MARKUS SCHRÖDER

Der risikobasierte Ansatz in der DS-GVO

Risiko oder Chance für den Datenschutz?

Verordnungsevaluierung
Berechtigte Interessen
Datenschutz-Compliance
Pflichtenskalierung

■ Der risikobasierte Ansatz ist eines der Kernelemente der DS-GVO. Nach überwiegender Auffassung dient der risikobasierte Ansatz der Skalierung innerbetrieblicher Maßnahmen, nicht aber dem Wegfall jeglicher Maßnahmen zur Herstellung von Datenschutz-Compliance. Dies erscheint nur konsequent, da die gesetzlichen Anforderungen durch den risikobasierten Ansatz nicht unterlaufen, sondern nur ergänzt werden sollen. Aber ist dies wirklich konsequent? Könnte ein risikobasierter Ansatz nicht vielmehr einen rechtsbasierten Ansatz ablösen? Wäre dies rechtlich überhaupt möglich? Schließlich handelt es sich beim Recht auf Datenschutz um ein Grundrecht.

■ The risk-based approach is one of the key elements of the General Data Protection Regulation (GDPR/DS-GVO). In the majority opinion, the risk-based approach serves the purpose of scaling inner-company measures, not, however, the discontinuation of all measures to create data protection compliance. This seems only consistent as the statutory requirements should not be subverted by the risk-based approach, but rather only supplemented. But is this truly consistent? Could a risk-based approach not rather replace a law-based approach? Would this even be legally possible? After all, the right to data protection is a basic right.
Lesedauer: 18 Minuten

I. Einleitung

Der risikobasierte Ansatz ist eine der durch die DS-GVO eingeführten Neuerungen im Datenschutzrecht.[1] An diesem Ansatz orientieren sich die nach Art. 32 Abs. 1 DS-GVO zu treffenden technisch-organisatorischen Maßnahmen. Wesentlicher Ausdruck des risikobasierten Ansatzes ist allerdings die nach Art. 35 DS-GVO durchzuführende Datenschutz-Folgenabschätzung. Diese ist bei einem voraussichtlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen durchzuführen. Doch wann liegt ein solches Risiko vor? Zwar gibt die DS-GVO in Erwägungsgrund 75 Hinweise für eine Risikobewertung. Dennoch kann bei dieser Bewertung eine Fehlerquote verbleiben.[2] Zur Implementierung eines Risikomanagements haben die Aufsichtsbehörden bereits Handlungsempfehlungen gegeben.[3] Aber was bedeutet es, wenn bei der Risikobewertung das Ergebnis ein allenfalls geringes Risiko der Datenverarbeitung ist? Nach überwiegender Auffassung dient der risikobasierte Ansatz der Skalierung innerbetrieblicher Maßnahmen, nicht aber dem Wegfall jeglicher Maßnahmen zur Herstellung von Datenschutz-Compliance.[4] Dies ist zunächst konsequent, da die gesetzlichen Anforderungen durch den risikobasierten Ansatz der DS-GVO ergänzt werden sollen.

