C-IAM GmbH: Industrie 4.0 - Mehr Erfolg durch Risikomanagement

KW 3: EU Datenschutz Grundverordnung 2018 von Joachim Jakobs (https://blog.c-iam.com)

Der Begriff „Risiko“ wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert Link „als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens“.

Risikomanagement in der DSGVO

Dieser Begriff ist für die Chefs essentiell, wenn sie ihrer Rechenschaftspflicht aus der Datenschutzgrundverordnung (DSGVO) nachkommen wollen – Artikel 32 Link Absatz 1 DSGVO verlangt von dem Verantwortlichen und dem Auftragsverarbeiter „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Dabei sollen der „Stand der Technik“, die „Implementierungskosten“ und die „Art“, der „Umfang“, die „Umstände“ und die „Zwecke der Verarbeitung“ sowie die unterschiedliche „Eintrittswahrscheinlichkeit“ und die „Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“ berücksichtigt werden.

Absatz 2 dieses Artikels fordert außerdem eine „Beurteilung des angemessenen Schutzniveaus“; dabei müssten die Risiken berücksichtigt werden, die mit der Verarbeitung „unbeabsichtigt oder unrechtmäßig“ einhergingen – „insbesondere durch Vernichtung, Verlust oder Veränderung“. Ausdrücklich wird auch auf den „unbefugten Zugang zu personenbezogenen Daten“ hingewiesen, „die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden“.

- Erwägungsgrund 75 Link DSGVO präzisiert für die Verarbeiter personenbezogener Daten die „Risiken für die Rechte und Freiheiten natürlicher Personen“, „die zu einem physischen, materiellen oder immateriellen Schaden führen“ könnten. Dabei sei mit „unterschiedlicher Eintrittswahrscheinlichkeit und Schwere“ der Risiken zu rechnen, „insbesondere wenn die Verarbeitung zu
- einer Diskriminierung,
- einem Identitätsdiebstahl oder -betrug,
- einem finanziellen Verlust,
- einer Rufschädigung,

- einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann“

Solche Nachteile seien zu befürchten, wenn Daten verarbeitet würden, aus denen

- „die rassische oder ethnische Herkunft“,
- „politische Meinungen“,
- „religiöse oder weltanschauliche Überzeugungen“
- „die Zugehörigkeit zu einer Gewerkschaft“
- „genetische Daten“
- „Gesundheitsdaten“
- „das Sexualleben“
- „strafrechtliche Verurteilungen und Straftaten“

hervorgingen. Nachteile könnten außerdem entstehen, wenn „persönliche Aspekte“ „analysiert oder prognostiziert werden“, „um persönliche Profile zu erstellen oder zu nutzen“. Zu diesen persönlichen Aspekten zählen

- die „Arbeitsleistung“,
- die „wirtschaftliche Lage“
- die „Gesundheit“
- „persönliche Vorlieben“
- „Interessen“
- „Zuverlässigkeit“
- „Verhalten“
- „Aufenthaltsort oder Ortswechsel“.

Hohe Risiken verlangen nach einer Datenschutz-Folgenabschätzung

Und schließlich sei mit Nachteilen zu rechnen, wenn es sich bei den Betroffenen um „Schutzbedürftige“ – „insbesondere Link Kinder“ – handele. Mit Nachteilen sei auch zu rechnen, wenn „eine große Menge personenbezogener Daten“ verarbeitet würde oder „eine große Anzahl“ von Personen betroffen sei. Erwägungsgrund 76 fordert Link die Beurteilung des Risikos „anhand einer objektiven Bewertung“ – damit soll bestimmt werden, „ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt“. Sollte es sich um ein hohes Risiko handeln, ist nach Artikel 35 Link eine „Datenschutz-Folgenabschätzung“ (DSFA) notwendig. Sie ersetzt die bisherige Vorabkontrolle aus § 4d (5) BDSG Link .

Nach Artikel 35 (3) ist eine DSFA „insbesondere in folgenden Fällen erforderlich“ – nämlich wenn es sich um eine

a. „systematischee und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
b. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
c. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche“

handelt.

Die Aufsichtsbehörden sollen dazu eine Liste von Verarbeitungsvorgängen erstellen, für die eine DSFA erforderlich sein soll (Art. 35 (4) DSGVO), oder können außerdem auch eine Liste von Verarbeitungsvorgängen erstellen, für die keine DSFA notwendig ist (Art. 35 (5) DSGVO).

Nach Absatz 7 enthält die DSFA „zumindest Folgendes“:

a. „eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
b. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d. 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 diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.“

Risikomanagements im Verkehrswesen – früher und heute

Um zu verstehen, was das für Ihr Unternehmen bedeutet, müssen Sie sich klarmachen, was mit den Risiken gemeint ist, die mit der Verarbeitung „unbeabsichtigt oder unrechtmäßig“ einhergehen:

Zum Weiterlesen des gesamten Artikels klicken Sie bitte auf:

http://blog.c-iam.com

Kontakt

Jamshed Kharkan
Geschäftsführer

Tel: +49 228 53459235
E-Mail: info@c-iam.com
blog@c-iam.com

C-IAM GmbH
Ballindamm 39
D-20095 Hamburg

https://www.c-iam.com
https://blog.c-iam.com