7 Jahre DSGVO – Ist der „Goldstandard“ noch zeitgemäß?

Streitgespräch

Dr. Stefan Brink ./. Dr. Winfried Veil

PinG: Vor nahezu neun Jahren ist die Datenschutz-Grundverordnung in Kraft getreten, und seit fast sieben Jahren gilt sie in allen 27 Mitgliedstaaten der Europäischen Union. Von ihren Befürwortern wurde die DSGVO seinerzeit als ein „Meilenstein“ in der Geschichte des Datenschutzes bezeichnet, als „Goldstandard“ gepriesen sowie als „Beginn einer neuen Zeitrechnung im Datenschutzrecht“ und als „festes Fundament für die anstehenden Herausforderungen der Digitalisierung gewürdigt. Sind Sie der Auffassung, dass diese Einschätzung zutreffend war?

: Ja. Allerdings haben wir im Laufe der letzten Jahre auch die Schwächen dieses „Goldstandards“ ausgemacht: Manches ist unhandlich, etwa der Umgang mit sensiblen Daten nach Art. 9 DSGVO oder die Rechenschaftspflicht des Art. 5 Abs. 2, anderes läuft systematisch falsch wie die Regulierung durch unabhängige Aufsichtsbehörden, welche die Interessen der Betroffenen prinzipiell überbewerten.

Veil: Ich bleibe bei meiner Einschätzung von 2018. Die DSGVO ist ein Irrweg – oder, um es mit den Worten des Herausgebers dieser Zeitschrift zu sagen: die ‚Perfektion einer Sackgasse‘. Und anscheinend wollen wir diese Sackgasse auch bis zum Ende gehen.

PinG: Die Kommission hat stets den „risikobasierten Ansatz“ der DSGVO betont. Bei genauerer Betrachtung drängt sich die Frage auf, ob es diesen Ansatz tatsächlich gibt. Zumindest dürften nur wenige Vorschriften das Vorhandensein eines Risikos voraussetzen. Teilen Sie diese Einschätzung und wie bewerten Sie diese Ausrichtung der DSGVO?

Brink: Tatsächlich hat die EU-Kommission die DSGVO 2016 damit angepriesen, dass

der „risikobasierte Ansatz“ für besonders passgenaue und verhältnismäßige Regelungen sorgt. Das Versprechen lautete: Nichts wird reguliert, was nicht reguliert werden muss, um Schaden abzuwenden.

Dieses Versprechen war riskant, denn beim Datenschutz geht es nicht immer um so handfeste Dinge wie Datendiebstahl oder die Veröffentlichung von Nacktbildern. Häufig geht es um immaterielle Schäden, um Ängste, Verhaltensänderungen oder Übermacht.

Der „risikobasierte Ansatz“ findet sich in der DSGVO eher selten, etwa bei der Datenpanne oder bei technisch-organisatorischen Maßnahmen. Er sollte häufiger vorkommen, denn nur wenn die informationelle Selbstbestimmung der Bürger wirklich auf dem Spiel steht sollte die wirtschaftliche Nutzung von Daten eingeschränkt werden.

Veil: Ja, der risikobasierte Ansatz – ein schillernder Begriff für ein vages Konzept. Mit ihm hat die EU-Kommission die DSGVO damals tatsächlich beworben. Letztlich wurde er zur Beruhigungspille für die Gegner eines „zu strengen“ Datenschutzes. Für die Vertreter der reinen Lehre des Datenschutzes war er zu Anfang ein rotes Tuch. Sie witterten im risikobasierten Ansatz ein trojanisches Pferd. Durchgesetzt haben sich im Großen und Ganzen die Gegner des risikobasierten Ansatzes.

