DSFA

Ampel für den Datenschutz

[27.01.2022] Die Datenschutz-Folgenabschätzung (DSFA) bereitet vielen Kommunen Kopfzerbrechen. Der Landesbeauftragte für Datenschutz in Bayern hat eine praktikable Methode ausgearbeitet, die auch für nichtbayerische Kommunen hilfreich ist.

Der Landesbeauftragte für Datenschutz in Bayern (BayLfD) liefert auf seiner Website konkrete Hilfestellung bei der Durchführung einer Datenschutz-Folgenabschätzung (DSFA). Zu finden sind zahlreiche Dokumente, die einen Überblick über das Vorgehen bei einer DSFA geben. Außerdem gibt es Musterformulare mit Ausfüllbeispielen.
Das Dokument „Orientierungshilfe“ zeigt anhand eines Prüfschemas, wie Kommunen prüfen können, ob eine DSFA erforderlich ist, und gibt einen Überblick über die Erstellung. Das Dokument „Methodik und Fallstudie“ beschreibt die Ziele des Standard-Datenschutzmodells und zeigt, wie eine Risikoanalyse durchgeführt wird. Hier wird auch erklärt, wie man über die Risikoanalyse zur Gesamtrisikobewertung einer Datenverarbeitung gelangt und welche Mindestpositionen der DSFA-Bericht enthalten muss. Besonders anschaulich: An einem praktischen Beispiel wird eine DSFA im Personalamt der Stadt Fiktivia durchgespielt. Als Praxishilfe werden fünf Module bereitgestellt, die Musterformulare und Ausfüllbeispiele enthalten, sowohl für die Erforderlichkeitsprüfung als auch für den DSFA-Bericht und die Risikoanalyse.
Allerdings ist nicht für jede Datenverarbeitung eine DSFA erforderlich. Ob dies der Fall ist, kann man über das Formular „DSFA-Erforderlichkeitsprüfung“ auf der Website des BayLfD prüfen. Darin wird abgefragt, ob es eine Ausnahme von der Durchführung einer eigenen DSFA gibt, etwa wenn eine solche bereits für einen ähnlichen Verarbeitungsvorgang mit vergleichbaren Risiken vorliegt, oder ob der Verarbeitungsvorgang auf der Blacklist der Aufsichtsbehörde steht.

Analyse der Risikofaktoren

Verneint man diese Punkte, so folgt eine eigene Risikoabschätzung nach den „Leitlinien zur Datenschutz-Folgenabschätzung“ der europäischen Artikel-29-Gruppe. Darin wird unter anderem gefragt, ob durch die Datenverarbeitung Personen systematisch überwacht und kontrolliert werden, ob vertrauliche Daten oder Daten schutzbedürftiger Personen verarbeitet werden oder ob es sich um eine innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen handelt. Das ausgefüllte Formular „DSFA-Erforderlichkeitsprüfung“ dient als Nachweis gegenüber einer Aufsichtsbehörde, dass die Notwendigkeit einer Datenschutz-Folgenabschätzung für eine Verarbeitungstätigkeit geprüft wurde.
Ist diese notwendig, muss festgestellt werden, welche Risiken für die Rechte und Freiheiten von Personen durch die Verarbeitungstätigkeit bestehen. Dazu schlägt der BayLfD eine Analyse vor, in der - Risikoszenarien erarbeitet und Schwachstellen und Risikoquellen der Verarbeitungstätigkeit betrachtet werden. Geprüft wird, ob die Verarbeitungstätigkeit die Ziele des Standarddatenschutzmodells der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder erfüllt. Das sind zum einen Datensicherheitsziele – Verfügbarkeit, Vertraulichkeit und Datenintegrität – und zum anderen Schutz-bedarfsziele: Datenminimierung, Intervenierbarkeit, Transparenz, Nichtverkettung, Konzeptionseinhaltung und Richtigkeit. Die Zielerfüllung wird anhand eines Ampelsystems bewertet.
Nach einer ersten Risikobetrachtung sollten Maßnahmen erarbeitet werden, die Risiken minimieren. Danach wird die Verarbeitungstätigkeit ein zweites Mal bewertet. Auch hierbei wird das Ampelsystem verwendet. Die Ergebnisse der zweiten Risikoanalyse fließen als Risikogesamtbewertung in den DSFA-

Bericht ein.

Risikogesamtbewertung mit Ampelsystem

Maßnahmen, die den Risiken für die Rechte und Freiheiten von Personen entgegenwirken, lassen sich drei Kategorien zuordnen:
• Maßnahmen, die in der Software voreingestellt sind (Privacy by Default), etwa ein System zur Vergabe eines Passworts oder einer Zwei-Faktor-Authentisierung, zur Einrichtung eines Berechtigungskonzepts oder zur Protokollierung.
• Technische Maßnahmen, die im Rechenzentrum oder den Server-Räumen, in denen die Software betrieben wird, umgesetzt werden müssen (Privacy by Design). Dazu zählen zum Beispiel die regelmäßige Datensicherung, eine unterbrechungsfreie Stromversorgung oder der Einbau einer Firewall.
• Auch die Kommune selbst muss zur Risikominimierung beitragen, indem sie beispielsweise vor Ort dafür sorgt, dass die Mitarbeitenden regelmäßig Schulungen zu Datenschutz und Informationssicherheit erhalten, dass Besuchern keine Einsicht in vertrauliche Daten gewährt wird und Unberechtigte keinen Zutritt zu sicherheitsrelevanten Gebäudeteilen erhalten.
Die Zusammenfassung der Datenschutz-Folgenabschätzung erfolgt im DSFA-Bericht. Darin werden Informationen zur Verarbeitungstätigkeit gegeben und der Kontext sowie die grundlegenden Prinzipien der Datenverarbeitung beschrieben. Schließlich folgt die Risikogesamtbewertung, die aus der Risikoanalyse resultiert. Die Verarbeitungstätigkeit ist datenschutzkonform, wenn die Ampel der Risikogesamtbewertung auf Grün oder Gelb steht. Steht die Ampel dagegen auf Rot, muss der Datenverarbeitungsvorgang noch einmal gründlich überprüft oder der Rat der Aufsichtsbehörde eingeholt werden. Der DSFA-Bericht listet am Ende alle Maßnahmen zur Risikominimierung noch einmal auf, die in der Risikoanalyse festgelegt wurden.

()

Dokumentationen, Muster und Ausfüllbeispiele zur Datenschutz-Folgenabschätzung finden Sie hier.
Dieser Beitrag ist im Titel der Ausgabe Januar 2022 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Datenschutz, DSFA, Bayern, BayLfD