II. Der risikobasierte Ansatz in der DS-GVO

1. Grundlagen des risikobasierten Ansatzes

Soweit ersichtlich war die erste Stellungnahme einer Datenschutzaufsichtsbehörde zu einem risikobasierten Ansatz im Datenschutz diejenige der *Information and Privacy Commissioner Ontario*, Canada, aus dem Jahre 2010 (Privacy Risk Management).[5] Zwar wird in der DS-GVO selbst und auch in der Diskussion, die zu deren risikobasiertem Ansatz geführt hat, nicht auf diese Quelle verwiesen. Da jedoch auch Privacy by Design, ein ebenfalls von *Ann Cavoukian* entwickeltes Konzept, Eingang in die DS-GVO gefunden hat, kann man jedenfalls davon ausgehen, dass diese Quelle in der Diskussion um den risikobasierten Ansatz bekannt war. Zumal dieses Papier selbst auf das Konzept Privacy by Design verweist. Im Jahre 2012 veröffentliche die *CNIL* das erste Papier einer europäischen Behörde hierzu.[6] In der Praxis haben insbesondere auch die Stellungnahmen des *ICO* zu einem Datenschutz-Risikomanagement Beachtung gefunden.[7] Vorarbeiten hierzu wurden im Auftrag des *ICO* durch *RAND Europe* bereits im Jahre 2009 erbracht.[8] Diese aufsichtsbehördlichen Papiere hatten im Wesentlichen die Übernahme und Anpassung bestehender Verfahren des Risikomanagements in und auf den Bereich des Datenschutzes zum Gegenstand. Auf Unternehmensseite waren Datenschutzrisiken aber ohnehin bislang schon einer Risikobewertung zu unterziehen [9] In den Verhandlungen zur DS-GVO war der *Rat* die treibende Kraft zur Implementierung eines risikobasierten Ansatzes in das Regelwerk.[10] Insbesondere Deutschland war hier sehr aktiv. Der damalige *Bundesinnenminister* befürwortete ausdrücklich einen risikobasierten Ansatz.[11] In der Folgezeit brachte die deutsche Delegation dann auch zahlreiche Änderungsanträge in diesem Sinne in die Ratsverhandlungen ein.[12] Zwar gab es auch aus dem *Parlament* Stimmen, die eine größere Risikoorientierung forder-

1 Was die Wirkung für die gesamte Verordnung betrifft, s.a. *Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 24 Rdnr. 19 ff. sowie *Veil*, in: Gierschmann/Schlender/Stenzel/Veil, Komm. Datenschutz-Grundverordnung, 1. Aufl. 2018, Art. 24 Rdnr. 78 ff.

2 *DSK*, Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, S. 4: „Für jeden möglichen Schaden werden die Eintrittswahrscheinlichkeit und Schwere abgeschätzt. Diese lassen sich nur in ganz wenigen Ausnahmefällen mathematisch fassen."

3 *Information and Privacy Commissioner Ontario*, Privacy Risk Management, abrufbar unter: https://www.ipc.on.ca/wp-content/uploads/2010/04/privacy-risk-management-building-privacy-protection-into-a-risk-management-framework-to-ensure-that-privacy-risks-are-managed.pdf; *CNIL*, Methodology for Privacy Risk Management, abrufbar unter: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf; *ICO*, Conducting privacy impact assessments – code of practice, abrufbar unter: https://www.pdpjournals.com/docs/88317.pdf ; *ICO*, Risk Management Policy and Procedures, abrufbar unter: https://de.scribd.com/document/323863550/Ico-Risk-Management-Policy-and-Procedures.

4 *Thoma*, ZD 2013, 578, 581; *CIPL*, A Risk-based Approach to Privacy: Improving Effectiveness in Practice, S. 4; *Kuner/Cate/Millard/Svantesson/Lynskey*, IDPL 2015, 95, 96.

5 *Information and Privacy Commissioner Ontario* (o. Fußn. 3).

6 *CNIL* (o. Fußn. 3).

7 *ICO*, Conducting privacy impact assessments – code of practice (o. Fußn. 3); *ICO*, Risk Management Policy and Procedures (o. Fußn. 3) – hier wird auf das Risiko aus Sicht des Verantwortlichen abgestellt.

8 *Robinson/Graux/Botterman/Valeri*, Review of the European Data Protection Directive, abrufbar unter: https://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf.

9 *Weiss*, Datenschutz im globalen Konzern, in: Inderst/Bannenberg/Poppe, Compliance, 3. Aufl. 2017, Kap. 6. A.

10 *Albrecht*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Einl. Rdnr. 198.

11 *EU-Kommission*, MEMO/13/177.

12 *EU-Rat*, Dok. Nr. 12267/2/14 REV 2, S. 9 ff.

