datenschutz-berater.de

45. Jahrgang

DSB 07+08/2021

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Interview

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Olaf Rossow

Die Risikoanalyse nach Artikel 32 DSGVO

Jedes Unternehmen ist nach der DSGVO verpflichtet, angemessene Maßnahmen zum Schutze personenbezogener Daten zu treffen. Damit ein Unternehmen beurteilen kann, welche Maßnahmen getroffen werden müssen oder ob vorhandene Maßnahmen ausreichen, ist es vom Verordnungsgeber aufgefordert eine Risikoanalyse durchzuführen. So sollen Risiken, die sich bspw. aus einem unbefugten Zugriff auf Gesundheitsdaten ergeben könnten, erkannt und bewertet werden können sowie geprüft werden, ob vorhandene Schutzmaßnahmen ausreichen oder entsprechend nachgesteuert werden muss. Die Risikoanalyse ist damit die Ausgangsposition für eine datenschutzkonforme Verarbeitung personenbezogener Daten.

Voraussetzungen für eine Risikoanalyse

Bevor eine Risikoanalyse durchgeführt werden kann, ist zunächst die Verarbeitungstätigkeit zu beschreiben und es sind die rechtlichen Grundlagen zu prüfen, da ohne gültige Rechtsgrundlage schon keine datenschutzkonforme Verarbeitung erfolgen kann. Dies geschieht beim Einfügen relevanter Informationen in das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO. Die Informationen aus dem Verzeichnis einschließlich der darin durchgeführten Beschreibungen und rechtlichen Prüfungen sind Ausgangspunkt und die Voraussetzung für die Durchführung einer adäquaten Risikoanalyse.

Beschreibung der Verarbeitungstätigkeit personenbezogener Daten

Der Verantwortliche ist nach Art. 30 DSGVO verpflichtet, ein Verzeichnis über die Verarbeitungstätigkeit zu führen, bei denen personenbezogenen Daten verarbeitet werden. Durch das Verzeichnis werden die Prozesse identifiziert und beschrieben, innerhalb derer personenbezogene Daten verarbeitet werden. Neben der Beschreibung des tatsächlichen Prozessablaufs, der Datenkategorien, des Zwecks, der Betroffenen und anderer vorgeschriebenen Angaben aus Art. 30 DSGVO, ist auch die Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO für eine Risikoanalyse erforderlich.

Technische und organisatorische Maßnahmen sind Vorkehrungen, die getroffen werden, um die personenbezogenen Daten vor unbefugten Zugriffen, Verlust, Zerstörung etc. zu schützen und eine rechtskonforme Verarbeitung sicherzustellen. Unter technischen Maßnahmen sind alle Schutzmaßnahmen zu verstehen, die im weitesten Sinne physisch umsetzbar sind, wie etwa die Umzäunung des Geländes, Sicherung von Türen und Fenstern, bauliche Maßnahmen allgemein, Alarmanlagen jeglicher Art, oder Maßnahmen die in Soft- und Hardware umgesetzt werden, wie etwa Benutzerkonto, Passwortvorgaben, Logging (Protokolldateien) oder ggf. sogar eine biometrische Benutzeridentifikation. Als organisatorische Maßnahmen sind solche Schutzmaßnahmen zu verstehen, die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden. Beispiele hierfür sind interne Richtlinien oder Arbeitsanweisung, Besucheranmeldung, Vier-Augen-Prinzip oder festgelegte Intervalle zur Stichprobenprüfungen.

Prüfung der Rechtsgrundlagen

Die Prüfung der Rechtmäßigkeit der Verarbeitungstätigkeit ist eine weitere Voraussetzung für eine Risikoanalyse. Für die Rechtmäßigkeit der Verarbeitung bedarf es einer Rechtsgrundlage. Wenn schon keine rechtmäßige Datenverarbeitung vorliegt, dann verstößt diese ohnehin gegen die DSGVO und eine Risikoanalyse erübrigt sich dann oder kann nur dazu dienen, Maßnahmen zur rechtskonformen Ausgestaltung der Datenverarbeitung zu identifizieren.

Risikoanalyse

Das Ziel der Risikoanalyse ist die Identifikation von Schwachstellen in der Verarbeitung von personenbezogenen Daten. Die Risikoanalyse selbst unterteilt sich in fünf Schritte. Im ersten Schritt ist zu prüfen, welche Vorfälle eintreten und welche möglichen Schäden daraus resultieren könnten.