Selten findet sich der risikobasierte Ansatz in der DSGVO allerdings nicht. Der Begriff des

Risikos taucht 73 Mal im Normtext auf. Man könnte die DSGVO unter Inanspruchnahme des risikobasierten Ansatzes auch datennutzungsfreundlicher interpretieren. Daran haben aber die Aufsichtsbehörden augenscheinlich kein Interesse. Von denen gibt es fast nichts zum risikobasierten Ansatz. Und für die Rechtsanwender ist eine extensive Interpretation ohne Unterstützung der Aufsichtsbehörden anscheinend zu „riskant“ (lacht).

Der Normgeber der DSGVO ist leider auf halber Strecke stehengeblieben. Ein wirkungsvoller risikobasierter Ansatz hätte risikoarme Datenverarbeitungen von allen oder bestimmten Bindungen des Datenschutzrechts freigestellt. Am Ende gelten aber fast alle der 68 Pflichten der DSGVO unabhängig vom Risiko der Datenverarbeitung. Durchgängig risikoabhängig ist nur, welche technisch-organisatorischen Maßnahmen zur Erfüllung der Pflichten ergriffen werden.

Die Grundidee des risikobasierten Ansatzes ist jedoch weiterhin lebendig. Die KIVerordnung verfolgt viel deutlicher als die DSGVO einen risikobasierten Ansatz. Und die Reformvorschläge von Professorin Wendehorst oder die von Jäkel, de Maizière, Steinbrück und Voßkuhle bauen auch auf dem risikobasierten Ansatz auf.

PinG: Wie verhält es sich mit der Vielzahl unbestimmter Rechtsbegriffe, die die DSGVO enthält? Ist es gelungen, hier im Laufe der vergangenen Jahre zu einer einheitlichen Rechtsanwendung zu gelangen oder besteht noch immer ein hohes Maß an Rechtsunsicherheit? Und haben die Mitgliedstaaten die Spezifikationsklauseln, die in die DSGVO aufgenommen wurden, gut genutzt oder nationale Rechtsvorschriften erlassen, die die gewollte Harmonisierung untergraben?

Veil: Die Prognose, dass EDSA und EuGH für Einheitlichkeit in der Rechtsanwendung sorgen würden, höre ich schon seit Inkrafttreten der DSGVO. Passiert ist in dieser Richtung jedoch wenig. Gefühlt fällt der EuGH jede Woche eine Entscheidung zur DSGVO. Dutzende Vorabentscheidungsverfahren liegen noch beim EuGH. Die Entscheidungen sind jedoch oft sibyllinisch oder nur sehr einzelfallbezogen. Gleichzeitig schießen die mitgliedstaatlichen Gerichtsentscheidungen ins Kraut. Und keiner von uns wird behaupten wollen, die Rechtspraxis in den anderen Mitgliedstaaten überblicken zu können.

Die Frage der Öffnungsklauseln würde ich davon gesondert betrachten. Sie sind zum Teil der Tatsache geschuldet, dass die EU überhaupt nicht regelungsbefugt ist (insbesondere im öffentlichen Bereich). Meines Erachtens sollte Deutschland viel stärker von den Öffnungsklauseln Gebrauch machen, um Rechtssicherheit herzustellen.

Brink: Die Anpassung der deutschen Rechtsordnung an die DSGVO verlief alles

andere als optimal, Deutschland hat Öffnungsklauseln gesehen, wo keine sind – und hat zu stark entgegen der DSGVO reguliert. Das aktuelle BDSG enthält eine Reihe von Beschränkungen der Betroffenenrechte, die nicht verordnungskonform sind. Und legendär ist die Fehlleistung des § 43 Abs. 4 BDSG, welche Bußgelder wegen Datenpan-nenmeldungen von der Zustimmung des Verantwortlichen abhängig machen.

Bei der Einheitlichkeit der Rechtsanwendung bin ich positiver gestimmt, sie wird im Laufe der kommenden Jahre vom EDSA und dem EuGH hergestellt werden. Solche Großprojekte wie die DSGVO benötigen sicherlich 10 bis 15 Jahre, bis sie auf europäischer Ebene rund laufen.

