Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

zur

Anwendung der DS-GVO

November 2019

Inhalt

Einleitender Überblick

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) hat den folgenden Bericht über die Erfahrungen bei der Anwendung der DS-GVO erarbeitet und auf der 98. DSK am 06. November 2019 verabschiedet. Die DSK möchte damit die Erfahrungen der in ihr vertretenen deutschen Aufsichtsbehörden aus der praktischen Anwendung seit Geltungsbeginn der DS-GVO in den Evaluierungsprozess nach Art. 97 DS-GVO einbringen und daran anknüpfend in einigen Punkten auch Vorschläge für Verbesserungen unterbreiten, um einen optimalen Vollzug der DS-GVO zu gewährleisten.

Nach einem Jahr der Geltung der DS-GVO zieht die Europäische Kommission im Juli 2019 zu Recht eine positive Bilanz. Die DS-GVO habe die EU-Bürger zunehmend auf die Datenschutzbestimmungen und ihre Rechte aufmerksam gemacht, die Unternehmen passen ihre Praktiken an, sie erhöhen die Sicherheit ihrer Daten und entwickeln den Datenschutz als Wettbewerbsvorteil. Die Verordnung habe den nationalen Datenschutzbehörden mehr Befugnisse zur Durchsetzung der Vorschriften gegeben. Im ersten Jahr haben die nationalen Datenschutzbehörden diese neuen Befugnisse bei Bedarf wirksam genutzt, sie arbeiten im Rahmen des Kooperationsmechanismus enger zusammen.

Die DSK teilt die Auffassung, dass sich die DS-GVO mit ihrem Regelungskonzept und ihren Zielen im Wesentlichen bewährt. Die Ziele des verbesserten Grundrechtsschutzes und der Schaffung eines einheitlichen digitalen Binnenmarktes erscheinen durch die DS-GVO vorangebracht und auch tatsächlich erreichbar.

Als ein zentraler Aspekt der gesellschaftlichen Wahrnehmung und als Motor zur Entwicklung eines breitangelegten datenschutzrechtlichen Bewusstseins erwies sich, dass bei Verstößen gegen Datenschutznormen erstmals empfindliche Geldbußen drohen. Behörden und Betriebe stellen sich den Anforderungen. Sie agieren aber teilweise unsicher, Umsetzungsdefizite sind zu beobachten. Die Vorgaben an die Verantwortlichen sind vielfältig (die DS-GVO selbst, die Erwägungsgründe, Guidelines), sodass ein umfassendes Datenschutzmanagement des Verantwortlichen geboten ist. Dazu bedarf es einer Interpretation der Vorgaben, die unzählige Datenschutzberater anbieten. Der Bedarf, Orientierung durch die Aufsichtsbehörden zu erhalten ist noch immer sehr hoch. Dieser erhöhten Nachfrage begegneten die Aufsichtsbehörden mit einer intensiven Beratungstätigkeit, deren Kern darin besteht aus einer gestiegenen Anzahl von Rechts- und Informationsquellen einen roten Faden zu wirken, der es erlaubt, den Verantwortlichen pragmatische Handlungsempfehlungen zu geben. Die so gestiegene Akzeptanz des Datenschutzrechts und der Arbeit der Aufsichtsbehörden muss nunmehr erhalten und ausgebaut werden.

In dieser Hinsicht sind die durch die enorm gestiegene Anzahl von Beschwerden, durch aufwändige grenzüberschreitende Zusammenarbeit (IMI) und intensivierte Beratung gestiegenen Anforderungen an die Aufsichtsbehörden teilweise nicht mit auskömmlicher Aufstockung an Personal und Sachmitteln begleitet worden. Gemäß Art. 52 Abs. 4 DS-GVO hat jeder Mitgliedstaat sicherzustellen, dass seine Aufsichtsbehörde mit den Ressourcen, „die sie benötigt“, ausgestattet wird.

Dies hat u. a. zur Folge, dass von einigen Aufsichtsbehörden anlasslose Kontrollen nicht im erforderlichen Maße durchgeführt werden können, so dass Verantwortliche ein Kontrolldefizit erkennen und in ihren Bemühungen zur Schaffung datenschutzkonformer Zustände nachlassen.

Neben den gesetzlich für die Evaluierung der DS-GVO durch die Kommission festgelegten Themen des Art. 97 Abs. 2 DS-GVO wurde der Fokus des vorliegenden Berichts auf etwaigen Änderungsbedarf aufgrund der Anwendungs-Erfahrungen im ersten Geltungsjahr der DS-GVO gelegt. Dies sowohl bezogen auf bestehende Vorschriften als auch auf die möglicherweise notwendige Schaffung weiterer Regelungen. Auch die Erwägungsgründe wurden in die Überlegungen miteinbezogen.