Identifikation der Risiken

Zunächst betrachtet man den möglichen Schaden. Hiermit beginnt man, um von vornherein nur solche Ereignisse und Handlungen zu betrachten, die für den möglichen Schaden relevant sind. Andernfalls müsste man am Ende Szenarien wieder aussortieren, da sie aufgrund eines fehlenden möglichen Schadens für die Risikoanalyse keine Relevanz besitzen.

Die DSGVO zählt beispielhaft im ErwGr. 75 folgende mögliche Schäden auf:

- Diskriminierung, Identitätsdiebstahl oder -betrug,
- finanzieller Verlust, Rufschädigung,
- wirtschaftliche oder gesellschaftliche Nachteile,
- Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen,

- Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten,
- Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte,
- körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter oder offengelegter Daten.

Dabei muss im Blick behalten werden, dass es um mögliche Schäden der betroffenen Person und nicht um Schäden für Verantwortliche und Auftragsverarbeiter geht.

Beispiel: Die Telefonnummer der betroffenen Person könnte missbraucht werden, um Kontakt mit ihr aufzunehmen, sich als das Beratungsunternehmen auszugeben und einen Betrugsversuch zu unternehmen. Dazu können auch die Angaben zum Gesundheitszustand dienlich sein. Ebenso könnten die Angaben zum Gesundheitszustand und die Adresse genutzt werden, um eine Hilflosigkeit für einen Einbruch auszunutzen. Mögliche Schäden sind bspw. finanzieller Verlust durch Vermögensschäden (Betrug, Einbruch), Stigmatisierung oder ggf. Erpressungsversuch aufgrund des Gesundheitszustandes, Belästigungen durch Anrufe.

Wenn nun ein möglicher Schaden für die betroffene Person ermittelt wurde, stellt sich die Frage, wie es zu diesem Schaden kommen könnte. Der Schaden kann insbesondere dann entstehen, wenn der Verantwortliche

- gegen die Datenschutzgrundsätze nach Art. 5 Abs. 1 DSGVO verstößt oder
- die Rechte der betroffenen Personen nach Art. 12 f. DSGVO missachtet.

Daraus ergeben sich dann unter anderem folgende relevante Ereignisse, die zu einem Schaden führen können und im Kurzpapier Nr. 18 der Datenschutzkonferenz (DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Stand 26.4.2018) niedergelegt sind:

- unbefugte oder unrechtmäßige Verarbeitung,
- Verarbeitung wider Treu und Glauben,
- für den Betroffenen intransparente Verarbeitung,
- unbefugte Offenlegung von und Zugang zu Daten,
- unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten,
- Verweigerung der Betroffenenrechte,
- Verwendung der Daten durch den Verantwortlichen zu Zwecken, die nicht auf eine Rechtsgrundlage aus Art. 6 DSGVO gestützt werden können,
- Verarbeitung von Daten, die nicht angefordert wurden,
- Verarbeitung nicht richtiger Daten,
- Verarbeitung über die Speicherfrist hinaus.

Darüber hinaus kann es weitere Ereignisse geben, die Schäden auslösen können. Weitere Beispiele aus Sicht der Informationssicherheit, die sich auf den Datenschutz übertragen lassen, finden sich im Grundschutzkompendium des Bundesamtes für Sicherheit in der Informationstechnik unter der Rubrik „Elementare Gefährdungen“ (BSI, IT-Grundschutz- Kompendium, Stand Februar 2021).

Weiter stellt sich die Frage, wie das Ereignis ausgelöst werden kann. Eine Handlung, die das entsprechende Ereignis auslöst, kann z. B. sein:

- der unbefugte Zugriff auf personenbezogene Daten,
- die ungewollte Modifikation von personenbezogenen Daten oder
- das ungewollte oder unbefugte Löschen von personenbezogenen Daten.

Ein Umstand wäre z. B. der Diebstahl oder Verlust eines Datenträgers. Eng verknüpft mit der Handlung und dem Umstand ist der Auslöser eines Schadens.

