Felix Bieker

Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell

Bei der Auswahl technischer und organisatorischer Maßnahmen zur Herstellung eines angemessenen Schutzniveaus nach dem neuen EU-Datenschutzrecht ist das Risiko für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Dies wird im Standard-Datenschutzmodell operationalisiert, das dadurch die rechtskonforme und überprüfbare Umsetzung ermöglicht.

1 Einführung

Die Beurteilung des Risikos für die Rechte und Freiheiten natürlicher Personen spielt bei der Auswahl und Umsetzung technischer und organisatorischer Maßnahmen gem. Art. 24 Abs. 1, 25 Abs. 1 und 32 Abs. 1 u. 2 Datenschutz-Grundverordnung (DSGVO) sowie Art. 19 Abs. 1, 20 Abs. 1 und Art. 29 Richtlinie zum Datenschutz im Bereich Justiz und Inneres (JI-Richtlinie)[1] eine wichtige Rolle. Im Standard-Datenschutzmodell (SDM)[2] ist dies folglich ebenfalls ein wesentlicher Aspekt: Die zu ergreifenden Maßnahmen sind abhängig von der Bestimmung des Schutzbedarfs und der Eingriffsintensität. Je höher diese sind, desto größer sind die Anforderungen an die zu ergreifenden Maßnahmen, um die Eingriffsintensität zu mindern und den Schutz der Grundrechte der betroffenen Personen effektiv gewährleisten zu können. Insoweit deckt sich das SDM vollständig mit den Anforderungen des EU-Datenschutzrechts und insbesondere mit Art. 32 Abs. 1 DSGVO und Art. 29 JI-Richtlinie, die die Gewährleistung eines angemessenen Schutzniveaus fordern und sich dabei auf die EU-Grundrechte beziehen. Das SDM operationalisiert diesen Schutz der Grundrechte. Zudem fordern die Vorschriften, dass der Verantwortliche den Nachweis erbringen kann, dass die Vorschriften der DSGVO/JI-Richtlinie eingehalten werden, dies ermöglicht das SDM durch eine objektive und überprüfbare Beurteilung eines Verfahrens.

In der aktuellen Version des SDM gibt es jedoch begriffliche Unklarheiten bei der Ermittlung von Schutzbedarf, Eingriffsintensität und der Risikoanalyse. So wird davon ausgegangen, dass der Schutzbedarf anhand der Eingriffsintensität bestimmt wird. Die Eingriffsintensität bestimmt sich wiederum anhand des Zwecks der Datenverarbeitung, der Schutzbedürftigkeit, der Dauer der Speicherung und der Verbreitung der Daten.[3] Insofern erfolgt die Bestimmung des Schutzbedarfs, die sich aus der Eingriffsintensität ergibt, u.a. über die Schutzbedürftigkeit. Diese Begriffe sind nicht ausreichend voneinander abgegrenzt und sollten zudem an die Vorgaben der DSGVO/JI-Richtlinie angeglichen werden. Im Folgenden werden daher die erheblichen Überschneidungen zwischen den neuen rechtlichen Anforderungen und dem SDM aufgezeigt und systematisiert.

Da sowohl DSGVO und JI-Richtlinie als auch das SDM einen erheblichen Grundrechtsbezug aufweisen, wird jedoch zunächst dargestellt, welche Grundrechte für die Beurteilung des Risikos für die Rechte und Freiheiten natürlicher Personen relevant sind und inwieweit diese Grundrechte auf Organisationen, also staatliche und private Stellen, angewandt werden können.

2 EU-Grundrechte als Maßstab

Im Unterschied zur Informationssicherheit sind im Datenschutzrecht die Grundrechte der betroffenen Personen maßgeblich. Dies wird bereits unter anderem in den Erwägungsgründen (ErwGr.) 1, 2, 10 und insbesondere Art. 1 Abs. 2 DSGVO und Art. 1 Abs. 2 JI-Richtlinie hervorgehoben, die auch ausdrücklich auf das Recht auf Schutz personenbezogener Daten gem. Art. 8 EU-Grundrechtecharta (GrCh) verweisen.

1 Den Nachweis der Anwendbarkeit der Schutzziele des SDM auch auf die JI-Richtlinie erbringt Schlehahn, in diesem Heft.

2 AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.): Das Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig zustimmend zur Kenntnis genommen (Enthaltung durch Freistaat Bayern), abrufbar unter: https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html.