Die Frage der Befassung mit etwaigen Problemen bei der Umsetzung der DS-GVO in Bundes- und Landesrecht wurde nicht in den Bericht miteinbezogen. Soweit einzelne nationale Umsetzungsnormen problematisch oder kritikwürdig erscheinen, kann sich hieraus allerdings auch ein Änderungsbedarf an Öffnungsklauseln der DS-GVO ergeben.

Grundsätzlich nicht berücksichtigt oder auf essentielle Punkte reduziert wurden außerdem Klarstellungs-, Auslegungs-, Definitions- und Übersetzungsprobleme. Auch strittige Punkte, welche sich bereits im Gesetzgebungsverfahren abgezeichnet und bis heute als in der Anwendung problematisch erwiesen haben, wurden weitestgehend ausgeklammert.

Im Ergebnis haben sich im Zuge der Anwendung der DS-GVO bisher folgende Schwerpunktthemen herausgestellt:

1. Alltagserleichterung & Praxistauglichkeit
2. Datenpannenmeldungen
3. Zweckbindung
4. data protection by design
5. Befugnisse der Aufsichtsbehörden und Sanktionspraxis
6. Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz
7. Direktwerbung
8. Profiling
9. Akkreditierung

Bei den **Informations- und Transparenzpflichten** nach Art. 13 und 14 DS-GVO haben sich in der Praxis Umsetzungsprobleme gezeigt, z. B. bei telefonischer Datenerhebung. Hier geht es insbesondere um die Frage, ob zunächst eine allgemeinere Information an zentraler Stelle ausreicht und konkrete Informationen nur auf Verlangen nachgereicht werden können. Auch Umfang und Inhalt der Informationspflichten könnten möglicherweise praktikabler und bürgerfreundlicher definiert werden. In der Praxis stellt sich teilweise die Frage nach der **Alltagstauglichkeit** der Regelungen der DS-GVO. Möglichkeiten zur erleichterten Anwendung der Informationspflichten, die Pflicht zur Meldung von Datenschutzbeauftragten an die Aufsichtsbehörden sowie das Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO wurden in den Fokus genommen.

Eine allgemein umgreifende Sorge vor den Sanktionsmöglichkeiten der DS-GVO führt nach der Erfahrung der Aufsichtsbehörden dazu, dass viele **Datenpannen** gemeldet werden, welche

tatsächlich gar keine Datenpannen sind oder deren Risiken schon längst beseitigt wurden. Daher waren exorbitante Steigerungsraten bei den Meldungen von Datenpannen zu verzeichnen.

Im Bereich der **Zweckbindung** haben sich in der Praxis vor allem Fragen im Hinblick auf die Rechtsgrundlage und die Voraussetzungen der Weiterverwendung der personenbezogenen Daten bei der Zweckänderung ergeben.

Data protection by design findet in der Praxis kaum Resonanz, da der Anwendungsbereich der DS-GVO Hersteller gerade nicht erfasst. Die DS-GVO stellt mit data protection by design / by default aber Grundsätze auf, die sich in der Sache an Hersteller richten, nimmt diesen aber nicht als Verantwortlichen in die Pflicht. Daher wird die Frage aufgeworfen, ob auch Hersteller, Lieferanten, Importeure und Verkäufer in die Pflicht genommen werden sollten, so wie es im Produkthaftungsrecht bereits der Fall ist.

Im Schwerpunktthema „**Befugnisse der Aufsichtsbehörden und Sanktionspraxis“** haben sich insbesondere Fragen nach dem Begriff des „Verarbeitungsvorgangs“ aus Art. 58 Abs. 2 lit. b DS-GVO sowie der Zusammenarbeit und des Auskunftsrechts der Aufsichtsbehörden im Bußgeldverfahren als besonders dringlich erwiesen. In einem weiteren in Art. 97 Abs. 2 lit. b DS-GVO aufgeführten Schwerpunkt werden die Erfahrungen der Aufsichtsbehörden mit den Themen „**Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz“** dargestellt.

Bei der **Direktwerbung** stellt sich in unterschiedlichen Konstellationen die Frage der Zulässigkeit, welche durch die Schaffung einer spezifischen Rechtsgrundlage gelöst werden könnte.

Als eine der zentralen datenschutzpolitischen Herausforderungen unserer Zeit wird das **Profiling** angesehen**.** Trotz vorhandener Begriffsdefinition wird der Prozess der Profilbildung als solcher von den meisten Normen der DS-GVO, etwa zur automatisierten Entscheidungsfindung, nicht erfasst, sodass eine Beurteilung meist nur nach den allgemeinen Tatbeständen des Art. 6 DS-GVO erfolgt. Die DSK fordert eine Verschärfung des geltenden Rechtsrahmens, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen.

Beim Schwerpunkt **Akkreditierung** könnte durch eine Klarstellung in der DS-GVO eine erhebliche nationale Zuständigkeitsfrage geklärt und die Aufsicht durch die deutschen Datenschutzaufsichtsbehörden sichergestellt werden.