ten.[13] Diese Position war jedoch im *Parlament* umstritten und fand dort schließlich keine Mehrheit. Im Mai 2013 legte die damalige *irische Ratspräsidentschaft* ein Arbeitspapier vor, welches die Aufnahme eines risikobasierten Ansatzes in den vorliegenden Entwurf der *Kommission* vorsah.[14] Erste Äußerungen der *britischen Regierung* unterstützten diese Position.[15] Dieser Position schloss sich in Teilen das *ICO* an.[16] Zu dieser Zeit begann auch die Unternehmensseite sich aktiv für einen risikobasierten Ansatz zu interessieren.[17] Diese Bemühungen fielen durchaus auch auf Zustimmung von Behördenseite.[18] Dennoch sah sich im Jahre 2014 die *Art. 29-Datenschutzgruppe* genötigt, in die mittlerweile in Gang gekommene Diskussion ein ihre Position klarstellendes Papier einzubringen.[19] Ein risikobasierter Ansatz wurde auch dort zwar grundsätzlich begrüßt. Er dürfe aber nicht zur Aufweichung der Zulässigkeitsvoraussetzungen für Datenverarbeitungen führen. In den Trilog-Verhandlungen hat sich dann dieser begrenzte risikobasierte Ansatz gegenüber den weitergehenden Positionen des *Rats* durchgesetzt.[20] Der risikobasierte Ansatz wird nunmehr auch bei Novellierungen nationaler Datenschutzgesetze von Drittstaaten, wie der Schweiz, als Kernbereich der DS-GVO erkannt und umgesetzt, um einen Angemessenheitsbeschluss der *EU-Kommission* nach Art. 46 Abs. 3 DS-GVO zu erhalten.[21]

2. Risikobegriff

Unabhängig davon, ob man nun einen risikobasierten Ansatz eher positiv oder eher negativ beurteilt, stellt sich die Frage, welches Risiko eigentlich Gegenstand dieses Ansatzes sein soll. Interessanterweise findet sich in Art. 4 DS-GVO (Begriffsbestimmungen) keine Definition des Risikos. Einen Hinweis auf den Risikobegriff der DS-GVO enthält Art. 24 Abs. 1 DS-GVO, wonach der Verantwortliche die „Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen" berücksichtigen muss. Dies ergibt zwar die Rechtsgüter, die ggf. von Gefahren bedroht sind, ist aber eher eine vage Vorgabe zur Risikoabschätzung, nicht jedoch eine greifbare Risikodefinition.

Konkretere Anhaltspunkte hierfür lassen sich den Erwägungsgründen 75 und 76 DS-GVO entnehmen. Nach Erwägungsgrund 75 DS-GVO können die „Risiken für die Rechte und Freiheiten natürlicher Personen mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, 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, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleitung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft." Dabei sollten nach Erwägungsgrund 76 DS-GVO „die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt." Die Zusammenstellung der potenziellen Risiken in Erwägungsrund 75 DS-GVO erscheint willkürlich und unsystematisch. Auf der anderen Seite begegnet aber auch eine weitere Konkretisierung der Risiken Kritik.[22] Allerdings dienen die Erwägungsgründe lediglich der Auslegung der jeweiligen europarechtlichen Normen.[23]

Die *DSK* hat in ihrem Kurzpapier zum „Risiko für die Rechte und Freiheiten natürlicher Personen"[24] folgerichtig eine Orientierungshilfe zur Auslegung des Risikobegriffs vorgelegt. Jedoch hat die *DSK* bei ihren dortigen Ausführungen den Risikobegriff teilweise contra legem überdehnt.[25] So nimmt sie insbesondere an, dass es keine Datenverarbeitung ohne Risiko für die Rechte und Freiheiten natürlicher Personen geben könne.[26] Zudem wird das Vorliegen eines Risikos mit einem Schaden gleichgesetzt.[27] Durch diese Überdehnung des Risikobegriffs wird das Potenzial des risikobasierten Ansatzes, eine Skalierbarkeit der zu ergreifenden Maßnahmen zu ermöglichen, konterkariert.

Wenig hilfreich ist leider auch ein Blick auf die Datenschutz-Folgenabschätzung als ein Kernelement des risikobasierten Ansatzes in der DS-GVO. Zwar gibt Art. 35 Abs. 3 DS-GVO zumindest Hinweise dazu, wann eine Datenschutz-Folgenabschätzung vorzunehmen ist und damit ein hohes Risiko i.S.v. Art. 35 Abs. 1 DS-GVO vorliegt. Allerdings finden sich bei diesen Regelbeispielen die unbestimmten Rechtsbegriffe „systematisch" und „umfassend", sodass sich hier noch nicht einmal Rechtssicherheit hinsichtlich eines hohen Risikos, geschweige denn hinsichtlich

13 *Alvaro*, Lifecycle Data Protection Management, S. 6, abrufbar unter: https://www2.acc.com/chapters/euro/upload/Alexander-Alvaro-LIFECYCLE-DATA-PROTECTION-MANAGEMENT.pdf.