3 AK Technik, Das Standard-Datenschutzmodell, S. 36.

Felix Bieker, LL.M. (Edinburgh)

ist juristischer Mitarbeiter im Projektreferat des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

E-Mail: fbieker@datenschutzzentrum.de

2.1 Anwendbare Grundrechte

Die EU-Grundrechte sind gem. Art. 51 Abs. 1 GrCh anwendbar, wenn eine Handlung oder ein Rechtsakt der EU vorliegen oder ein Mitgliedstaat Unionsrecht durchführt. Während die Anwendung auf die EU selbst unproblematisch ist, bleibt die Frage, wie der Begriff der „Durchführung" auszulegen ist. Der EuGH legt dieses Tatbestandsmerkmal in seiner ständigen Rechtsprechung weit aus um sicherzustellen, dass ein umfassender Grundrechtsschutz innerhalb der EU gewährleistet ist. Die EU-Grundrechte sind demnach in Fällen anwendbar, die unionsrechtlich geregelt sind, also in den Geltungsbereich des Unionsrechts fallen.[4] Dies gilt jedoch nur insoweit, als ein Zusammenhang zwischen einem EU-Rechtsakt und der nationalen Maßnahme besteht; die fraglichen Materien also nicht nur benachbart sind oder sich nur mittelbar beeinflussen.[5]

Auch wenn die Abgrenzung des Anwendungsbereichs der Charta in Einzelfällen aufgrund des weiten Anwendungsbereichs des Unionsrechts schwierig sein mag, gilt dies nicht in gleichem Maß für das EU-Datenschutzrecht, denn die EU hat nach Art. 16 AEUV und Art. 39 EUV weitgehende Kompetenzen für den Datenschutz. Soweit Regelungen der DSGVO[6] betroffen sind, kann, von Einzelfällen abgesehen, davon ausgegangen werden, dass die EU-Grundrechte anwendbar sind.[7] Insbesondere kommt Art. 8 GrCh in Betracht. Allerdings sind auch Grundrechte zu berücksichtigen, die eng mit den Zielen des Datenschutzes verwandt sind, wie etwa das Recht auf Schutz des Privatlebens gem. Art. 7 GrCh, das Recht auf freie Meinungsäußerung gem. Art. 11 GrCh und das Recht auf Schutz vor Diskriminierung gem. Art. 21 GrCh.

2.2 Eingriffe in den Schutzbereich von Grundrechten

Eingriffe in den Schutzbereich von Grundrechten sind, unabhängig von der konkreten Handlungsform, hoheitliche Maßnahmen, die zu einer Beeinträchtigung eines Grundrechts führen.[8] Der EuGH geht von einem weiten Eingriffsbegriff aus, sodass auch mittelbare Beeinträchtigungen erfasst sind.[9] Mittelbare Beeinträchtigungen sind solche, bei denen eine Beeinträchtigung von Grundrechten nicht der eigentliche Zweck ist.[10] Ein Beispiel ist die Verpflichtung privater Internetanbieter zur Erfassung von Metadaten für die Vorratsdatenspeicherung, die dabei auch, jedoch nur mittelbar und nicht final, in die Grundrechte der Nutzer*innen eingreift.[11] Eine mittelbare Beeinträchtigung kann aber auch durch einen Realakt eines Hoheitsträgers entstehen: etwa wenn personenbezogene Daten an Dritte herausgegeben werden.[12]

Ein Eingriff in das Recht auf Schutz personenbezogener Daten gem. Art. 8 GrCh liegt nach der ständigen Rechtsprechung des EuGH schon vor, wenn personenbezogene Daten verarbeitet werden.[13] Das Recht auf Schutz des Privatlebens gem. Art. 7 GrCh umfasst auch die Verarbeitung von personenbezogenen Daten; ein Eingriff besteht, wenn Daten verarbeitet und daraus Rückschlüsse auf das Privatleben einer natürlichen Person gezogen werden können, weil die Vertraulichkeit der Daten aufgehoben wird.[14] Nach ständiger Rechtsprechung ist es dabei unerheblich, ob die Daten sensibel sind oder die betroffenen Personen Nachteile erlitten haben könnten.[15] In das Recht auf freie Meinungsäußerung gem. Art. 11 GrCh wird durch jegliche Behinderung der freien Kommunikation eingegriffen.[16] Ein Eingriff in das Recht auf Schutz vor Diskriminierung gem. Art. 21 u. 23 GrCh besteht, wenn aufgrund der nicht abschließend aufgezählten Merkmale oder eines gleichgestellten Merkmals vergleichbare Sachverhalte unterschiedlich und unterschiedliche Sachverhalte gleich behandelt werden, es sei denn, dass eine solche Behandlung objektiv gerechtfertigt ist.[17] Dies umfasst sowohl unmittelbare, als auch mittelbare Diskriminierungen, also solche, die nicht direkt an ein bestimmtes Merkmal anknüpfen, aber sich zumeist auf Personen auswirken, die ein bestimmtes Merkmal aufweisen. Ein Beispiel für mittelbare Diskriminierung ist etwa ein Wohnsitzerfordernis, das insbesondere Personen betrifft, die nicht Staatsangehörige des betreffenden Staates sind.