In einer kurzen Liste weiterer Änderungsvorschläge sind konkrete Textänderungen samt Kurzbegründung aufgeführt, welche keinem Schwerpunktthema zuzuordnen sind, aber weitere Erleichterungen in der Anwendung der DS-GVO ermöglichen würden.

Zum aktuell vorherrschenden Thema in der wissenschaftlichen Auseinandersetzung – der Frage des Datenschutzes im Bereich der **Künstlichen Intelligenz** und automatisierten Entscheidungsverfahren – übersendet die DSK außerdem ihre „Hambacher Erklärung zur Künstlichen Intelligenz - Sieben datenschutzrechtliche Anforderungen“ vom 3. April 2019 im Anhang zur Kenntnis. Wenngleich die enthaltenen Forderungen sich auf zukünftige Fall- und Normkonstellationen beziehen, halten die deutschen Datenschutzaufsichtsbehörden die Beachtung dieser Grundsätze in den zukünftigen Evaluierungsprozessen für unerlässlich.

Schwerpunktthema Nr. 1 – Alltagserleichterung & Praxistauglichkeit

Bei der Beratung, Fallbearbeitung sowie dem Austausch mit Verantwortlichen ist den deutschen Datenschutzaufsichtsbehörden häufig Unverständnis für die Regelungen beziehungsweise den Umfang der Informationspflichten, des Verzeichnisses der Verarbeitungstätigkeiten sowie der Notwendigkeit von Datenschutzfolgenabschätzungen entgegengeschlagen. Vor allem kleine und mittlere Unternehmen (KMU) sowie nicht-gewerbliche Vereine fühlen sich in Deutschland durch die Vorgaben der DS-GVO übermäßig belastet und fordern Ausnahmeregelungen.

I. Informationspflichten

1. Problemaufriss

Die in Art. 13 und 14 DS-GVO geregelten Informations- und Transparenzpflichten sind ein Kernstück der Datenschutz-Grundverordnung. Die deutschen Aufsichtsbehörden erachten das u. a. in Art. 12 Abs. 1 DS-GVO ausgedrückte Anliegen, die betroffene Person in verständlicher und angemessener Form über ihre Datenschutzrechte zu informieren, für eine der wesentlichen Neuerungen durch die DS-GVO.

Teilweise wurde an deutsche Aufsichtsbehörden die Befürchtung herangetragen, die Erfüllung der Informationspflichten sei für Verantwortliche, wie z. B. Vereine und KMU möglicherweise zu aufwändig. Jedoch können auch kleine Einrichtungen Datenverarbeitungen vornehmen, die tiefgreifende Auswirkungen auf die Betroffenen haben.

Einige Verantwortliche haben außerdem gegenüber deutschen Aufsichtsbehörden Probleme adressiert, die bei der Erfüllung der Informationspflichten in bestimmten Kontexten auftreten, wie z. B. bei telefonischer Terminabsprache oder telefonischem Vertragsschluss und der damit verbundenen Datenerhebung.

Als Lösungsansatz wird zum Teil die Einführung einer an Art. 30 Abs. 5 DS-GVO angelehnten Ausnahme für Vereine und KMU mit unter 250 Mitarbeitern vorgeschlagen. Ein weiterer, am Risiko für die Betroffenen orientierter Lösungsansatz ist eine Reduzierung der Informationspflicht in Fällen, in denen die Datenverarbeitung sich in einem sehr engen und für die Betroffenen erwartbaren Rahmen hält.

2. Bewertung

Die Aufsichtsbehörden befürworten grundsätzlich einzelne Praxis-Erleichterungen, warnen aber vor generellen Ausnahmen von Verantwortlichen-Pflichten.

Aus den Erfahrungen der Aufsichtsbehörden in der Beratung von Unternehmen, deren Datenverarbeitung hauptsächlich im Rahmen von Kundenbeziehungen stattfindet, ergibt sich für gewisse Fallgestaltungen ein Bedarf an Erleichterungen bei den Informationspflichten. In der Bewertung kann zwischen einer digitalen und einer nicht digitalen Umgebung unterschieden werden.

In einer digitalen Umgebung sind die Informationspflichten regelmäßig gut erfüllbar. Gemäß ErwG 58 Satz 2 DS-GVO können die Informationen grundsätzlich in elektronischer Form zum Zeitpunkt der Erhebung bereitgestellt werden. Sofern der Verantwortliche eine Webseite betreibt, kann von ihm erwartet werden, die erforderlichen Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ anzubieten.