14 *EU-Rat*, Dok. Nr. 10227/13 ADD 1.

15 *Hawk*, Hawktalk, v. 17.6.2013, abrufbar unter: https://amberhawk.typepad.com/amberhawk/2013/06/how-the-uks-risk-based-data-protection-policy-can-result-in-lower-standards-of-data-protection.html.

16 *ICO*, Letter to Chris Grayling MP, v. 24.5.2013, abrufbar unter: https://ico.org.uk/media/about-the-ico/documents/1042558/rt-hon-chris-grayling-ministry-of-justice-20130603.pdf.

17 *Digital Europe*, Comments on the risk-based approach, abrufbar unter: https://teknologiateollisuus.fi/sites/default/files/file_attachments/elinkeinopolitiikka_digitalisaatio_tietosuoja_digitaleurope_risk_based_approach.pdf.

18 *Hustinx*, in: Ft.com v. 26.6.2013, Brussels – Astroturfing takes root, abrufbar unter: https://www.ft.com/content/74271926-dd9f-11e2-a756-00144feab7de.

19 *Art. 29 Data Protection Working Party*, WP 218: Statement on the role of a risk-based approach in data protection legal Frameworks. Dieses Working Paper wurde allerdings bislang nicht vom *EDSA* befürwortet.

20 *Albrecht* (o. Fußn. 10), Rdnr. 200.

21 *Gordon*, SJZ 2018, 162, 165 f.

22 *Rost*, vorgänge #221/222, 79, 82.

23 *Schroeder*, JuS 2004, 180, 183.

24 *DSK*, Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen.

25 So auch *Veil*, CR-online.de Blog, v. 2.5.2018, abrufbar unter: https://www.cr-online.de/blog/2018/05/02/datenschutzverstoss-schaden/.

26 *DSK* (o. Fußn. 24), S. 2: „Da es vollständig risikolose Verarbeitungen nicht geben kann ..."

27 *DSK* (o. Fußn. 24), S. 1: „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."

eines Risikos unterhalb eines hohen Risikos erlangen lässt. Die Blacklist der *DSK*[28] gem. Art. 35 Abs. 4 DS-GVO ist diesbezüglich etwas detaillierter, überlässt dem Anwender aber ebenfalls Zweifelsfälle. Mehr Rechtssicherheit könnten Whitelists nach Art. 35 Abs. 5 DS-GVO bringen, da hier verbindlich gesagt werden müsste, in welchen Fällen jedenfalls kein hohes Risiko vorliegt. Die einzige Whitelist wurde – soweit ersichtlich – bislang von der *österreichischen Datenschutzbehörde* veröffentlicht und nimmt wichtige Handlungsfelder, wie Kundenverwaltung und -betreuung, Marketing für eigene Zwecke und Personalverwaltung von dem Erfordernis, eine Datenschutz-Folgenabschätzung durchführen zu müssen, aus[29] und stellt damit für diese Verarbeitungsvorgänge fest, dass dort jedenfalls kein hohes Risiko gegeben ist. Der risikobasierte Ansatz droht in Anbetracht der Rechtsunsicherheit und der damit einhergehenden Zweifelsfälle allerdings zu einer Erhöhung und nicht zu einer sinnvollen Abstufung der Accountability-Pflichten zu führen.[30]

