Datenschutzfolgenabschätzung und Schwellwertanalyse

Die DSGVO verfolgt einen risikoorientierten Ansatz. Das bedeutet, jene Datenverarbeitungen, welche ein Unternehmen betreibt, sind in Bezug auf ein mögliches Risiko für die Rechte und Freiheiten von Betroffenen zu überprüfen. Das von der DSGVO vorgesehene Instrument für die Analyse und Bewertung der Risiken ist die sogenannte Datenschutz-Folgenabschätzung (DSFA). Die einschlägigen Regelungen dazu sind vor allem im Artikel 35 DSGVO enthalten. Die näheren inhaltlichen Vorgaben zur DSFA werden wir in einem gesonderten Beitrag beschreiben und erläutern.

Ob eine DSFA tatsächlich durchzuführen ist, ergibt sich aus einer Vorabeinschätzung der Risiken, die allgemein als Schwellwertanalyse bezeichnet wird. Dabei wird die jeweilige Datenverarbeitung an Hand eines Kriterien-Kataloges geprüft, ob eine DSFA zu erstellen ist.

An dieser Stelle wollen wir Aspekte der Schwellwertanalyse behandeln, die es den Verantwortlichen, also den Unternehmern und den Geschäftsführern, ermöglichen, sich darüber ein Bild zu machen, welches Risiko mit der Verarbeitung verbunden ist. Wenn die Schwellwertanalyse das Ergebnis erbringt, dass mit der Verarbeitung kein hohes Risiko verbunden ist, ist damit der Prozess abgeschlossen und die Verarbeitung kann erfolgen.

Die maßgeblichen Kriterien richten sich nach der DSGVO, nach dem Datenschutzgesetz (DSG) und nach der Verordnung der Datenschutzbehörde zu Verarbeitungen, für die eine Ausnahme von der DSFA-Pflicht besteht (White-List) sowie der Verordnung der Datenschutzbehörde zu Verarbeitungen, für die eine DSFA-Pflicht besteht (Black-List).

Die DSGVO nennt die drei Faktoren, die wahrscheinlich zu einem hohen Risiko führen, und zwar:

a) die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen

b) die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten und

c) die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Zur Erleichterung der Einschätzung wurde vom Europäischen Datenschutzausschuss eine Leitlinie verabschiedet, die neun Kriterien nennt, die für eine DSFA-Pflicht sprechen, soweit sie zutreffen. Diese stellen wir weiter unten zur Verfügung.

Eine korrekt erstellte DSFA ist keine optionale Tätigkeit, sondern bringt dem Unternehmen die Rechtsgrundlage für die erlaubte Verarbeitung von personenbezogenen Daten. Eine unterlassene DSFA stellt einen Verstoß gegen die DSGVO dar, womit die Datenverarbeitung nicht rechtskonform ist, was das Risiko eines Bußgeldes nach sich zieht.

Die wichtigsten und häufigsten Kriterien aus der Praxis sollen hier in Form eines Quick-Check angeführt werden. Sollten sie als Verantwortlicher bei ihrer Analyse feststellen, dass diese Kriterien erfüllt sind, empfehlen wir ihnen, dies mit einem Mitglied des Vereins der Kärntner Datenschutzexpert:innen zu besprechen, um ehestmöglich ein entsprechendes rechtskonformes Vorgehen auszuarbeiten und festzulegen.

Wie erstelleicheine Schwellwertanalyse?

Bei neuen Verarbeitungen sieht die DSGVO vor, dass bereits vor Beginn der Verarbeitung eine Risikoabschätzung erfolgen muss. Bei bestehenden Datenverarbeitungen kann sich die Notwendigkeit der Überprüfung bei wesentlichen Veränderungen der Verarbeitung ergeben. Grundsätzlich müsste also die Verarbeitung bereits im Verzeichnis der Verarbeitungstätigkeiten erfasst sein, wenn sie sich bereits im Einsatz befindet. Darauf kann bei der Schwellwertanalyse aufgebaut werden. Eine Überprüfung hat aber auch nachträglich Sinn, wenn sich beispielsweise aufgrund von neuen Informationen eine Veränderung der Risikoeinschätzung ergibt. Dies trifft zum Beispiel auf das EuGH Urteil zu, das unter der Bezeichnung Schrems II bekannt ist. Wegen der Ungültigkeit des Angemessenheitsbeschlusses zum Privacy-Shield-Abkommen muss die Übertragung von Daten in die USA auf eine neue Rechtsgrundlage gestellt werden.

Ausgangspunkt der Beurteilung ist die Beschreibung der Datenverarbeitung und die Überprüfung der tragfähigen Rechtsgrundlage gem. Art 6 bzw. Art 9 DSGVO und die Überprüfung der Regelungen aus der White-List (DSFA-AV). Ist nämlich eine Ausnahme gemäß DSFA-Ausnahmeverordnung anwendbar, ist die Prüfung damit auch schon wieder abgeschlossen und dies muss nur noch in diesem Sinn dokumentiert werden. Ist jedoch keine Ausnahme anwendbar, ist im Anschluss zu prüfen, ob die maßgeblichen Kriterien für eine DSFA-Pflicht zutreffen oder nicht. Dies hat risikoorientiert in Bezug auf die Rechte und Freiheiten der Betroffenen zu erfolgen.

Die nachstehend angeführten Kriterien und Kontrollfragen stellen nach unserer Einschätzung einen ausreichenden Querschnitt dar, um für gängige Datenverarbeitungen eine allgemeine Aussage treffen zu können. Ein vollständiger Kriterienkatalog mit allen theoretisch möglichen Aspekten würde für einen Quick-Check nicht angemessen sein, da dieser Katalog zahlreiche zusätzliche Fragen umfassen müsste. Daher erscheint die Eingrenzung auf ausgewählte Fragen ausreichend, um den interessierten Unternehmen eine erste Orientierungsmöglichkeit zu geben.

<u>Auswertung und Schlussfolgerung:</u>

Wird aus den in der beigefügten Checkliste aufgeführten Kriterien mindestens eine Kontrollfrage mit Ja beantwortet, ist davon auszugehen, dass eine Pflicht zur DSFA besteht. Der Verantwortliche hat dann darüber zu entscheiden, ob aufgrund der getätigten Feststellungen eine DSFA erstellt wird. Jedenfalls benötigt er aber eine entsprechende Dokumentation zu seiner Entscheidungsfindung und Vorgangsweise.

Die Mitglieder des Vereins der Kärntner Datenschutzexpert:innen stehen für die Klärung von Spezialfragen bzw. eine ausführliche Beratung gerne zur Verfügung, denn dieser allgemeine Beitrag kann eine individuelle Beratung nicht ersetzen.

Walter Wratschko **Rudolf Urban**

der Scout DATENSCHUTZ | DATENSICHERHEIT

DATAEXPERT DAS TEAM FÜR IHREN DATENSCHUTZ

Geprüfte Datenschutzexperten