Der Auslöser bringt mit seiner Handlung oder dem hervorgerufenen Umstand das Ereignis ins Rollen, das am Ende zu einem Schaden führen kann. Er ist damit die Quelle, die erst das Risiko hervorruft. Solche Auslöser können z. B. sein:

- Beschäftigte beim Verantwortlichen oder Auftragsverarbeiter (bewusst oder unabsichtlich),
- Angreifer von außen oder
- äußere Einflüsse (Umwelt, höhere Gewalt).

Beispiel: Ein Einbrecher (Auslöser) bricht das Fahrzeug des Außendienstmitarbeiters auf, während dieser eine Pause in einem Restaurant einlegt, und stiehlt (Handlung) den Laptop aus dem Fahrzeug und nimmt Zugriff (Handlung) auf die Daten auf der unverschlüsselten Festplatte.

Schwere des möglichen Schadens

Bis zu diesem Punkt wurde das Risiko identifiziert. Nun ist im zweiten Schritt, die Schwere der Auswirkung des Schadens für die betroffene Person zu bewerten. Dazu gibt der ErwGr. 76 der DSGVO vor, dass die Schwere des möglichen Schadens mit Blick auf Art und Umfang, die Umstände und den Zweck der Datenverarbeitung bestimmt werden soll.

Für die bessere Einschätzung und Kategorisierung der Schwere des möglichen Schadens kann auf das Schutzstufenkonzept der LfD Niedersachsen (LfD Niedersachsen, Schutzstufenkonzept der LfD Niedersachsen, Stand Oktober 2018) zurückgegriffen werden. Dieses sieht vier Kategorien für die Schwere eines möglichen Schadens vor (geringfügig, überschaubar, substantiell und groß), beschreibt die Art der Daten abstrakt und gibt Beispiele für die Datenarten.

Beispiel: Sind bspw. Kontakt- und Gesundheitsdaten (Art. 9-Daten) betroffen, führt die Kombination dieser Da-

ten theoretisch möglicherweise dazu, dass die betroffene Person Opfer eines Verbrechens werden kann. Eine erhebliche Beeinträchtigung der Person und auch eine körperliche Beeinträchtigung können nicht ausgeschlossen werden. Daher ist die Schwere des möglichen Schadens als „substanziell" einzustufen.

Vorhandene technische und organisatorische Maßnahmen

Im dritten Schritt geht es um in der Regel bereits bestehende technische und organisatorische Maßnahmen zur Datensicherheit, wie zum Beispiel ein abgesicherter Serverraum oder Virenscanner auf Endgeräten. Diese haben Auswirkungen auf den Eintritt eines möglichen Schadensereignisses. Daher sind an dieser Stelle die vorhandenen Maßnahmen zu identifizieren, um die Eintrittswahrscheinlichkeit bewerten zu können.

Abschätzung der Eintrittswahrscheinlichkeit

Es stellt sich im vierten Schritt die Frage, mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis eintreten könnte, das entweder selbst ein Schaden ist oder zu einem Schaden führt. Außerdem ist zu klären, mit welcher Wahrscheinlichkeit es zu Folgeschäden kommen kann. Hier soll – wie bei der Schwere des Schadens – die Eintrittswahrscheinlichkeit mit Blick auf Art und Umfang, die Umstände und den Zweck der Datenverarbeitung bestimmt werden.

Um die Eintrittswahrscheinlichkeit entsprechend einschätzen zu können, können folgende Kriterien der Orientierungshilfe „Vorabkontrolle" der LfD Niedersachsen (LfD Niedersachsen, Vorabkontrolle leicht gemacht, Stand 3.7.2001) unterstützen:

- Umfang der Verarbeitung,
- Präsenz von Gefährdungslagen.
- Risiko, beim Missbrauch entdeckt zu werden,
- Aufwand, um Schäden herbeizuführen,
- statistische Erhebungen/Studien,
- Missbrauchsinteresse eines Schädigers.

Dabei ist zu berücksichtigen, dass die Kriterien nicht isoliert voneinander betrachtet werden, sondern die Wechselwirkungen zu beachten sind. So kann es die Eintrittswahrscheinlichkeit erhöhen, wenn das Risiko entdeckt zu werden gering und das Missbrauchsinteresse des Schädigers hoch ist. Sollte das Entdeckungsrisiko aber hoch sein, dann muss das Missbrauchsinteresse des Schädigers so weit gehen, dass er das Entdeckungsrisiko eingehen will. Neben diesen Kriterien, sind bereits getroffene Maßnahmen zu berücksichtigen. Diese Maßnahmen können sich auf die Eintrittswahrscheinlichkeit auswirken.