Zudem ist für die EU-Grundrechte das Konzept der staatlichen Schutzpflichten, das der Europäische Gerichtshof für Menschenrechte (EGMR) entwickelt hat, besonders relevant, da die Rechte der Europäischen Menschenrechtskonvention (EMRK) gem. Art. 6 Abs. 3 EUV indirekt auch in der EU zu beachten sind. Dieses Konzept besagt, dass wenn eine Privatperson eine andere schädigt und der Staat es unterlassen hat, dies durch Rechts- oder Realakte zu verhindern, der Staat durch dieses Unterlassen die Rechte der geschädigten Person beeinträchtigt.[18]

Gemäß Art. 51 Abs. 1 GrCh sind ausschließlich die EU selbst und die Mitgliedstaaten bei der Durchführung von Unionsrecht an die Einhaltung der Charta gebunden und damit Grundrechtsverpflichtete. Der Eingriff muss daher stets durch einen Hoheitsträger erfolgen oder einem solchen zugerechnet werden können.[19]

4 EuGH, Urteil vom 26. Feburar 2013, Åkerberg Fransson, C-617/10, ECLI:EU:C:2013:105, Rn. 19.

5 Zuletzt in EuGH, Urteil vom 10. Juli 2014, Hernández u.a., C-198/13, ECLI:EU:C:2014:2055, Rn. 34.

6 Dies gilt auch für das neue BDSG, insbesondere bezüglich der Umsetzung der Vorschriften der JI-Richtlinie.

7 Vgl. im Allgemeinen und speziell für den vermeintlich nationalrechtlich determininerten Bereich des Personenstands- und Meldrechts Kieck/Pohl, Zum Anwendungsbereich des europäischen Datenschutzrechts, DuD 2017, S. 567-571, die verdeutlichen, dass der Anwendungsbereich des EU-Datenschutzrechts eben sehr weitgehend ist.

8 Gärditz, in: Grabenwarter, Enzyklopädie Europarecht Band 2, Baden-Baden 2014, § 4, Rn. 56-62; von Danwitz, in: Tettinger/Stern, Europäische Grundrechte-Charta, München, 2006, Art- 52, Rn. 32

9 Vgl. Gärditz in: Grabenwarter, Enzyklopädie Europarecht Band 2, § 4, Rn. 58.

10 Jarass, in: Jarass, Charta der Grundrechte der EU, 3. Aufl., München 2016, Art. 52, Rn. 13-15.

11 Vgl. EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 und 594/12, ECLI:EU:C:2014:238, Rn. 34 und 37.

12 EuGH, Urteil vom 20. Mai 2003, Österreichischer Rundfunk u.a., C-465/00, C-138/01 und C-139/01, ECLI:EU:C:2003:294, Rn. 74.

13 Erstmals in EuGH, Urteil vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 and C-93/09, ECLI:EU:C:2010:662, Rn. 60-63.

14 Vgl. EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 und 594/12, ECLI:EU:C:2014:238, Rn. 32-34 und EuGH, Urteil vom 13. Mai 2014, Google und Google Spain, C-131/12, ECLI:EU:C:2014:317, Rn. 80, wobei der EuGH in letzterem Fall den Eingriffsbegriff auch bei Beeinträchtigungen durch Private verwendet.

15 Erstmals in Urteil vom 20. Mai 2003, Österreichischer Rundfunk u.a., C-465/00, C-138/01 und C-139/01, ECLI:EU:C:2003:294, Rn. 75.

