Kurzpapier Nr. 18

Risiko für die Rechte und Freiheiten natürlicher Personen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Ziel dieses Kurzpapieres ist es, das Risiko im Kontext der DS-GVO zu definieren und aufzuzeigen, wie Risiken für die Rechte und Freiheiten natürlicher Personen bestimmt und in Bezug auf ihre Rechtsfolgen bewertet werden können. Die Eindämmung von Risiken durch Ergreifen geeigneter technischer und organisatorischer Maßnahmen ist nicht Gegenstand des Papiers.

I. Rechte und Freiheiten natürlicher Personen nach der DS-GVO (Begriffsklärung)

„Rechte und Freiheiten natürlicher Personen“ ist ein zentraler Begriff in der DS-GVO. Ziel der DS-GVO ist es gem. Art. 1 Abs. 2 DS-GVO, die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen. Diese bestimmen sich nach der Charta der Grundrechte und Grundfreiheiten der Europäischen Union (Grundrechtecharta – GrCh) und der Europäischen Menschenrechtskonvention (EMRK). Der Begriff Rechte und Freiheiten natürlicher Personen umfasst zudem einfachgesetzliche individuelle Rechte. Er ist im Rahmen des europarechtlichen Kontextes und nicht nach rein nationalem Verständnis auszulegen. Ausgangspunkt der Auslegung dieses Begriffes ist das Grundrecht auf Schutz personenbezogener Daten nach Art. 8 GrCh, er umfasst aber grundsätzlich alle Grundrechte, die durch das Datenschutzrecht zumindest mittelbar geschützt werden. In besonderem Maße dienen auch die in Art. 5 DS-GVO normierten Grundsätze für die Verarbeitung personenbezogener Daten sowie die Vorschriften über die Betroffenenrechte (Art. 12 ff. DS-GVO) diesem Schutz

Die Rechte und Freiheiten natürlicher Personen sind zentral bei der Abschätzung eines Risikos gemäß der DS-GVO. Jede Verarbeitung personenbezogener Daten ist mindestens eine Beeinträchtigung des Grundrechts auf den Schutz personenbezogener Daten, die durch eine Rechtsgrundlage gerechtfertigt werden muss (Art. 8 GrCh und Art. 6 DS-GVO).

II. Risiko nach der DS-GVO (Begriffsklärung)

Der Begriff des Risikos ist in der DS-GVO nicht ausdrücklich definiert. Aus den ErwGr. 75 und 94 Satz 2 DS-GVO kann folgende Definition hergeleitet werden:

> Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.
>
> Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.

Gemäß ErwGr 75 sind unter die möglichen Schäden physische, materielle und immaterielle Schäden einzuordnen. Ungerechtfertigte Beeinträchtigungen der Rechte und Freiheiten von natürlichen Personen (Grundrechtsverletzungen) sind unter die immateriellen Schäden zu rechnen. Dementsprechend wird im Folgenden allgemein von Schadensereignissen gesprochen und hierunter auch der Eintritt einer

ungerechtfertigten Beeinträchtigung von Rechten und Freiheiten natürlicher Personen gefasst. Ein Schadensereignis kann das Entstehen weiterer Risiken nach sich ziehen. Unrechtmäßige Verarbeitungstätigkeiten oder Verarbeitungstätigkeiten, die nicht den Grundsätzen des Art. 5 DS-GVO entsprechen, sind in sich Beeinträchtigungen des Grundrechts auf Datenschutz und stellen daher bereits ein Schadensereignis dar. Zudem können sie zusätzliche Risiken, etwa der Diskriminierung natürlicher Personen, nach sich ziehen.

Als Beispiel hierfür kann ein fehlerhafter Eintrag in einer Datei für Hausverbote oder eine falsche Einstufung der Kreditwürdigkeit dienen – ein Verstoß gegen das Prinzip der Richtigkeit gemäß Art. 5 Abs. 1 lit. d DS-GVO –, die darüber hinaus zu finanziellen Folgeschäden und Rufschädigungen führen können.