Beispiel: Nach einer Studie aus dem Jahr 2017 sind knapp ein Drittel der Unternehmen von einem Laptop- oder Smartphone-Diebstahl betroffen. Der Diebstahl eines Laptops ist daher realistisch. Eine gesonderte organisatorische Maßnahme, womit die Außendienstmitarbeiter angewiesen werden, den Laptop immer bei sich zu haben, besteht im Beispiel nicht. Weiter besteht für Schädiger kein großer Aufwand, die Festplatte des Laptops zu entnehmen. Der Zugriff auf Daten auf der Festplatte wird dadurch erleichtert, dass die Daten unverschlüsselt sind. Das Risiko, dass man beim Missbrauch der Daten entdeckt wird, ist im konkreten Fall als gering einzustufen.

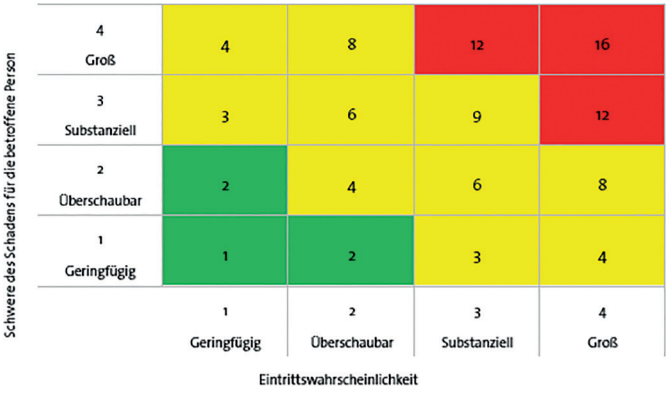
Für eine Risikobewertung ist es sinnvoll, das Ergebnis der Einschätzung zu kategorisieren, um später einen Risikowert mit den Kategorien der Schwere des möglichen Schadens bilden zu können. So können auch hier vier Kategorien gebildet werden (geringfügig, überschaubar, substantiell und groß). Für eine Risikoquelle (Umstand oder Handlung) scheint es dabei nicht sehr wahrscheinlich, schwierig, möglich, oder einfach zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen.

Beispiel: Da der Diebstahl eines Laptops realistisch ist, im hier gewählten Beispiel keine großen technischen Hürden bestehen, auf die Daten der Festplatte Zugriff zu nehmen und das Entdeckungsrisiko als gering einzuschätzen ist, ist die Eintrittswahrscheinlichkeit als „groß" einzustufen.

Ermittlung des Risikowerts

Im fünften und letzten Schritt werden aus dem Produkt der Gewichtung des möglichen Schadens und der Gewichtung der Eintrittswahrscheinlichkeit Risikoklassen gebildet.

Hierzu ist es sinnvoll, sich am Gesetzestext zu orientieren, der ein „Risiko" und ein „hohes Risiko" kennt. Daneben kann auch noch die Risikoklasse „geringes Risiko" gebildet werden, was in einer Matrix folgendermaßen aussähe:



Beispiel: Im konkreten Fall des gestohlenen Laptops wurde die Schwere des Schadens als „substanziell" und die Eintrittswahrscheinlichkeit als „groß" eingestuft. Dies ergibt einen Risikowert von „12" und damit ein „hohes Risiko" für die Datenverarbeitung.

Konsequenzen aus der Risikoanalyse

Nachdem ein Risikowert ermittelt worden ist, stellt sich die Frage nach den Konsequenzen. Das Standard-Datenschutzmodell 2.0b der Aufsichtsbehörden (DSK, Das Standard-Datenschutzmodell, Version 2.0b, beschlossen am 17.04.2020) verweist in diesem Zusammenhang darauf, dass eine Risikoakzeptanz oder ein Risikotransfer – wie im Bereich der Informationssicherheit – im datenschutzrechtlichen Kontext nicht zur Verfügung steht. Es bestehe aber ein Spielraum bei der Auswahl und der Art und Weise der Umsetzung von Anforderungen mit Hilfe von technischen und organisatorischen Maßnahmen, die in einem angemessenen Umfang gefordert werden.