3. Rechte und Freiheiten natürlicher Personen

Vor dem Hintergrund der Konturenlosigkeit des Risikobegriffs der DS-GVO wird weiterhin kritisiert, dass das Datenschutzrecht keinen klaren Schutzbereich habe.[31] Dies ist sicher richtig. Vielmehr handelt es sich dabei um eine Schnittmenge aus verschiedenen Bereichen, die wiederum nicht klar voneinander abzugrenzen sind. Diese Rechtsunsicherheit ist jedoch bis zu einem gewissen Grad hinzunehmen. Würde man das Datenschutzrecht auf einen oder mehrere Schutzbereiche ausdrücklich beschränken, bestünde die Möglichkeit, das erfasste Risiko für nicht mehr existent und damit auch das Datenschutzrecht für überholt anzusehen. Beschränkt man z.B. den Schutzbereich des Datenschutzrechts auf die Risiken Diskriminierung, Rufschädigung und gesellschaftliche Nachteile, könnte man mit der Post-Privacy-Bewegung diese Risiken für nicht mehr existent ansehen, falls es keine datenschutzrechtlichen Restriktionen mehr gebe. Da dann alles öffentlich wäre, könnten diese Risiken auch nicht mehr entstehen.[32] Eine restriktive Definition des Schutzbereichs birgt daher die Gefahr, zu kurz zu greifen und andere gleichwertige potenzielle Risiken nicht zu beachten. Zudem ist die Kritik, dass der Schutzbereich des Datenschutzrechts zu unbestimmt sei, bereits zum BDSG a.F. geäußert worden.[33]

Daher handelt es sich um keine originär durch die Einführung der DS-GVO entstandene Diskussion, sondern um eine sehr grundsätzliche Debatte. Orientieren muss sich diese Diskussion rechtlich an Art. 7 und Art. 8 GRCh. Art. 7 GRCh übernimmt weitestgehend den Schutzbereich von Art. 8 EMRK, d.h. das Recht auf Privatsphäre. Zu dieser Norm liegt eine ausführliche Rechtsprechungskasuistik des *EGMR* vor.[34] Art. 8 GRCh normiert demgegenüber ein Recht auf den Schutz personenbezogener Daten. Ungeklärt ist jedoch das Verhältnis dieser Normen zueinander. So lässt es sich vertreten, dass Art. 8 GRCh lex specialis zu Art. 7 GRCh ist.[35] Der *EuGH* wiederum prüft Art. 8 GRCh regelmäßig i.V.m. Art. 7 GRCh.[36] Dies spricht dafür, dass Art. 8 GRCh nur eine Konkretisierung von Art. 7 GRCh und kein originäres Grundrecht darstellt. Bei Sachverhalten im nicht-öffentlichen Bereich erfolgt vom *EuGH* allerdings auch eine Prüfung von Art. 8 GRCh ohne Verbindung zu Art. 7 GRCh.[37] Unabhängig von der dogmatischen Einordnung von Art. 8 GRCh ist aber davon auszugehen, dass bei der Verarbeitung personenbezogener Daten die Voraussetzungen von Art. 8 Abs. 2 GRCh vorliegen müssen, wonach jede Verarbeitung personenbezogener Daten einer rechtlichen Grundlage bedarf. Allerdings ist auch bei einem grundrechtlichen Bezug des Datenschutzes ein risikobasierter Ansatz nicht per se abzulehnen.[38]

4. Diskussion des risikobasierten Ansatzes in der Literatur

a) Contra risikobasierter Ansatz

Bereits während der Verhandlungen zur DS-GVO wurde der risikobasierte Ansatz kritisiert. Hier bediente man sich z.T. polemischer Behauptungen. So wurde der risikobasierte Ansatz als trojanisches Pferd der Datenschutzreform bezeichnet.[39] Auf der sachlichen Ebene wurde die Befürchtung geäußert, dass durch den risikobasierte Ansatz die Pflichten der datenverarbeitenden Unternehmen sowie die Rechte der Betroffenen reduziert werden sollten.[40] Ein beachtliches Argument, das gegen den risikobasierten Ansatz vorgebracht wurde, ist, dass eine Risikoabschätzung durch den Verantwortlichen regelmäßig an sämtlichen Betroffenen eines bestimmten Verarbeitungsvorgangs im Kollektiv vorgenommen werden dürfte und damit das individuelle Risiko eines Betroffenen außer Acht gelassen werde.[41] Dieses Argument ist aber nur teilweise tragfähig, da i.R.d. Beurteilung einer Datenschutzverletzung auch das Risiko für die betroffene Person zu prüfen ist. Damit wird deutlich, dass die Risikobewertung nach der DS-GVO unterschiedliche Schwerpunkte hat.[42] Eine weitere beachtliche Position gegen den risikobasierten Ansatz geht davon aus, dass sich die Asymmetrie zwischen den Verantwortlichen und den Betroffenen vergrößere, wenn die das Risiko begründende Stelle zugleich über die Tragbarkeit dieses Risikos entscheide.[43] Auch dieses Argument vermag jedoch nur teilweise zu überzeugen, da isoliert auf den Schutzzweck der Informationsasymmetrie abgestellt wird.[44]