Schäden können sich grundsätzlich ergeben aus:

a) der geplanten Verarbeitung selbst,
b) eigenverantworteten und
c) fremdverursachten Abweichungen von der geplanten Verarbeitung (z. B. Drittwirkung, Naturkatastrophen, Hardwaredefekte, …)

III. Risiko und Rechtsfolgen

Die DS-GVO verwendet die Unterscheidungen „Risiko“ und „hohes Risiko“ (z. B. ErwGr. 76). Daneben wird die Formulierung „voraussichtlich nicht zu einem Risiko“ führend verwendet (Art. 27 Abs. 2 lit. a und Art. 33 Abs. 1 DS-GVO). Da es vollständig risikolose Verarbeitungen nicht geben kann, wird die Formulierung „nicht zu einem Risiko“ von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko“ führend verstanden. Ziel der Risikobeurteilung ist es daher, die Risiken nach den Abstufungen „geringes Risiko“, „Risiko“ und „hohes Risiko“ zu bestimmen.

Das Risiko mit Blick auf Rechtsfolgen unter der DS-GVO ist relevant insbesondere bei:

- Verantwortung des für die Verarbeitung Verantwortlichen (Art. 24 Abs. 1 DS-GVO)
- Datenschutz durch Technikgestaltung (Art. 25 Abs. 1 DS-GVO)
- Sicherheit der Verarbeitung (Art. 32 DS-GVO)
- Umgang mit einer Verletzung des Schutzes personenbezogener Daten (Artt. 33, 34 DS-GVO)
- Datenschutz-Folgenabschätzung und vorherige Konsultation (Artt. 35, 36 DS-GVO)

IV. Risikobeurteilung

Zur Risikobeurteilung sind die im Folgenden beschriebenen Phasen zu durchlaufen:

1. Risikoidentifikation
2. Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden
3. Zuordnung zu Risikoabstufungen

Grundlage einer Risikobeurteilung muss eine konkrete Beschreibung des zugrunde gelegten Sachverhalts sein, für den das Risiko abgeschätzt werden soll.

1. Risikoidentifikation

Zur Identifikation von Datenschutzrisiken bietet es sich an, von folgenden Fragen auszugehen:

a. Welche Schäden können für die natürlichen Personen auf der Grundlage der zu verarbeitenden Daten bewirkt werden?
b. Wodurch, d. h. durch welche Ereignisse kann es zu dem Schaden kommen?
c. Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?

<u>Zu a.) Schäden für natürliche Personen</u>

Schäden können nach der DS-GVO physischer, materieller oder immaterieller Natur sein (ErwGr. 75 Satz 1). Der Schadensbegriff ist somit in einem umfassenden Sinne zu verstehen und nicht auf monetär bezifferbare Schäden begrenzt.

Es müssen die negativen Folgen der geplanten Verarbeitung selbst betrachtet werden. Dazu gehören auch Einschränkungen von Rechten und Freiheiten, beispielsweise wenn betroffene Personen aus Angst vor Nachteilen auf die Ausübung ihrer Rechte verzichten (z. B. Verzicht auf Teilnahme an einer Demonstration aufgrund umfangreicher Überwachung).

Auch negative Folgen von Abweichungen von der geplanten Verarbeitung müssen betrachtet werden (z. B. Datenzugang durch unbefugte Personen oder Stellen, unbefugte Offenlegung oder Verknüpfung von Daten, zufällige Vernichtung von Daten, Ausfall oder Einschränkungen von vorgesehenen Prozessen, unbeabsichtigte oder vorsätzliche unbefugte Veränderung der Daten, Nichterfüllung eines Auskunftsanspruchs). Die Abweichungen können zu einer unrechtmäßigen oder einer die Datenschutzgrundsätze verletzenden Verarbeitung führen.

Durch jede Verarbeitung personenbezogener Daten erfolgt mindestens eine Beeinträchtigung des Grundrechts auf Schutz personenbezogener Daten (vgl. Art. 8 GrCh). Daneben können weitere Grundrechte betroffen sein, wie z. B. die Achtung des Familienlebens in Art. 7 GrCh oder die Meinungs- und Versammlungsfreiheit in Artt. 11 und 12 GrCh oder das Recht auf Nichtdiskriminierung in Art. 21 GrCh. Diese Beeinträchtigungen führen zu Schäden, wenn Sie nicht gerechtfertigt sind.

