als Bausteine zur Erfüllung dieser Pflicht.

14) Konsultation der Aufsichtsbehörde oder Freigabe der Verarbeitungsvorgänge

Sofern aus der DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hat, ist gemäß § 34 Abs. 9 DSG-EKD die Aufsichtsbehörde zu konsultieren.

Ist ein hohes Risiko ausgeschlossen worden, können die Verarbeitungsvorgänge mit Vorliegen der vollständigen Dokumentation formal durch die verantwortliche Stelle freigegeben werden.

Überprüfung und Fortschreibung

Bezüglich der Überprüfung und Fortschreibung wird auf den obigen Abschnitt „Zeitpunkt der Durchführung und Fortschreibung“ verwiesen.