16 Calliess, in: Calliess/Ruffert, Kommentar EUV/AEUV, 5. Aufl., München 2016, Art. 11 GrCh, Rn. 28.

17 Vgl. EuGH, Urteil vom 11. April 2013, Soukupová, C-401/11, ECLI:EU:C:2013:223, Rn. 29 explizit zu Art. 21 GrCh.

18 Krieger, in: Dörr/Grote/Marauhn, EMRK/GG Konkordanzkommentar, Tübingen 2013, Kapitel 6, Rn. 64.

19 Allerdings hat der EuGH in Einzelfällen und vor in Kraft treten der Charta EU-Grundrechte auch horizontal zwischen Privaten angewandt, insbesondere im Verhältnis zwischen Arbeitnehmer*innen und Arbeitgeber*innen, vgl. EuGH, Urteil vom 22. November 2005, Mangold, C-144/04, ECLI:EU:C:2005:709; EuGH, Urteil vom 19. Januar 2010, Kücüdevici, C-555/07, ECLI:EU:C:2010:21; EuGH, Urteil

Das SDM unterscheidet nicht zwischen der Verarbeitung durch private und staatliche Stellen. Bezüglich der Verarbeitung von personenbezogenen Daten ist das Individuum diesen Akteuren ausgeliefert, da diese die Verarbeitung kontrollieren und Datenmacht ausüben,[20] unabhängig davon, ob diese nun staatlich oder privat handeln. Um Missverständnissen vorzubeugen, sollte im Rahmen des SDM dennoch nicht von Eingriffen von Organisationen, sondern von Beeinträchtigungen der Grundrechte durch Organisationen gesprochen werden; dies umfasst dann korrekt die Handlungen von staatlichen wie auch privaten Stellen.

3 Risikoanalyse

Vor dem Hintergrund dieser Überlegungen kann nun der regulatorische Ansatz der DSGVO, der auf dem Konzept des Risikos für die Rechte und Freiheiten natürlicher Personen basiert, erschlossen werden. In der DSGVO sind bestimmte Rechtsfolgen davon abhängig, wie das Risiko für die Rechte und Freiheiten natürlicher Personen zu beurteilen ist. Von Interesse ist hier die Ermittlung dieses Risikos bei der Umsetzung geeigneter technischer und organisatorischer Maßnahmen gem. Art. 24 Abs. 1, 25 Abs. 1 und Art. 32 Abs. 1 DSGVO sowie Art. 19 Abs. 1, 20 Abs. 1 und Art. 29 JI-Richtlinie. Dies ist natürlich auch im Rahmen der Schutzbedarfsbestimmung des SDM relevant. Das SDM sieht ebenfalls eine Risikoanalyse vor: Dabei soll bewertet werden, wie wahrscheinlich es ist, dass eine Organisation, die Daten befugt verarbeitet, Vorgaben zum Datenschutz nicht einhält. [21]

3.1 Begriff des Risikos

Zunächst ist allerdings zu beachten, dass der Begriff des Risikos in DSGVO und JI-Richtlinie nicht mit dem Risikobegriff des Risiko-Managements korrespondiert, wie er in der Informationssicherheit verwendet wird.[22] Letzterer bezeichnet das Risiko für eine Organisation, das sich aus der Nicht-Einhaltung rechtlicher Anforderungen ergibt. Das für das EU-Datenschutzrecht maßgebliche Risiko ist jedoch das für die Rechte und Freiheiten natürlicher Personen, also deren EU-Grundrechte.[23] ErwGr. 75 erläutert, dass diese Risiken nicht nur zu physischen und materiellen Schäden führen könnten, sondern benennt ausdrücklich auch immaterielle Schäden, maßgeblich ist dabei vor allem die Verletzung betroffener Personen in ihren Grundrechten. Eine Grundrechtsverletzung liegt bei einem ungerechtfertigten Eingriff vor. Diese Bedeutung von Grundrechtsverletzungen für die Risikoermittlung wird unterstrichen durch die Klarstellung des ErwGr. 94 S. 2, der ausdrücklich besagt, dass ein Risiko nicht nur einen möglichen Schaden, sondern bereits die Beeinträchtigung eines Grundrechts umfasst. Für das Grundrecht auf Datenschutz nach Art. 8 GrCh bedeutet dieses Risiko, dass die – bereits durch jegliche Verarbeitung bestehende – Beeinträchtigung nicht in dem Maße verringert wird, wie es der Schutz der natürlichen Person erfordert. In Bezug auf das Recht auf Privatleben gem. Art. 7 GrCh und das Recht auf freie Meinungsäußerung gem. Art. 11 GrCh besteht das Risiko etwa darin, dass ein bestimmtes Verhalten aufgrund der damit einhergehenden Verarbeitung personenbezogener Daten unterlassen wird (sog. chilling effect). Ein Diskriminierungsrisiko besteht zum Beispiel, wenn besondere Kategorien von Daten im Sinne von Art. 9 DSGVO und 10 JI-Richtlinie sowie Daten über strafrechtliche Ermittlungen oder Straftaten nach Art. 10 DSGVO erhoben werden.