Letztlich müssen alle denkbaren negativen Folgen der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen, ihre wirtschaftlichen, finanziellen und immateriellen Interessen, ihren Zugang zu Gütern oder Dienstleistungen, für ihr berufliches und gesellschaftliches Ansehen, für ihren gesundheitlichen Zustand und für alle ihre sonstigen legitimen Interessen betrachtet werden.

Beispiele möglicher Schäden sind unter anderem:

- 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

Zu b.) Ereignisse

Für jeden bereits identifizierten möglichen Schaden werden die Ereignisse ermittelt, die zu seiner Verwirklichung führen können. Diese bestehen in der Nichteinhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DS-GVO sowie der Nichtgewährung der Betroffenenrechte nach Artt. 12 ff DS-GVO, insbesondere:

- 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 inkompatiblen Zwecken
- Verarbeitung nicht vorhergesehener Daten
- Verarbeitung nicht richtiger Daten
- Verarbeitung über die Speicherfrist hinaus

Bei Schäden, die sich aus der Verarbeitung selbst ergeben, besteht das Ereignis in eben dieser Verarbeitung.

Zu c.) Risikoquellen

Ein relevanter Teil der Risikoquellen ist dem Bereich des Verantwortlichen oder Auftragsverarbeiters und der von diesen plangemäß durchgeführten Verarbeitung zuzuordnen.

Dabei ist auch in Betracht zu ziehen, inwieweit Personen im Bereich des Verantwortlichen oder etwaiger Auftragsverarbeiter bewusst oder unbeabsichtigt den für die Verarbeitung vorgesehenen Rahmen überschreiten könnten (z. B. eine Vertriebsabteilung, die die Zweckbindung von Kundendaten ändern könnte, etwa um eine Zielvorgabe zum Umsatz zu erfüllen).

Ein weiteres Beispiel sind Beschäftigte, die vorsätzlich gegen Anweisungen zum Umgang mit personenbezogenen Daten verstoßen oder vorsätzlich in Verfolgung eigener Interessen unbefugt handeln.

Des Weiteren sind Risiken durch unbefugte Angreifer wie Cyberkriminelle zu berücksichtigen. Risikoquellen können ggf. auch staatliche Stellen sein, die sich unbefugt Zugang verschaffen können. Schließlich können Risikoquellen bei Kommunikationspartnern liegen, mit denen personenbezogene Daten befugt ausgetauscht werden, oder bei Herstellern und Dienstleistern, die Informationstechnik einschließlich der mit ihr verwendeten Software, die für die Verarbeitung personenbezogener Daten oder in ihrem Umfeld eingesetzt wird, bereitstellen oder warten.

Schließlich sind technische Fehlfunktionen und äußere Einflüsse, z.B. durch höhere Gewalt, als Risikoquellen zu berücksichtigen.

2. Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden

Für jeden möglichen Schaden werden die Eintrittswahrscheinlichkeit und Schwere abgeschätzt. Diese lassen sich nur in ganz wenigen Ausnahmefällen mathematisch fassen.

Dennoch verlangt die DS-GVO, das Risiko anhand objektiver Kriterien zu beurteilen (ErwGr. 76). Insbesondere in Fällen immaterieller Schäden, wie z. B. einer Rufschädigung, muss auch – auf Basis objektiver Kriterien – beurteilt werden, als wie schwerwiegend die möglichen negativen Folgen für die Lebensführung der betroffenen Personen einzustufen sind.

Eine Möglichkeit für die Bemessung eines Risikos besteht darin, eine Abstufung der Ausprägungen von Schwere und Eintrittswahrscheinlichkeit eines möglichen Schadens auf einer Skala – mit beispielsweise vier Ausprägungen – darzustellen.

Sowohl für die Differenzierung der **Eintrittswahrscheinlichkeit** als auch für **mögliche Schäden** könnten jeweils folgende Abstufungen verwendet werden:

- geringfügig
- überschaubar
- substanziell
- groß

Die Einordnung in die Stufen ist zu begründen.

Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit eines Risikos beschreibt, mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt und mit welcher weiteren Wahrscheinlichkeit es zu Folgeschäden kommen kann.