PinG: Die Institution des Europäischen Datenschutzausschusses hat bislang nicht die Erwartungen erfüllt, die in sie gesetzt wurden. Die Entscheidungen wurden bisher nicht zeitnah getroffen, und die meisten verbindlichen Beschlüsse wurden gerichtlich angefochten. Insbesondere für die großen Fälle wurde deshalb schon sehr früh gefordert, diese von einer zentralen Behörde auf europäischer Ebene bearbeiten und entscheiden zu lassen. Wie beurteilen Sie diese Forderung, die

zugleich verhindern würde, dass unabhängige Aufsichtsbehörden zugleich als Regulierungsbehörde agieren.

Brink: Je länger ich mir die Rolle von – Datenschutzaufsichtsbehörden ansehe – national und im EDSA – desto „schräger" kommt mir die Idee vor, unabhängige Stellen (die Datenschutzaufsichtsbehörden) zum Schiedsrichter über kollidierende Interessen von Grundrechtsträgern zu berufen: der Betroffenen als Inhaber der informationellen Selbstbestimmung und der Verantwortlichen als gewerblichen Verwertern von Daten. Dass es staatliche Stellen gibt, die prinzipiell Schwächere schützen, finde ich natürlich gut – aber den Aufsichtsbehörden einerseits die Parteinahme zugunsten der „Betroffenen" aufzuerlegen und sie gleichzeitig zum Schiedsrichter zu machen und als „Marktregulierungsbehörde" auftreten zu lassen, muss schief gehen.

Veil: Zur Rolle der Datenschutzaufsichtsbehörden wäre viel Kritisches, aber auch Mitleidiges zu sagen. Aber zunächst einmal hat Herr Brink natürlich recht. Dass diese einerseits wohlmeinender Berater des Verantwortlichen, andererseits Fürsprecher des

Betroffenen und schließlich mit Zwangsgewalt ausgestattete Vollzugsbehörde sein sollen, muss schief gehen. Noch negativer fällt der Befund aus, wenn man in Rechnung stellt, dass wir im Datenschutzrecht immer sofort im Grundrechtsbereich sind und die Aufsichtsbehörden eigentlich ständig Grundrechtsabwägungen vornehmen müssen, dabei aber „biased" zugunsten des Betroffenen sind bzw. sogar sein sollen.

PinG: Die EU hat in den vergangenen Monaten eine Vielzahl neuer Digitalgesetze wie zum Beispiel den Data Act und den AI Act verabschiedet. Halten Sie diese Rechtsakte wie die Kommission für eine willkommene Ergänzung und Verstärkung der DSGVO oder stellen sie aus Ihrer Sicht das Datenschutzsystem der EU ganz oder teilweise in Frage?

Veil: Wir haben es mit einem gesetzgeberischen Tsunami zu tun. Die EU will offenbar Regulierungsweltmeister sein. Allein die neun unmittelbar datenbezogenen Rechtsakte DSGVO, FFOD-VO, OD-PSI-RL, DMA, DGA, DSA, HVD-DVO, DA und AIA summieren sich auf 483 Artikel und 927 Erwägungsgründe. Niemand kann das noch überblicken. Immer behaupten die Rechtsakte, die DSGVO bliebe unberührt – nur, um dann doch Regelungen im Anwendungsbereich der DSGVO vorzunehmen. Natürlich unterminiert das die Rechtssicherheit und damit auch die DSGVO.

Brink: Die europäischen Digitalrechtsakte sorgen tatsächlich für Verwirrung und Frustration. Zwar sind nicht alle für jeden Verantwortlichen einschlägig oder auch nur von Bedeutung, aber die Fülle an Regelungen verunsichert bereits. Schon das schadet der Beachtung der DSGVO, denn auch Unternehmen, die rechtskonform arbeiten wollen, verlieren den Überblick und die Überzeugung, dass langfristig nur Compliance funktioniert. Hier sehe ich eine wichtige Aufgabe für die Aufsichtsbehörden, für Klarheit zu sorgen und wieder mehr Vertrauen herzustellen: Rechtskonformität ist wichtig und machbar.