3.2 Ermittlung des Risikos

Bezüglich der Ermittlung des Risikos ist die DSGVO aber zirkelschlüssig: So sollen laut ErwGr. 75 u. 76 die Risiken selbst verschiedene Eintrittswahrscheinlichkeiten und eine zu ermittelnde Schwere haben. Allerdings bestimmen sich Risiken, wie dies etwa aus der Informationssicherheit bekannt ist, aus der Eintrittswahrscheinlichkeit und Schwere eines möglichen Schadens, wobei sich in dem Schaden das Risiko materialisiert. Die bekannte Risikoformel lässt sich aber aufgrund des Grundrechtsbezugs nicht ohne Weiteres auf das EU-Datenschutzrecht übertragen.[24]Neben den möglichen Schäden verweist die DSGVO in ErwGr. 94 S. 2 eben auch auf die reine Beeinträchtigung von Grundrechten.

Nach Art. 1 Abs. 2 DSVO ist es ausdrückliches Ziel der Verordnung, die Grundrechte natürlicher Personen zu schützen. Um das Risiko für die Rechte und Freiheiten dieser natürlichen Personen zu ermitteln, ist eine Grundrechtsbeeinträchtigung der Ausgangspunkt. Selbstverständlich können diese Beeinträchtigungen auch zu weiteren materiellen und immateriellen Schäden führen. Diese Schäden sind allerding grundsätzlich bei der Untersuchung der Beeinträchtigungen bereits umfasst, sodass im Folgenden nur auf die Ermittlung von Beeinträchtigungen detailliert eingegangen wird.

Folglich ermittelt sich das Risiko für die Rechte und Freiheiten natürlicher Personen nach der DSGVO aus der Schwere der Beeinträchtigung der Rechte und Freiheiten natürlicher Personen durch die Verarbeitung personenbezogener Daten an sich. Bezüglich einer Beeinträchtigung des Grundrechts aus Art. 8 GrCh erübrigt sich die gesonderte Feststellung der Eintrittswahrscheinlichkeit, da eine Beeinträchtigung bei jeder Verarbeitung gegeben ist und die Eintrittswahrscheinlichkeit somit stets bei 100% liegt. Bezüglich der anderen betroffenen Grundrechte ist diese jedoch im Einzelfall, also in Bezug auf das konkrete Verfahren, zu ermitteln.

3.2.1 Identifikation von Risikoquellen

Zunächst müssen Quellen möglicher Risiken identifiziert werden. Risiken gehen dabei von der Verarbeitung selbst, aber auch von unerwünschten Ereignissen, wie z.B. Angriffen auf Schutzmaßnahmen der Informationssicherheit oder Störungen durch

vom 11. Dezember 2007, The International Transport Workers' Federation und The Finnish Seamen's Union – Viking, C-438/05, ECLI:EU:C:2007:772.

20 von Lewinski, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt (Hg.), Freiheit, Sicherheit, Öffentlichkeit, Baden-Baden 2009, S. 200.

21 AK Technik, Das Standard-Datenschutzmodell, S. 39 f.

22 Vgl. Forum Privatheit, White Paper Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz, 3. Aufl., 2017, abrufbar unter: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums.php.

23 Der Begriff der „Rechte und Freiheiten" findet sich in Art. 52 Abs. 1 GrCh und geht auf die EMRK zurück; die Begriffe sind synonym und bezeichnen die EU-Grundrechte, wie sie in Art. 6 EUV benannt sind, vgl. Borowsky, in: Meyer, Charta der Grundrechte der Europäischen Union, 4. Aufl., München 2014, Art. 52, Rn. 19; Becker, in: Schwarze u.a. (Hrsg.), EU-Kommentar, 3. Aufl., Baden-Baden 2012, Art. 52, Rn. 2.

24 Zur Gefahr pseudo-mathematischer Berechnungen im Rahmen der Risikobewertung vgl. Bieker/Hansen/Friedewald, Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung, RDV 2016, S. 193.

Naturereignisse aus, vgl. Art. 32 Abs. 2 DSGVO. Die Identifikation möglicher Risikoquellen geschieht anhand der Schutzziele. In diesem Zusammenhang ist auch eine Angreifermodellierung vorzunehmen, wie sie aus dem Bereich der Informationssicherheit bekannt ist, die im Datenschutz jedoch aus Sicht der betroffenen Personen und nicht der Organisation zu erfolgen hat. Daher liegt hierbei ein wichtiger Fokus auf der verantwortlichen Stelle selbst, da sie die Verarbeitung durchführt und somit die Beeinträchtigung von Art. 8 GrCh von ihr ausgeht.