In bestimmten nicht digitalen Sachverhalten führt jedoch das Erfordernis der Information zum Zeitpunkt der Erhebung gemäß Art. 13 DS-GVO zu praktischen Zweifelsfragen. Vor allem bei mündlichen oder telefonischen Kontakten im geschäftlichen Bereich ist es lebensfremd zu erwarten, dass der Verantwortliche, wenn er eine Bestellung aufnimmt, eine Visitenkarte entgegennimmt oder einen Termin notiert, umfassende Informationen gemäß Art. 13 Abs. 1 und 2 DS-GVO erteilt, also die Rechtsgrundlage benennt, über die zuständige Datenschutzaufsichtsbehörde oder über Auskunfts-, Beschwerde- und sonstige Betroffenenrechte und anderes mehr informiert. Eine solche Information würde auch häufig auf das Unverständnis der Betroffenen stoßen und von diesen als störend empfunden werden.

Art. 13 Abs. 4 DS-GVO schließt die Informationspflichten zwar praxisgerecht aus, wenn und soweit die betroffene Person bereits über die Informationen verfügt; gerade im Rahmen von Unternehmen-Kunden-Beziehungen sind dem beauftragenden Kunden viele der informationspflichtigen Daten bereits bekannt. Nicht als bekannt vorausgesetzt werden kann grundsätzlich aber beispielsweise die Rechtsgrundlage der Datenverarbeitung (vgl. Art. 13 Abs. 1 lit. c DS-GVO). Diese ist jedoch nicht bei jeder Auftragserteilung, Terminvereinbarung etc. von Interesse. Betroffene klagten an dieser Stelle häufig über eine Informationsflut. Unter Berücksichtigung des risikobasierten Ansatzes bei der Beauftragung beispielsweise eines Handwerksbetriebs mit risikoarmer Datenverarbeitung würde es hier auch aus Sicht der Betroffenen genügen, wenn sie auf die Auffindbarkeit der Informationen hingewiesen werden.

In Einklang mit dem Working Paper der Art. 29-Gruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01), sprechen sich die deutschen Aufsichtsbehörden grundsätzlich dafür aus, die in Art. 13 DS-GVO genannten Informationspflichten in einem gestuften Verfahren erfüllen zu können. In geeigneten Fällen können die notwendigen Informationen beispielsweise auch mit der Übersendung einer Auftragsbestätigung, durch Aushang im Ladengeschäft oder auf ähnliche Weise erteilt werden. Von generellen Ausnahmen sollte allerdings abgesehen werden, um dem Ziel der Vorschrift nicht zuwider zu laufen.

3. Konkreter Änderungsvorschlag

Einfügen eines neuen Absatzes in Art. 13 DS-GVO:

Die Informationen nach den Absätzen 1 und 2 werden nur auf Verlangen der betroffenen Person mitgeteilt, soweit der Verantwortliche Datenverarbeitungen vornimmt, die der Betroffene nach den konkreten Umständen erwartet oder erwarten muss und

1. sowohl die Offenlegung von Daten gegenüber anderen Stellen als auch die Übermittlung in Drittländer ausgeschlossen sind,

2. keine Daten verarbeitet werden, die unter Art. 9 DS-GVO fallen,

3. die Daten nicht zu Zwecken der Direktwerbung verarbeitet werden und

4. weder Profiling noch automatisierte Entscheidungsfindungen stattfinden.

Die betroffene Person ist auf diese Möglichkeit hinzuweisen.

Außerdem sollte eine Ausnahme von den Informationspflichten zum Zeitpunkt der Erhebung für die Fälle vorgesehen werden, in denen Daten auf der Grundlage von Art. 6 Abs. 1 lit. d DS-GVO verarbeitet werden.

Begründung: Mit diesem Vorschlag soll der risikobasierten Betrachtung bei den Alltagserleichterungen Ausdruck verliehen werden.

II. Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO

Das Auskunftsrecht nach Art. 15 DS-GVO ist eines der grundlegenden Betroffenenrechte. Ohne Informationen über die Verarbeitung ihrer personenbezogenen Daten können die betroffenen Personen ihre weiteren Rechte, wie z. B. das Recht auf Berichtigung oder Löschung oder das Recht zur Beschwerde bei einer Aufsichtsbehörde nicht effektiv wahrnehmen.

Allerdings ist die Weite des Auskunftsanspruchs umstritten, insbesondere in welchem Umfang Art. 15 Abs. 3 DS-GVO ein „Recht auf Kopie“ einräumt. Ein solches könnte den betroffenen Personen ermöglichen, vom Verantwortlichen die Herausgabe sämtlicher verarbeiteter personenbezogener Daten im Originalkontext zu verlangen. In der Praxis verlangen betroffene Personen zum Teil ohne nähere Konkretisierung Herausgabe aller beim Verantwortlichen vorhandenen Dokumente, die personenbezogene Daten enthalten. Dieser Anspruch kann z. B. auf die Kopie ganzer Verfahrensakten durch eine Behörde gerichtet sein oder auf die Herausgabe des gesamten geschäftlichen E-Mail-Verkehrs eines ehemaligen Mitarbeiters durch ein Unternehmen.