Handelt es sich zum Beispiel bei dem Schadensereignis um die ungewollte Offenlegung der sexuellen Orientierung einer Person, so ist die Wahrscheinlichkeit sowohl dieser Offenlegung, als auch der hieraus resultierenden weiteren Schäden einzuschätzen.

Die Wahrscheinlichkeiten der verschiedenen Wege, die zu einer solchen Offenlegung führen können, summieren sich hierbei. Im genannten Beispiel

gehören unzureichende Vorkehrungen des Verantwortlichen, sorgloser Umgang von Beschäftigten unter seiner direkten Verantwortung mit der Information, technische Fehlfunktionen oder Ausspähung durch Dritte zu den zu betrachtenden Wegen.

Die Schwere des möglichen Schadens

Die Schwere eines möglichen Schadens muss in jedem Einzelfall insbesondere unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung bestimmt werden (ErwGr. 76). Wesentliche Faktoren sind insbesondere:

- Die Verarbeitung besonders geschützter Daten im Sinne von Art. 9 und 10 DS-GVO, bei denen die DS-GVO ausdrücklich eine gesteigerte Schutzbedürftigkeit vorsieht.
- Verarbeitung von Daten schützenswerter Personengruppen (z. B. Kinder, Beschäftigte).
- Verarbeitung nicht veränderbarer und eindeutig identifizierenden Daten wie z. B. eindeutigen Personenkennzahlen im Vergleich zu pseudonymisierten Daten.
- Automatisierte Verarbeitungen, die eine systematische und umfassende Bewertung persönlicher Aspekte (z. B. Profiling) beinhalten und auf deren Grundlage dann Entscheidungen mit erheblichen Rechtswirkungen für betroffene Personen getroffen werden (vgl. Art. 35 Abs. 3 lit. a DS-GVO).
- Wenn der Schaden nicht oder kaum reversibel ist oder die betroffene Person nur wenige oder beschränkte Möglichkeiten hat, die Verarbeitung selbst zu prüfen oder gerichtlich prüfen zu lassen oder sich dieser Verarbeitung zu entziehen, etwa, weil sie von der Verarbeitung gar keine Kenntnis hat.
- Wenn die Verarbeitung eine systematische Überwachung ermöglicht.
- Die Anzahl der betroffenen Personen, die Anzahl der Datensätze und die Anzahl der Merkmale in einem Datensatz sowie die geographische Abdeckung, die mit den verarbeiteten Daten erreicht wird.

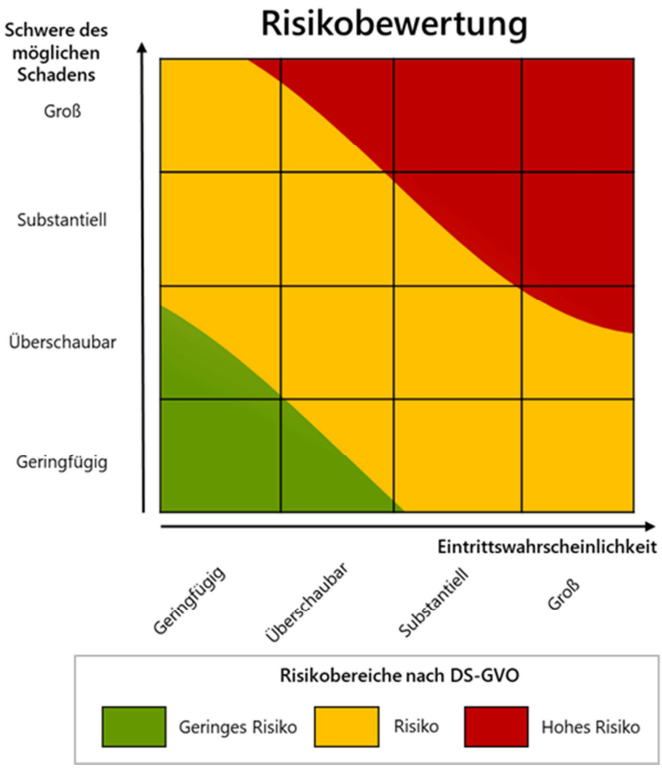
3. Zuordnung zu Risikoabstufungen

Nachdem die Eintrittswahrscheinlichkeit und die Schwere möglicher Schäden bestimmt wurden, müssen diese den Risikoabstufungen „geringes Risiko“ „Risiko“ und „hohes Risiko“ zugeordnet werden. Wie diese Abbildung konkret erfolgt, wird in der DS-GVO nicht näher beschrieben – es besteht daher grundsätzlich Spielraum für verschiedene Modelle.