---

28 *DSK*, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist; auf die bereits auf Länderebene ergangenen Blacklists soll an dieser Stelle nicht eingegangen werden.

29 Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung, Bundesgesetzblatt für die Republik Österreich, 2018 Teil II, v. 25.5.2018; diese Verordnung ist aber i.R.d. rechtsvergleichenden Auslegung und der Lückenfüllung auch in Deutschland beachtlich, vgl. *Mansel*, JZ 1991, 529, 531.

30 S. hierzu auch *Veil*, ZD 2018, 9, 13 ff.

31 *Veil*, CR-online.de Blog, v. 6.2.2019, abrufbar unter: https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/; s. dazu aber *Bock*, Schutzgut des Datenschutzrechts – Eine Replik auf Veil, Schutzgutmisere – Teil I, CR-online.de Blog, v. 22.3.2019, abrufbar unter: https://www.cr-online.de/blog/2019/03/22/schutzgut-des-datenschutzrechts-eine-replik-auf-veil-schutzgutmisere-teil-i/ und Teil II, CR-online.de Blog, v. 29.3.2019, abrufbar unter: https://www.cr-online.de/blog/2019/03/29/schutzgut-des-datenschutzrechts-eine-replik-auf-veil-schutzgutmisere-teil-ii/.

32 *Heller*, Post Privacy – Prima leben ohne Privatsphäre, S. 7 f.

33 *Bull*, NJW 2006, 1617 ff.; *ders.*, Sinn und Unsinn des Datenschutzes, 1. Aufl. 2015, S. 37 ff.; zu einer Übersicht der verschiedenen Schutzgüter s. *von Lewinski*, Die Matrix des Datenschutzes, 1. Aufl. 2014, S. 17 ff.

34 S. hierzu *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 1. Aufl. 2014, S. 54 ff.

35 Zum Verhältnis dieser Normen s. *Michl*, DuD 2017, 349.

36 *EuGH* ZD 2014, 296, 297; *EuGH* MMR 2011, 122 m. Anm. *Hornung*; zust. *Roßnagel*, NJW 2019, 1, 2.

37 *EuGH* K&R 2012, 35 m. Anm. *Schröder*; *EUGH* MMR 2012, 334 m. Anm. *Solmecke/Dam*.

38 *Quelle*, Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level?, S. 3 f., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2726073.

39 *Bergemann*, netzpolitik.org, v. 11.3.2013, abrufbar unter: https://netzpolitik.org/2013/innen-und-justizminister-reiten-auf-trojanischen-pferden-richtung-datenschutzreform/.

40 *Albrecht*, PM v. 7.3.2013, abrufbar unter: https://www.gruen-digital.de/2013/03/eu-datenschutz-ministerrat-muss-beim-datenschutz-liefern/; *vzbv*, PM v. 25.11.2014, abrufbar unter: https://www.vzbv.de/pressemitteilung/eu-datenschutzverordnung-weichen-stellen-fuer-mehr-datenschutz-0.

41 *Hawk* (o. Fußn. 15).

42 *Art. 29-Datenschutzgruppe*, WP 250 rev.01: Guidelines on Personal data breach notification under Regulation 2016/679, S. 23.

43 *Rost*, vorgänge #221/222, 79, 84.