Eine Klarstellung hinsichtlich des Umfangs des von Art. 15 Abs. 3 DS-GVO gewährten Rechts erscheint wünschenswert.

III. Pflicht zur Meldung von Datenschutzbeauftragten nach Art. 37 Abs. 7 DS-GVO

1. Problemaufriss

In Art. 37 Abs. 7 DS-GVO wird derzeit eine Pflicht konstatiert, der Aufsichtsbehörde Kontaktdaten von Datenschutzbeauftragten mitzuteilen. Die Verantwortlichen und Auftragsverarbeiter müssen gewährleisten, dass deren Meldung/en stets auf aktuellem Stand sind. Sie müssen diese nachhalten und ggf. gegenüber der zuständigen Aufsichtsbehörde korrigieren.

Durch die Pflicht, neben der Veröffentlichung der Kontaktdaten diese auch den Aufsichtsbehörden zu melden und beständig zu aktualisieren, entsteht bei den Verantwortlichen ein zusätzlicher Verwaltungsaufwand. Auf Seiten der Aufsichtsbehörden wird hierdurch eine nicht erforderliche Datenverarbeitung in Form einer Entgegennahme von Erst-, Änderungs- und Löschungsmeldungen ausgelöst. Teilweise wird Art. 37 Abs. 7 DS-GVO so interpretiert, dass die Aufsichtsbehörden ein Register der Datenschutzbeauftragten zu führen hätten (inkl. der Verpflichtung, eine Vollständigkeit sicherzustellen und Unstimmigkeiten von Amts wegen zu bereinigen). Eine Vollständigkeit und

Richtigkeit kann nur angestrebt, aber nie ganz erreicht werden. Im Hinblick auf die Tatsache, dass im nicht-öffentlichen Bereich ohne nähere Kenntnis der Organisation und des Geschäftsmodells des Verantwortlichen nicht über eine Benennungspflicht entschieden werden kann, sind dafür umfangreiche Datenerhebungen im Rahmen von Anhörungen erforderlich.

2. Bewertung

In der Praxis ist das Bereithalten von Kontaktdaten der oder des Datenschutzbeauftragten bei den Aufsichtsbehörden nicht erforderlich, da es eine Veröffentlichungspflicht gibt (Art. 37 Abs. 7 erster Satzteil DS-GVO). Bei Erstkontakten einer Aufsichtsbehörde mit Verantwortlichen könnten ggf. aktuelle Kontaktdaten der oder des Datenschutzbeauftragten mitgeteilt werden.

Zur Entlastung der Verantwortlichen bzw. Auftragsverarbeiter und der Datenschutzaufsichtsbehörden sollte diese Meldepflicht und die nicht erforderliche Datenverarbeitung, die zudem mangels Aktualität der Meldungen ungeeignet ist, entfallen.

3. Konkreter Änderungsvorschlag

In Art. 37 Abs. 7 DS-GVO sollte der letzte Halbsatz „und teilt diese Daten der Aufsichtsbehörde mit“ ersatzlos gestrichen werden.

Schwerpunktthema Nr. 2 – Datenpannenmeldungen

I. Art. 33 Abs. 1 DS-GVO

1. Problemaufriss

Nach Art. 33 Abs. 1 DS-GVO ist grundsätzlich jede Datenschutzverletzung der Aufsichtsbehörde zu melden. Eine Ausnahme besteht nur dann, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Verletzung des Schutzes personenbezogener Daten ist in Art. 4 Nr. 12 DS-GVO als Verletzung der Sicherheit legal definiert, die zu Vernichtung, Verlust, zur Veränderung oder unbefugten Offenbarung führt, und somit mit Art. 5 Abs. 1 lit. f) DS-GVO korrespondiert. Nach dem ErwG 85 DS-GVO kann die Verletzung des Schutzes einen physischen, materiellen oder immateriellen Schaden nach sich ziehen.

Da nach der vorherigen nationalen Rechtslage (§ 42a BDSG aF) eine Meldung nur bei bestimmten Datenarten erfolgen musste, hat sich die Zahl der Meldungen in der Bundesrepublik Deutschland deutlich erhöht. Für die Verantwortlichen besteht darüber hinaus die Schwierigkeit, einzuschätzen, in welchen Fällen kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Häufig dürfte dieses Risiko von Faktoren abhängen, die dem Verantwortlichen nicht bekannt sind. Darüber hinaus melden viele Verantwortliche vermeintliche Verstöße aus Furcht vor hohen Bußgeldern, ohne dass sie eine Risikoabwägung vorgenommen haben. Die sehr weite Fassung des Abs. 1 („voraussichtlich kein Risiko“) führt somit dazu, dass in sehr vielen Trivial- und Bagatellfällen Meldungen erfolgen, die eine hohe Belastung für die Aufsichtsbehörden darstellen und letztlich den Blick auf wirklich relevante Fälle verstellen.

