Bewertung der Ergebnisse des Standards ISO 29134 zur Durchführung einer DSFA nach Artikel 35 DS-GVO

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat das Planspiel „Pay-As-You-Drive“ auf Basis der ISO 29134 durchgeführt. Im ersten Schritt wurde festgelegt – was eigentlich selbstverständlich ist – dass Vorgaben der DS-GVO vollständig und im Zweifel vorrangig zum ISO-Standard umzusetzen sind.

Die ISO 29134 beinhaltet den zentralen Begriff des Risikos, das mittels einer Risikobeurteilung ermittelt und eingedämmt werden soll. Dabei lässt die Norm ausreichend Raum, um eine Risikomodell nach DS-GVO zu entwickeln und zu verwenden. Als Empfehlung sei an dieser Stelle auf das Kurzpapier „Risiko der Rechte und Freiheiten “ verwiesen.

Das BayLDA modellierte die einzelnen Datenschutzrisiken ausgehend von den einzelnen Risiko-Ursachen („Risk sources“). Obwohl dies eine möglichst vollständige Erhebung aller Varianten von Risiken für eine Verarbeitungstätigkeit verspricht, kann die Anzahl der Kombinationen sehr schnell recht umfangreich werden. Aus diesem Grund empfiehlt das BayLDA – analog zum Kurzpapier Risiko (siehe vorheriger Absatz) - zuerst verschiedene Risiken anhand von Expertenwissen sowie gesundem Menschenverstand festzulegen und bei der Ermittlung der Eintrittswahrscheinlichkeiten und der Schwere eines möglichen Schadens die Risiko-Ursachen zu modellieren und zu bewerten.

Ergebnis:

- Das BayLDA kommt zu dem Ergebnis, dass die Norm ISO 29134 – sofern richtig angewendet – eine angemessene Vorgehensweise zur Durchführung einer DSFA darstellt.

- Das BayLDA kommt zu dem Ergebnis, dass auch das Standard-Datenschutzmodell (Version 1.1) für eine DSFA verwendet werden kann, sofern ausreichende Security-Maßnahmen flankierend vorhanden sind.

- Ein zentrales Element bei der Durchführung einer DSFA ist das richtige Verständnis des Datenschutzrisikos – in Unterschied zum Unternehmensrisiko, das Unternehmenswerte (Assets), nicht aber primär Grundrechte adressiert.

- Es müssen neben den Security-Schutzzielen (Vertraulichkeit, Verfügbarkeit und Integrität) auch sogenannte Gewährleistungsziele (für Datenminimierung, Zweckbindung, Transparenz und Sicherstellung Betroffenenrechte) zur Risikobeurteilung und - eindämmung abgebildet werden.

- Eine systematische und ausführliche Beschreibung der Datenflüsse, Akteure und technischer Systeme bildet die Basis für eine DSFA.

- Eine DSFA kann nur von einem spezialisierten DSFA-Team durchgeführt werden – der Datenschutzbeauftragte berät „nur“.

- Eine DSFA nach DS-GVO kann ein wirksames Instrument zur Behandlung von Hochrisikoverarbeitungen sein, bei denen Artikel 25 DS-GVO (Privacy by Design) und Artikel 32 DS-GVO (Security) alleine nicht ausreichen, um das Datenschutzrisiko nachweisbar einzudämmen.

Weitere Schritte:

Das BayLDA arbeitet momentan an Anwendungshinweisen zur Umsetzung einer DSFA mittels der ISO 29134 für die Datenschutzgrundverordnung. Diese wird vermutlich im Herbst 2019 auf der Webseite des BayLDA veröffentlicht.