Veil: Dafür ist es zu spät. Die Gesetze sind ja alle schon da. Und sie gehen auch nicht mehr weg. Und keiner blickt mehr durch. Ohne Rechtsänderungen wird es nicht gehen. Immerhin verspricht sogar die EUKommission in ihrem neuen Arbeitsprogramm Konsolidierung, Straffung und

Vereinfachung. Meine Prognose ist dennoch, dass das Datenschutzrecht aufgrund seiner durch immer weitere Rechtsakte gesteigerten Komplexität implodiert. Und über die KI-Disruption haben wir dabei noch gar nicht gesprochen. Ich meine, was ChatGPT da macht, ist doch alles offensichtlich datenschutzrechtswidrig. Und die ganze Welt nutzt es, obwohl die KI mit Quadrilliarden personenbezogener Daten europäischer Internetnutzer trainiert wurde und laufend weiterhin trainiert wird.

PinG: Viel Kritik wurde von Anfang an am sog. „one size fits all"-Ansatz geäußert. Die Tatsache, dass die DSGVO ohne jegliche Differenzierung dem Verantwortlichen Dokumentationspflichten sowie umfangreiche Transparenzund Informationspflichten auferlegt, bedeutet aus Sicht vieler unnötigen und kostenintensiven Aufwand. Aus einer jüngst veröffentlichten Umfrage des Bitkom geht hervor, dass über 80 % der befragten 600 Unternehmen von hohem oder sogar noch wachsendem Aufwand bei der Umsetzung des Datenschutzrechts berichten. Ein wesentlicher Schritt zur Entlastung könnte deshalb sein, Erleichterungen insbesondere für kleine und mittlere Unternehmen, aber auch für ehrenamtliche Vereine und ehrenamtlich Tätige zu schaffen. Ganz aktuell wird zudem gefordert, einen dreistufigen risikobasierten Ansatz einzuführen, der sich an der Unternehmensgröße orientiert. Halten Sie diese Forderungen für sinnvoll, vielleicht sogar für erforderlich?

Brink: One size fits all ist kein Zufall, und auch kein Zugeständnis an die sog. very large online platforms (VLOPs): Einheitliche Pflichten aller Datenverarbeiter sorgen für Rechtsklarheit und gleichmäßige Standards. Aus Sicht des Betroffenen ist es nämlich irrelevant, ob seine Daten von einem großen oder kleinen Verarbeiter genutzt werden: Er möchte seine Daten immer geschützt sehen. Einheitliche Pflichten erleichtern zudem den einheitlichen Rechtsvollzug durch die Aufsichtsbehörden.

Der von MdEP Voss verfolgte asymmetrische Ansatz, Datenschutzpflichten von der Unternehmensgröße abhängig zu machen, harmoniert bereits nicht mit dem risikobasierten Ansatz: die bloße Unternehmensgröße korreliert eben nicht notwendig mit dem Risiko der Datenverarbeitung. Tatsächlich ergeben sich Verarbeitungsrisiken aus der Datenmenge, betroffenen Datenarten (Art. 9 DSGVO) und den (nicht) eingesetzten TOMs als risikomindernde Maßnahmen – sie bestimmen das konkrete Ausmaß der Bedrohung des Grundrechts des Betroffenen, und eben nicht die schiere Größe des Verarbeiters.

Wichtiger wäre in der aufkeimenden Reformdiskussion, die EU-Kommission zu stärken. Dadurch würde jedenfalls die Transparenz und Vorhersehbarkeit der Entscheidungsprozesse auf EU-Ebene erhöht – einschließlich einer fairen Anhörung und Beteiligung aller Stakeholder. Die Kommission ist sicherlich am besten in der Lage, eine einheitliche, konsistente und nicht einseitig auf den Datenschutz fixierte Position zu entwickeln und langfristig zu vertreten.