Als Quellen von Risiken sind neben der Organisation und ihrer Vertragspartner, wie etwa Auftragsverarbeiter, Technologie-/Software-Hersteller, IT-Diensteanbieter, Wirtschaftsauskunfteien, Marketingunternehmen, auch staatliche Stellen, wie Sicherheitsbehörden oder die staatliche Leistungsverwaltung zu betrachten, wobei die Bereiche Gesundheitswesen und Forschung hervorzuheben sind.[25]

3.2.2 Schwere der Beeinträchtigung

Wie von ErwGr. 76 gefordert, ist die Schwere der Beeinträchtigung selbstverständlich in Bezug auf die Verarbeitung zu beurteilen; bezogen auf Art. 8 GrCh besteht die Beeinträchtigung ja gerade in dieser. Es muss also abgeschätzt werden, welche negativen Folgen sich aus der Verarbeitung selbst ergeben, gleichgültig, ob diese erwünscht oder unerwünscht sind.

Die Einordnung von Grundrechtsbeeinträchtigungen hat *Alexy* aus grundrechtstheoretischer Sicht systematisiert und schlägt, um eine konkrete Beeinträchtigung beurteilen zu können, eine dreistufige Skalierung vor, anhand derer sich verschiedene Fälle prima facie kategorisieren lassen sollen.[26] Um diese Kategorisierung in der Praxis zu vereinfachen und zu systematisieren, grenzt das SDM drei Schutzbedarfskategorien (normal, hoch, sehr hoch) voneinander ab.[27] Diese wurden aufbauend auf der IT-Grundschutz-Methodik speziell für den Bereich des Datenschutzes entwickelt und sollen den durch die Verarbeitung selbst bestehenden „Grundrechtseingriff" klassifizierbar machen. Aus juristischer Sicht lässt sich diese Klassifizierung auch durch Rückgriff auf *Alexys* Abwägungsgesetz und Gewichtsformel begründen. Die Unterscheidung in der aktuellen Version des SDM zwischen Eingriffsintensität, mit der die Schwere des Grundrechtseingriffs bemessen wird, und Schutzbedarf, der den Grundrechtseingriff klassifiziert, lässt sich daher aufheben, da beide letztlich dasselbe bezeichnen und daher zusammengeführt werden können. Denn die Systematisierung der einzelnen Schutzbedarfsabstufungen, die sich wiederum auf die gesetzlichen Wertungen der DSGVO stützen, sind als Kriterien für die Bestimmung der Schwere einer Beeinträchtigung nutzbar. Damit wird diese Bestimmung objektiver und nachvollziehbarer. Letztlich bezeichnen also Eingriffsintensität und Schutzbedarf das gleiche, nämlich die Schwere der Beeinträchtigung, allerdings jeweils aus juristischer und technischer Perspektive.

So ist im Standardfall, also jeglicher Verarbeitung personenbezogener Daten, von einer normalen Schwere der Beeinträchtigung auszugehen. Die Schwere der Beeinträchtigung erhöht sich, wenn besondere Kategorien von Daten im Sinne von Art. 9 DSGVO und 10 JI-Richtlinie sowie Daten über strafrechtliche Ermittlungen oder Straftaten nach Art. 10 DSGVO oder Daten zu Zwecken der Profilerstellung oder -nutzung durch die Bewertung persönlicher Aspekte verarbeitet werden.[28] Diese Einordnung entspricht der Wertung des Gesetzgebers aus Art. 9, 10 und 22 DSGVO.

Die Schwere der Beeinträchtigung ist hoch, wenn die betroffene Person auf die Entscheidung oder Dienste einer Organisation angewiesen ist und die Datenverarbeitung ernsthafte Folgen für sie haben kann und/oder es keine effektiven Sicherungsmaßnahmen oder Interventionsmöglichkeiten für die betroffene Person gibt.

Eine sehr hohe Schwere der Beeinträchtigung besteht schließlich, wenn die betroffene Person von den Entscheidungen bzw. Diensten der Organisation unmittelbar existentiell abhängig ist und das Verfahren für die betroffene Person nicht transparent ist und die Interventionsmöglichkeiten beschränkt sind.[29]

Eine erhöhte Schwere der Beeinträchtigung kann sich auch aufgrund kumulativer Effekte verschiedener Aspekte ergeben: etwa wenn personenbezogene Daten einer großen Gruppe von Menschen gesammelt werden oder für verschiedene Zwecke erfasst und analysiert werden und die betroffenen Personen daher in verschiedenen Rollen betroffen sind.[30] Diese Effekte werden auch in ErwGr. 75 a.E. benannt.