Erst wenn das nach Art. 32 DSGVO geforderte angemessene Schutzniveau erreicht wurde und somit die Interessen und Rechte der Betroffenen angemessen berücksichtigt sind, könnten verbleibende Restrisiken durch den Verantwortlichen weiter gemindert oder eben akzeptiert werden. Die Risikoeinstufung kann daher nur eine Orientierung geben. Bei jeder Art der Einstufung ist zu prüfen, ob ein angemessenes Schutzniveau vorliegt und es sind die Empfehlungen der Aufsichtsbehörden zu berücksichtigen. Bei der Einstufung als „hohes Risiko“ schreibt die DSGVO vor, dass Rahmen einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO Maßnahmen zur Risikominimierung zu ergreifen sind. Soweit ein „Risiko“ ermittelt wurde, ist im Einzelfall zu bewerten, ob Empfehlungen der Aufsichtsbehörden umgesetzt und auch Standards der Informationssicherheit nach dem BSI berücksichtigt worden sind. Sollte dies der Fall sein, kann bei einer entsprechenden Begründung von einem Restrisiko gesprochen werden, dass der Verantwortliche akzeptiert. Das Ziel ist es, ein angemessenes Schutzniveau zu erreichen.

Maßnahmen zur Risikominimierung

Um die Risiken zu minimieren, kann ein Risikobehandlungsplan hilfreich sein. Er erfasst alle identifizierten Gefährdungen und deren ermittelte Risiken aus der Risikoanalyse. Für die Risiken wird die Risikobehandlungsoption, die geplanten Maßnahmen, der Umsetzungsverantwortliche (risk owner) und der geplante Umsetzungszeitpunkt festgelegt.

Bei den auszuwählenden Maßnahmen zur Risikovermeidung sind folgende Punkte zu beachten:

- der Risikowert (Ermittelte Wert aus Gewichtung des möglichen Schadens und der Gewichtung der Eintrittswahr-scheinlichkeit)
- Stand der Technik (Entwicklungsstand, der die Eignung einer Schutzmaßnahme gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt
- Implementierungskosten

Beispiel: Nachdem ein „hohes“ Risiko identifiziert worden ist, muss das Unternehmen über Maßnahmen zur Risikominimierung nachdenken. In Betracht kommen insbesondere zwei Maßnahmen:

- Die Vollverschlüsselung der Festplatte, wodurch auch bei einem unbefugten Zugriff auf die Festplatte die Daten nicht lesbar sind und
- eine Anweisung an die Außendienstmitarbeiter den Laptop nicht unbeaufsichtigt zu lassen.

Dabei ist im Rahmen des Stands der Technik auf eine entsprechend starke Verschlüsselung zu achten, die nach heutigem Stand als sicher gilt. Bei den Kosten zur Einführung sind die finanziellen Ressourcen des Unternehmens zu berücksichtigen. Sofern große oder besonders kleine Ressourcen verfügbar sind, kann dies bei der Auswahl der Verschlüsselungslösung beachtet werden.

Nach Implementierung der Abhilfemaßnahmen sollten diese und die verbleibenden Risiken beschrieben und eine erneute datenschutzrechtliche Bewertung durchgeführt werden. Es beginnt damit erneut eine Risikoanalyse. Dabei sollte aufgezeigt werden, warum ggf. verworfene Lösungen nicht zum Einsatz kamen. Sollte auch nach der zusätzlichen Implementierung von Maßnahmen ein nicht angemessenes Schutzniveau erreicht werden können, ist die Durchführung der Datenverarbeitung datenschutzrechtlich in der Regel unzulässig. Die Risikoanalyse sollte regelmäßig überprüft und dokumentiert werden.

Fazit

Der Aufwand einer solchen Risikoanalyse ist nicht zu unterschätzen und es sollten hinreichend Ressourcen und Zeit eingeplant werden. Sobald dieser Prozess einmal etabliert ist, können dadurch Mängel aufgedeckt und Vorfälle verhindert werden, die die wiederum Zeit und Geld gekostet hätten. Zudem kann eine einmal entworfene Struktur für eine Risikoanalyse für vielfältige Datenverarbeitungen wiederverwendet werden.

Autor: Olaf Rossow ist Justiziar bei der datenschutz nord GmbH in Bremen.