2. Bewertung

Ein Risiko für die Rechte und Freiheiten natürlicher Personen kann in der Regel nicht vollkommen ausgeschlossen werden. Die Meldepflicht sollte daher auf Fälle beschränkt werden, die voraussichtlich zu einem mehr als nur geringen Risiko für die Rechte und Freiheiten natürlicher Personen führen.

Darüber hinaus sollte Art. 33 Abs. 1 DS-GVO auf Fälle ausgeweitet werden, bei denen nicht bekannt ist, ob eine Verletzung des Schutzes personenbezogener Daten stattgefunden hat, diese aber zu vermuten ist. Häufig liegt eine Verletzung der Sicherheit von Daten vor, es ist aber nicht bekannt, ob dies zu einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DS-GVO geführt hat.

Beispiel: Eine Dump (eine Kopie) einer umfangreichen Kundendatenbank war über Monate ungesichert über das Web zugänglich, Logfiles, über die ein Zugriff ausgeschlossen werden kann, liegen aber nur für wenige Tage vor. Eine Verletzung im Sinne von Art. 4 Nr. 12 DS-GVO kann (je nach Auslegung des Begriffs „Offenlegen“) hier nicht positiv festgestellt werde.

Hier sollte, wenn die Verletzung des Schutzes personenbezogener Daten wahrscheinlich ist, eine Meldepflicht bestehen, sofern voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen gegeben ist.

3. Änderungsvorschlag

Art. 33 Abs. 1 Satz 1 und 2 DS-GVO neu, der bisherige Satz 2 wird zu Satz 3:

Im Falle einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich nicht nur zu geringen Risiken für die Rechte und Freiheiten natürlicher Personen führt, meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Art. 55 zuständigen Aufsichtsbehörde. Darüber hinaus meldet der Verantwortliche einen Verstoß gegen die Anforderungen an die Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 DS-GVO, die wahrscheinlich zur Verletzung des Schutzes personenbezogener Daten geführt hat oder führen wird, unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung der Sicherheit bekannt wurde, sofern im Fall der Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht.

Schwerpunktthema Nr. 3 – Zweckbindung

1. Problemaufriss

Das Prinzip der Zweckbindung ist ein tragendes Prinzip des Datenschutzrechts. Es ist für die betroffenen Personen von praktisch sehr hoher Bedeutung, ob Daten, die sie einem Verantwortlichen zu bestimmten Zwecken preisgegeben haben, für andere Zwecke Verwendung finden dürfen. Die DS-GVO stellt daher besondere Voraussetzungen für die Weiterverarbeitung zu anderen Zwecken auf und sieht bei erlaubten zweckändernden Verarbeitungen eine Informationspflicht des Verantwortlichen vor.

Bei Anwendung des Art. 6 Abs. 4 DS-GVO gibt es Uneinigkeit darüber, ob für die zweckändernde Verarbeitung, die die Voraussetzungen des Art. 6 Abs. 4 DS-GVO an die Vereinbarkeit der Zwecke erfüllt, eine eigene Rechtsgrundlage erforderlich ist. Verantwortliche berufen sich z. B. bei der Weiterverwendung von Daten, die nach dem Gesetz, das ihnen die Datenverarbeitung erlaubt, streng zweckgebunden sind, darauf, dass nach ErwG 50 S. 2 DS-GVO für die zweckändernde Weiterverarbeitung keine eigene Rechtsgrundlage erforderlich sei, wenn der neue Zweck mit dem alten vereinbar ist. Demgegenüber haben jedoch betroffene Personen, die z. B. Daten gegenüber einem Verantwortlichen ohne rechtliche Verpflichtung preisgegeben haben, ein großes Interesse daran, auch vor einer Weiterverwendung zu einem neuen Zweck erneut über die Preisgabe der Daten entscheiden zu können. Deutsche Aufsichtsbehörden haben in derartigen Konflikten unter Berufung auf Art. 5 Abs. 1 lit. a in Verbindung mit Art. 6 Abs. 1 DS-GVO sowie auf ErwG 50 S. 8 DS-GVO gefordert, dass auch die zweckändernde Datenverarbeitung einer Rechtsgrundlage bedarf.

Abgesehen von dieser Frage hat sich in der Praxis die Privilegierung von Wissenschaft und Forschung in Art. 5 Abs. 1 lit. b i.V.m. Art. 6 Abs. 4 DS-GVO als zu weitgehend erwiesen.

2. Bewertung

Nach Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1 DS-GVO muss jede Datenverarbeitung mindestens eine der in Art. 6 Abs. 1 DS-GVO genannten Bedingungen erfüllen, um rechtmäßig zu sein. Rechtmäßigkeit (Art. 5 Abs. 1 lit. a DS-GVO) und Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO) sind zwei unterschiedliche, nebeneinander stehende Prinzipien der Datenverarbeitung. Die Vorschrift des Art. 6 Abs. 4 DS-GVO betrifft das Prinzip der Zweckbindung. Hätte im Rahmen dieser Vorschrift eine Ausnahme von dem Erfordernis einer Rechtsgrundlage gemacht werden sollen, so hätte dies angesichts der Bedeutung und Konsequenzen einer solchen Ausnahme ausdrücklich im Verordnungstext geregelt werden müssen.