44 Zu diesem Schutzzweck s. *von Lewinski* (o. Fußn. 33), S. 55 ff.; *Drackert* (o. Fußn. 34), S. 280 ff.

b) Pro risikobasierter Ansatz

■ Begrenzter risikobasierter Ansatz

Der begrenzte risikobasierte Ansatz, der letztlich auch Eingang in die DS-GVO gefunden hat, geht davon aus, dass die grundlegenden datenschutzrechtlichen Prinzipien durch diesen Ansatz nicht ersetzt werden sollen.[45] Es gehe vielmehr um eine Skalierung der zu ergreifenden Maßnahmen auf Basis eines Risikomanagements.[46] Dieser Ansatz wurde in Teilen der Literatur allerdings nicht als große Neuerung, sondern eher als Feststellung einer Selbstverständlichkeit angesehen: „We have always managed risks in data protection law",[47] „Understanding data protection as risk regulation"[48] oder „Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing".[49] Auf der anderen Seite wurde aber auch zu bedenken gegeben, dass man nicht beides habe könne: einen risikobasierten Ansatz und ein Festhalten an den bisherigen datenschutzrechtlichen Grundprinzipien.[50] Daher wurde folgerichtig auch die Frage aufgeworfen, ob Art. 24 Abs. 1 DS-GVO auch für die Grundsätze der Datenverarbeitung, für die Rechtsgrundlagen und für die Betroffenenrechte gelte.[51] De lege lata sprechen aber rechtssystematische Erwägungen eher gegen diese Auffassung, da Art. 24 Abs. 1 DS-GVO nicht „vor die Klammer gezogen" als Grundsatz in Art. 5 DS-GVO formuliert wurde.

■ Reiner risikobasierter Ansatz

In Teilen der Literatur wird der risikobasierte Ansatz als Möglichkeit gesehen, bisherige Grundprinzipien des Datenschutzes, wie das sog. Verbotsprinzip[52] und das unscharfe Kriterium des Personenbezugs,[53] abzulösen. Diese Ansätze sind vielversprechend, um das Datenschutzrecht in praktischer und dogmatischer Hinsicht weiterzuentwickeln. Allerdings handelt es hierbei um Ansätze, die auch de lege ferenda Paradigmenwechsel hinsichtlich bestehender Regelungskonzepte bedeuten würden.[54] Es bleiben aber auch Vorhaben, wie die Verordnung über den freien Verkehr nicht personenbezogener Daten in der EU, zu beobachten, die ebenfalls in diese Richtung deuten.

III. Fazit

Der risikobasierte Ansatz stellt zwar nicht das Allheilmittel für ein zeitgemäßes Datenschutzrecht dar. Er bietet allerdings eine nicht zu unterschätzende Möglichkeit, den Datenschutz zu bereichern. Unterscheiden muss man hier gerade vor dem Hintergrund der Evaluierung nach Art. 97 DS-GVO allerdings zwischen Ansätzen, die allenfalls de lege ferenda umsetzbar wären, und Ansätzen, die de lege lata durch reine Konkretisierungen des aktuell begrenzten risikobasierten Ansatzes der DS-GVO umsetzbar sind. Zu Ersteren gehören die Erwägungen, den risikobasierten Ansatz als Substitut für Kernprinzipien des aktuellen Datenschutzrechts, namentlich das sog. Verbotsprinzip und den Personenbezug der Daten, zu etablieren. Diese Konzepte verdienen aber eine Begleitung und Vertiefung in der weiteren Diskussion um die Fortentwicklung des Datenschutzrechts.[55] Allerdings dürfte eine Veränderung der aktuellen Grundprinzipien des Datenschutzrechts zeitlich und argumentativ sehr aufwändig sein. Es ist aber de lege ferenda wünschenswert, den risikobasierten Ansatz in Art. 5 DS-GVO zu den Verarbeitungsgrundsätzen aufzunehmen. Damit würde klargestellt, dass dieser Ansatz ein übergreifendes Grundprinzip der DS-GVO darstellt. Schon de lege lata lässt sich aber durch eine stärkere Berücksichtigung von Risikofaktoren bei der Interessenabwägung i.R.v. Art. 6 Abs. 1Satz 1 lit. f DS-GVO eine größere Konturierung des risikobasierten Ansatzes erzielen.[56] So könnte ein Erfüllen aller von Art. 24 Abs. 1 DS-GVO geforderten Maßnahmen zu einem regelmäßigen Überwiegen des berechtigten Interesses des Verantwortlichen führen. Hier könnte ein klarstellender Hinweis in den Erwägungsgründen erfolgen. Zudem könnte auch durch eine Justierung des erforderlichen Präzisierungsgrads bei der Angabe des Verarbeitungszwecks mehr Risikoadäquanz erreicht werden.[57] So wäre es denkbar, als Verarbeitungszweck für Big-Data-Analysen z.B. „stochastische Analysen" anzugeben. Ein weiterer Anwendungsfall des risikobasierten Ansatzes i.R.d. berechtigten Interesses ist eine stärkere Berücksichtigung der vernünftigen Erwartungen der betroffenen Person bei der Interessenabwägung.[58] Es könnten unternehmensbezogene Daten, auch soweit sie z.B. Ein-Mann-GmbHs oder Personengesellschaften betreffen, auf dieser Grundlage verarbeitet werden. Damit könnten im Einzelfall Abgrenzungsschwierigkeiten bei der Frage, ob ein Personenbezug vorliegt, entbehrlich sein. Darüber hinaus kann der risikobasierte Ansatz insbesondere bei einer Skalierung der Rechenschaftspflichten hilfreich sein.[59] Diese Ansätze könnten durch eine entsprechende klarstellende Stellungnahme des *EDSA* nach Art. 70 DS-GVO flankiert werden. Diese Erwägungen sollten zudem bei der Evaluierung nach Art. 97 DS-GVO berücksichtigt werden. Der risikobasierte Ansatz ist eine sinnvolle Ergänzung und Weiterentwicklung des Konzepts der regulierten Selbstregulierung.[60] Er bedarf lediglich weiterer Konkretisierung. Aber bei allem Interesse für einen risikobasierten Datenschutz darf auch nicht vergessen werden, dass Risikobewertungen auch immer selbst das Risiko bergen, einmal danebenliegen zu können.[61] Auch ein schwarzer Schwan[62] könnte durchaus einmal auftauchen.