Veil: Das ist natürlich viel zu kurz gesprungen, lieber Herr Brink. Der One-size-fitsall-Ansatz ist neben dem Verbotsprinzip der zentrale Kritikpunkt an der DSGVO. Dass dieselben exorbitanten Pflichten der DSGVO für das Finanzamt, für Google und Facebook, für das Forschungsdatenzentrum, für den Bäcker um die Ecke, für den Blogger, für den kleinen Handwerker, für den Hobbyfotografen, für den Sportverein, für die NGO und für die Oma bei der Einschulung des Enkels gelten sollen, ist doch Wahnsinn. Diese Erkenntnis scheint sich jetzt auch mehr und mehr durchzusetzen. Interessanterweise waren sich jüngst ja sogar Axel Voss und Max Schrems in dieser Kritik einig.

Die Anwendbarkeit der DSGVO an der Unternehmensgröße festzumachen, halte ich aber auch für unterkomplex. Man sollte vielmehr nichtkommerzielle Datenverarbeitungen ganz aus dem Anwendungsbereich der DSGVO ausnehmen. Man bräuchte nur die Haushaltsausnahme entsprechend zu erweitern. Es wäre ein kleiner Schritt für den Normgeber, aber ein großer für die Freiheit und das Grundrecht auf Datenverarbeitung. Advokaten des Datenschutzrechts vergessen gerne, dass der Betroffene ohne Datenschutz ja nicht schutzlos gestellt ist. Zahlreiche Schadensersatz-, Schmerzensgeld- und Unterlassungsansprüche des Zivilrechts sowie Verbote des Strafrechts schützen ihn.

PinG: In der Debatte um die DSGVO gab es in den vergangenen Jahren immer wieder Vorstöße, den Einsatz von Datenschutzbeauftragten in den Unternehmen zu dezimieren. Die jüngsten Reformvorschläge

weisen hier in eine Richtung, die befürchten lässt, dass nur noch in wenigen Unternehmen Datenschutzbeauftragte tätig sein werden. Wie stehen Sie dazu?

Brink: Betriebliche und behördliche Datenschutzbeauftragte sind essenziell für die Datenschutzkultur, mit ihnen steht und fällt das Datenschutzniveau vor Ort. Wir haben besonders in Deutschland eine ungute Tradition, viel zu sehr auf die Aufsichtsbehörden zu schielen und dabei zu vergessen, dass es viel wichtiger ist, die sinnvolle und praktische Datenschutzlösung vor Ort zu finden. Daher sehe ich mit großer Sorge, dass die neue Bundesregierung unsere Datenschutzlotsen von Bord schickt.

Veil: Die Anhebung der Mitarbeiterzahl, ab der Unternehmen einen Datenschutzbeauftragten benötigen, war schon in der Vergangenheit eher Ausdruck der Einfallslosigkeit der Politik beim Versuch, wenigstens ein bisschen Bürokratie abzubauen. Ich hätte da viele andere und auch wirkungsvollere Ideen. Aber angesichts der Überregulierung und Überbürokratisierung des Wirtschaftslebens kann ich (fast) jede Maßnahme zur Reduzierung des Erfüllungsaufwandes nur begrüßen, auch wenn ich die wertvolle Arbeit vieler Datenschutzbeauftragter zu schätzen weiß. Ich habe nur immer das Beispiel dieser kleinen Kreuzberger Independent-Filmproduktionsfirma von Freunden von mir vor Augen, deren Mitarbeiter unter körperlicher und finanzieller Selbstaufopferung täglich am Rande der Insolvenz ums Überleben kämpfen. Wenn ich denen erzähle, dass sie jetzt einen von ihnen dafür abstellen müssen, der sich um das Verzeichnis von Verarbeitungstätigkeiten, um geeignete Garantien für Drittstaatsübermittlungen und um technisch-organisatorische Maßnahmen zur Beantwortung etwaiger Auskunftsbegehren betroffener Personen kümmern muss, zeigen die mir – zu Recht – einen Vogel.