Art. 6 Abs. 4 DS-GVO spricht nur von der Vereinbarkeit der Zwecke. Sein Satz 1 sagt aus, dass bei zweckändernden Verarbeitungen, die nicht auf der Rechtsgrundlage Art. 6 Abs. 1 lit. a DS-GVO oder auf bestimmten Rechtsvorschriften der Union oder Mitgliedstaaten beruhen, die Vereinbarkeit der Zwecke geprüft werden muss. Nach dem Wortlaut bedeutet das nicht, dass bei diesen anderen zweckändernden Verarbeitungen die Prüfung der Vereinbarkeit des Zwecks die Rechtsgrundlage ersetzt, sondern, dass bei zweckändernden Verarbeitungen, die auf anderen Rechtsgrundlagen beruhen, eine Prüfung der Vereinbarkeit der Zwecke erfolgen muss. Die Regelung impliziert also gerade, dass alle zweckändernden Verarbeitungen auf einer Rechtsgrundlage beruhen müssen.

Insofern irritiert die Aussage in Satz 2 des ErwG 50 DS-GVO, in dem es heißt, es sei bei Vereinbarkeit der Zwecke „keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten“.

Auch wenn Satz 8 des gleichen ErwG konstatiert, dass in jedem Fall die in der Verordnung niedergelegten Grundsätze anzuwenden sind, kann dies die Irritation nicht ganz beseitigen, da der Widerspruch zwischen dem nur auf die Rechtsgrundlage bezogenen Satz 2 und dem auf alle Grundsätze der DS-GVO bezogenen Satz 8 des ErwG 50 DS-GVO bestehen bleibt. Zum Teil wird der Verbleib des Satzes 2 in ErwG 50 nach den Trilogverhandlungen als Redaktionsversehen angesehen. In der Praxis führt er zu großen Schwierigkeiten bei der Durchsetzung der Rechtmäßigkeitsanforderungen an zweckändernde Datenverarbeitung und sollte daher gestrichen werden.

3. Änderungsvorschläge

ErwG 50 Satz 2 DS-GVO wird gestrichen.

Klarstellung in Art. 6 Abs. 4 DS-GVO: Weiterverarbeitungen auf Grundlage dieses Absatzes werden auf solche durch denselben Verantwortlichen beschränkt.

Schwerpunktthema Nr. 4 – data protection by design

1. Problemaufriss

Es sollten auch Hersteller, Lieferanten, Importeure, Verkäufer usw. in die Pflicht genommen werden, so wie dies im Produkthaftungsrecht (ProdHaftG bzw. RL 85/374/EWG) bereits der Fall ist.

Beim Begriff „Datenschutz durch Technikgestaltung“ (data protection by design), der in Art. 25 Abs. 1 DS-GVO für den Verantwortlichen vorgeschrieben ist, stellt sich in der Praxis der Adressatenkreis als nicht weitreichend genug heraus.

Verantwortliche entwickeln in der Regel nicht selbst Hard- und Software. Sie sind weitgehend auf Hardware und Standardbetriebssysteme und -anwendungssoftware angewiesen. Auf Anbieterseite bestehen oft Mono- oder Oligopole, sodass Produkte und Einsatzbedingungen von der Anbieterseite diktiert werden können.

Die DS-GVO stellt mit „data protection by design / data protection by default“ Grundsätze auf, die sich an Hersteller richten, nimmt Hersteller aber nicht als solche in die Pflicht. Die Forderung nach „data protection by design / data protection by default“ läuft, wenn sie ausschließlich an die Verantwortlichen gerichtet wird, häufig ins Leere.

Die DS-GVO sollte daher auch die Hersteller von Software zur Einhaltung dieses datenschutzfördernden Designprinzips verpflichten. In der Praxis trifft dies insb. auf Hersteller von komplexer Software wie z. B. Betriebssystemen, Datenbankmanagementsystemen, Standard-Office-Paketen oder sehr speziellen Fachanwendungen zu.

Hierzu zwei Beispiele:

1. Betriebssysteme

Verantwortliche, die Server, Desktop-Computer, Notebooks, Tablets, Smartphones oder ähnliche Geräte betreiben, müssen eines der wenigen am Markt erhältlichen Betriebssysteme, die auf der jeweiligen Hardware laufen, einsetzen. In der Regel sind diese schon vorinstalliert. Nach derzeitiger Rechtslage ist es die Pflicht dieser Verantwortlichen, etwaige datenschutzrechtlich relevante Schwachstellen, Fehlkonfigurationen, aus ihrer Sicht unerwünschte Funktionen etc. zu finden und abzustellen. Den Hersteller trifft keine Pflicht, seine Produkte ohne diese Fehler auszuliefern.