Markus Schröder, LL.M. (Informationsrecht), CIPP/E, ist Rechtsanwalt in Köln.

45 *CIPL* (o. Fußn. 4), S. 4; *Kuner/Cate/Millard/Svantesson/Lynskey*, IDPL 2015, 95, 96.
46 *Thoma*, ZD 2013, 578, 580 f.; *Drackert* (o. Fußn. 34), S. 280 ff.
47 *Gellert*, EDPL 2016, 481.
48 *Gellert*, Journal of Internet Law 2015, 3.
49 *Gellert*, IRIS 2017 Tagungsband, S. 527.
50 *Quelle*, The risk revolution in EU data protection law, S. 21 f., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000382.
51 *Veil* (o. Fußn. 25).
52 *Schneider/Härting*, DGRI Jahrbuch 2011, S. 15, 36 ff.
53 *Schmitz*, ZD 2018, 5, 8.
54 Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff s. *Roßnagel*, NJW 2019, 1.
55 So auch *Bull*, JZ 2017, 797, 804 ff.; *Veil*, NVwZ 2018, 686; *ders.*, ZD 2015, 347; *ders.*, CR-online Blog, v. 7.12.2018, abrufbar unter: https://www.cr-online.de/blog/2018/12/07/verhasst-gefuerchtet-geleugnet-ignoriert/.
56 So auch *Härting*, Datenschutz-Grundverordnung, 2016, Rdnr. 134.
57 Vgl. *Veil*, NJW 2018, 3337, 3339 ff.
58 Diese aus dem US-Recht stammende Rechtsfigur (reasonable expectation of privacy) hat auch Eingang in die Rspr. des *EGMR* zu Art. 8 EMRK gefunden, Übersicht s. bei *Drackert* (o. Fußn. 34), S. 73 ff.; zur Berücksichtigung der Sphärentheorie i.R.d. DS-GVO s. *Raji*, ZD 2019, 61, 66.
59 Vgl. *Veil*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil II. Kap. 1. E.
60 Zu diesem Konzept vgl. *Schröder*, ZD 2012, 418.
61 Vgl. *Hofstetter*, Sie wissen alles, 2014, S. 172 ff.
62 Der Begriff wurde von *Nassim Nicholas Taleb* geprägt: „Der Schwarze Schwan: Die Macht höchst unwahrscheinlicher Ereignisse".