Als Risiko der Verarbeitung insgesamt ist grundsätzlich die höchste Risikoklasse der Einzelrisiken anzunehmen. Sollten in dieser Risikoklasse viele Einzelrisiken vorhanden sein, kann es jedoch im Einzelfall erforderlich sein, eine höhere Risikoklasse anzunehmen.

Risikomatrix

Für die Abschätzung des Risikos der Verarbeitung gemäß der Eintrittswahrscheinlichkeit und der Schwere des möglichen Schadens kann die folgende Matrix verwendet werden:



Bei der Abschätzung des Risikos anhand der Matrix können Fälle eintreten, in denen der Eintritt des Schadens relativ wahrscheinlich ist oder der potentielle Schaden besonders schwer wiegen würde und somit Grenzbereiche zwischen den Risikobereichen betroffen sein können. Hier sind in den Feldern der Matrix zwei Farben eingetragen. Dies macht deutlich, dass in diesen Grenzfällen eine Einzelfallbetrachtung notwendig ist. Diese kann im Zweifel zu dem Schluss kommen, dass trotz des Ergebnisses der generischen Abschätzung anhand der Matrix, der Einzelfall als so schwerwiegend erscheint, dass dennoch ein hohes Risiko gegeben ist. Umgekehrt kann im Einzelfall z. B. auch ein geringfügiger möglicher Schaden, der eine überschaubare Eintrittswahrscheinlichkeit hat, ein geringes Risiko darstellen.

Mit der bis zu diesem Punkt beschriebenen Vorgehensweise wird das Ausgangsrisiko einer Datenverarbeitung unter Berücksichtigung der Umstände der Verarbeitung bestimmt.

V. Eindämmung des Risikos

Im Wege der Datenschutz-Folgeabschätzung oder – falls voraussichtlich kein hohes Risiko vorliegt – in einem vereinfachten Verfahren sind als nächster Schritt die Maßnahmen zur angemessenen Eindämmung der Risiken zu ermitteln.

Grundsätzlich ist das Risiko einer Verarbeitung mittels Abhilfemaßnahmen einzudämmen. Oft wird dies mit dem Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen (TOMs) zu erreichen sein, die geeignet sind, die Rechte und Freiheiten der betroffenen natürlichen Personen angemessen zu gewährleisten, indem die Eintrittswahrscheinlichkeit und/oder die Schwere des möglichen Schadens eingedämmt werden. Dazu gehören auch Maßnahmen zur Eindämmung unerwünschter Ereignisse (z. B. Angriffe von Cyberkriminellen), wie die klassischen Security-Maßnahmen aus der Informationssicherheit, die jedoch im Hinblick auf den Schutz der betroffenen Personen und nicht der Verantwortlichen zu bewerten sind.

VI. Restrisiko

Das nach Umsetzung dieser Maßnahmen verbleibende Risiko wird als Restrisiko bezeichnet. Wenn dieses Restrisiko als hoch einzustufen ist, besteht die Pflicht zur vorherigen Konsultation gemäß Art. 36 DS-GVO.

Der Verantwortliche muss genau prüfen (und gem. Art. 5 Abs. 2 DS-GVO als Nachweis für die Erfüllung der Anforderungen der DS-GVO dokumentiert haben), ob er alle ihm nach dem Grundsatz der Verhältnismäßigkeit möglichen Maßnahmen zur Eindämmung des Risikos ergriffen hat, bevor er mit einer Verarbeitung beginnt.

Nach Umsetzung der Abhilfemaßnahmen müssen diese auf ihre Wirksamkeit getestet und kontinuierlich überwacht werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

Fazit

Die objektive Ermittlung und Beurteilung des Risikos einer Verarbeitung personenbezogener Daten im o.g. Sinn ist erforderlich, um festzustellen, wie die Rechte und Freiheiten natürlicher Personen wirksam geschützt werden.

****