3.2.3 Eintrittswahrscheinlichkeit

Wie bereits oben erwähnt, beträgt die Eintrittswahrscheinlichkeit für Beeinträchtigungen des Rechts auf Schutz personenbezogener Daten gem. Art. 8 GrCh in jedem Fall 100%. Dies gilt jedoch nicht unbedingt für andere Rechte und Freiheiten natürlicher Personen, wie etwa die Grundrechte aus Art. 7, 11 und 21 GrCh. Auch sind mögliche Schäden in den Blick zu nehmen, die nach ErwGr. 75 materieller und immaterieller Art sein können. Im Fall einer Beeinträchtigung in Form einer Diskriminierung ist zu beachten, dass diese in ErwGr. 75 auch konkret als möglicher Schaden benannt ist.

Zunächst ist festzuhalten, dass die Eintrittswahrscheinlichkeit sich ebenfalls grundrechtstheoretisch verorten lässt. *Alexys* epistemisches Abwägungsgesetz besagt: Je schwerer eine Beeinträchtigung von Grundrechten wiegt, desto größer müssen die Anforderungen an die Gewissheit der die Beeinträchtigung tragenden Prämissen sein.[31] Die Bestimmung der Eintrittswahrscheinlichkeit knüpft daran an, indem sie bestimmt, mit welcher Gewissheit eine Beeinträchtigung oder ein möglicher Schaden eintreten. Auch diese Prämissen werden dann triadisch skaliert in die Stufen gewiss, plausibel oder evident falsch.[32] Diese Klassifizierung ist eine wichtige Erkenntnis, denn auch die Eintrittswahrscheinlichkeit einer Beeinträchtigung von Grundrechten lässt sich nicht exakt mathematisch berechnen.

Um die Bestimmung der Eintrittswahrscheinlichkeit nachvollziehbar zu machen, bietet das SDM ebenfalls Kriterien. So sind insbesondere zu beurteilen:

- die Motivation (die sich ebenfalls in normal, hoch und sehr hoch skalieren lässt) und

25 Ausführlicher dazu Forum Privatheit, White Paper Datenschutz-Folgenabschätzung.

26 Alexy, Die Gewichtsformel, in: Jickeli/Kreutzer/Reuter, Gedächtnisschrift für Jürgen Sonnenschein, Berlin 2003, S. 777 f.

27 AK Technik, Das Standard-Datenschutzmodell, S. 37 f.

28 Diese sind auch beispielhaft in ErwGr. 75 als Verarbeitungsverfahren benannt, die an sich bereits eine besonders schwere Beeinträchtigung darstellen.

29 AK Technik, Das Standard-Datenschutzmodell, S. 38.

30 AK Technik, Das Standard-Datenschutzmodell, S. 39.

31 Alexy, Die Gewichtsformel, S. 789.

32 Alexy, Die Gewichtsformel, S. 789.

- die operativen Möglichkeiten (normal, hoch, sehr hoch) einer Organisation,
- eine unbefugte Zweckänderung durchzuführen oder etwa auch einen unrechtmäßigen Zweck zu verfolgen.[33]

Mit Hilfe dieser Kriterien lässt sich dieser Schritt verobjektivieren und beispielsweise beurteilen, wie wahrscheinlich es auf einer bestimmten Skala ist, dass eine Organisation, die Waren oder Dienstleistungen verkauft und dafür Kund*innendaten verarbeitet, Profile ihrer Kund*innen bildet und diese etwa für diskriminierende Preisgestaltungen verwendet.

3.3 Beurteilung des Risikos

Wenn für die identifizierten Risikoquellen jeweils die Schwere der Beeinträchtigung und ggf. ihre Eintrittswahrscheinlichkeit bestimmt sind, kann das Risiko der Verarbeitung beurteilt werden. In dieser Abwägung werden die einzelnen Grundrechte sowie die Schutzziele abgewogen, um das für die Grundrechte angemessene Schutzniveau herzustellen.[34] Dabei werden, abhängig von der ermittelten Schwere der jeweiligen Beeinträchtigungen sowie ihrer Eintrittswahrscheinlichkeit und der sich daraus ergebenden Gewichtung, die gegenläufigen Prinzipien ins Verhältnis gesetzt.[35] Auch hier ist eine dreistufige Skalierung sinnvoll. In Anbetracht der grundrechtlichen Ausgestaltung des Datenschutzes und der Tatsache, dass jede Verarbeitung jedenfalls eine Beeinträchtigung von Art. 8 GrCh darstellt, ist davon auszugehen, dass nach der Wertung des Gesetzgebers (in diesem Fall sogar dem EU-Äquivalent zum verfassungsgebenden Gesetzgeber) jede Verarbeitung personenbezogener Daten ein ihr inhärentes Risiko erzeugt. Daraus folgt, dass es keine Verarbeitung ohne Risiko geben kann, sondern sich diese am besten in die Kategorien gering, normal und hoch unterteilen lassen, um auch die unterschiedlichen Rechtsfolgen, die die DSGVO an unterschiedliche Grade eines Risikos knüpft, abbilden zu können.

3.4 Eindämmung des Risikos

Im Anschluss an die Bewertung folgt der für den praktischen Schutz der Rechte und Freiheiten natürlicher Personen wesentliche Schritt: Aufgrund der Kategorisierung des Risikos werden, im Sinne von Art. 32 DSGVO/Art. 29 JI-Richtlinie und des SDM, geeignete technische und organisatorische Maßnahmen getroffen. Dabei gilt es, Beeinträchtigungen und mögliche Schäden für die Rechte und Freiheiten natürlicher Personen so weit einzudämmen, dass ein angemessenes Schutzniveau gewährleistet wird. Das SDM liefert dafür generische Standardmaßnahmen, die die Umsetzung der Schutzziele gewährleisten können[36] und die zukünftig durch einen Maßnahmenkatalog mit einzelnen Bausteinen ergänzt werden.

Bei einem hohen Risiko werden auch die Anforderungen an die Maßnahmen erhöht: Sowohl das Ergreifen zusätzlicher Maßnahmen als auch die Erhöhung der Wirkung einer bereits ergriffenen, skalierbaren Maßnahme kommen dafür in Betracht.[37] Ein Beispiel für eine solche Erhöhung ist etwa eine Erhöhung der Schlüssellänge in einem kryptografischen Verfahren. Zudem kommt auch eine Erhöhung der Zuverlässigkeit der Ausführung einer Maßnahme durch Ausschluss von Störeinflüssen in Betracht. Einfache Beispiele hierfür sind die Einführung des Vier-Augen-Prinzips oder geteilter Schlüssel in einem bestimmten Verfahren.

In diesem Schritt ist es wichtig zu beachten, dass ein iteratives Vorgehen gefordert ist. Auf diese Weise lassen sich die Auswirkungen, die verschiedene technische und organisatorische Maßnahmen aufeinander haben, berücksichtigen. Zudem kann die Einführung einer bestimmten Maßnahme auch zu neuen Risiken führen.

Der Prozess, der für eine solche Analyse erforderlich ist, lässt sich im Rahmen einer auf dem SDM basierenden Datenschutz-Folgenabschätzung im Sinne von Art. 35 DSGVO/Art. 27 JI-Richtlinie umsetzen. Diese lässt sich nach der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen skalieren, sodass die Datenschutz-Folgenabschätzung auch für Verarbeitungsvorgänge, die nur ein geringes Risiko aufweisen geeignet ist.[38] Zudem macht die Datenschutz-Folgenabschätzung die Risikobeurteilung nachvollziehbar und unterstützt so die verantwortliche Stelle bei der Umsetzung ihrer Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO und Art. 4 Abs. 4 JI-Richtlinie.

4 Fazit

Aus dem neuen EU-Datenschutzrecht ergibt sich nicht ohne Weiteres wie das Risiko für die Rechte und Freiheiten natürlicher Personen ermittelt wird. Diese Ermittlung muss aber von der Bestimmung möglicher Beeinträchtigungen der EU-Grundrechte geleitet sein. Die abstrakten Anforderungen der neuen Regelungen werden durch das SDM operationalisiert und lassen sich mit dessen Hilfe in der Praxis umsetzen lassen. Über die Schutzziele lassen sich die Risiken für die Rechte und Freiheiten natürlicher Personen, die sich aus der Beeinträchtigung ihrer EU-Grundrechte bei einer Verarbeitung ergeben, identifizieren und eindämmen. Zusammen mit dem Maßnahmenkatalog des SDM kann so die Einhaltung der rechtlichen Anforderungen für eine Organisation erheblich erleichtert werden.

33 AK Technik, Das Standard-Datenschutzmodell, S. 40.

34 Zur Abwägung der Schutzziele miteinander vgl. Bock/Robrahn, in diesem Heft.

35 Alexy, Die Gewichtsformel, S. 778-783.

36 AK Technik, Das Standard-Datenschutzmodell, S. 30-33.

37 AK Technik, Das Standard-Datenschutzmodell, S. 40.

38 Ausführlicher dazu Forum Privatheit, White Paper Datenschutz-Folgenabschätzung.