2. Haustür-Schließzylinder mit App

Es gibt Schließsysteme für Haustüren, die ohne physischen Schlüssel auskommen. Der Berechtigte identifiziert sich mit seinem Smartphone, auf dem eine passende App läuft. Zwischen der App und dem (in einem Drittland ohne angemessenes Datenschutz-Niveau befindlichen) Hersteller findet Datenverkehr statt.

a) Setzt ein Unternehmen derartige Systeme ein, ist es selbst Verantwortlicher und muss Datenverarbeitungen verantworten, die es nicht durchschauen kann. Der Hersteller ist nicht effektiv greifbar.

b) Setzt eine Privatperson im Rahmen privat-familiärer Tätigkeit derartige Systeme ein, ist ein Verantwortlicher im Sinne der DS-GVO schon nicht vorhanden. Die Pflichten der DS-GVO treffen

niemanden, gehen also ins Leere. Würde man hier den Importeur, Händler o.ä. in die Verantwortung nehmen können, so wäre für „den Datenschutz“ viel gewonnen.

2. Bewertung

Die bisherige Rechtslage widerspricht dem Ansatz von „data protection by design“ bzw. „by default“.

Entgegen ErwG 78 S. 4 DS-GVO werden Hersteller in keiner Weise ermutigt, „das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen“.

Damit bestehen nicht nur erhebliche Lücken im Bereich des Schutzes personenbezogener Daten (und anderer Daten, vgl. Richtlinie (EU) 2016/943), sondern es kommt zu einer Potenzierung von technischem und bürokratischem Aufwand bei dem Versuch, dezentral Mängel zu beseitigen, die zentral verursacht werden. Dies belastet alle Verantwortlichen und Auftragsverarbeiter, wobei KMU überproportional belastet werden.

Die Rechtslage widerspricht so auch allgemeinem Recht. Nach dem über die RL 85/374/EWG harmonisierten Produkthaftungsrecht haften Hersteller für Schäden, die durch ihre Produkte entstehen. Neben Herstellern haften auch Importeure, Lieferanten, etc. Es gilt, diese bereits harmonisierte Rechtslage in den Bereich des Schutzes personenbezogener Daten zu übertragen.

Daher sollte Ziel sein, auch für datenschutzrechtlich relevante Produkte stärker auch die Hersteller in die Verantwortung zu nehmen.

3. Änderungsvorschläge

Durch die folgenden Änderungsvorschläge (unterstrichen dargestellt) würde die DS-GVO Pflichten für Hersteller usw. aufstellen, deren Durchsetzung aber dem Verbraucherschutz- und ggf. auch dem Wettbewerbsrecht überlassen.

Art. 4 - Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck…

27. „Hersteller“ den Hersteller im Sinne von Art. 3 der Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte. Nr. 16 Buchstabe a gilt entsprechend. Soweit er über Zwecke und Mittel der Datenverarbeitung entscheidet, ist der Hersteller auch Verantwortlicher im Sinne der Nr. 7.

KAPITEL IV - Verantwortlicher und Auftragsverarbeiter, Hersteller
Abschnitt 1 - Allgemeine Pflichten

Art. 24 - Verantwortung des für die Verarbeitung Verantwortlichen und des Herstellers

(4) Der Hersteller entwickelt und gestaltet seine Produkte, Dienste und Anwendungen unter Berücksichtigung des Rechts auf Datenschutz und des Standes der Technik so, dass er sicherstellt, dass Verantwortliche und Auftragsverarbeiter in der Lage sind, ihren Datenschutzpflichten

nachzukommen, ohne unzumutbare Änderungen an diesen Produkten, Diensten und Anwendungen vornehmen zu müssen. Er unterstützt sie bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30), bei der Meldung einer Verletzung des Schutzes personenbezogener Daten (Art. 33) und bei der Benachrichtigung betroffener Personen (Art. 34), indem er ihnen auf Anfrage alle dazu notwendigen Informationen bereitstellt.

Art. 79 - Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche, Auftragsverarbeiter oder Hersteller

(1) Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Art. 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

(2) Für Klagen gegen einen Verantwortlichen, gegen einen Auftragsverarbeiter oder gegen einen Hersteller sind die Gerichte des Mitgliedstaats zuständig, in dem der Hersteller, Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen, dem Auftragsverarbeiter oder dem Hersteller um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

Art. 82 - Haftung und Recht auf Schadenersatz

(7) Beruht der Schaden ganz oder teilweise auf Handlungen oder Versäumnissen des Herstellers, so haftet dieser gegenüber der betroffenen Person neben dem Verantwortlichen oder Auftragsverarbeiter. Er haftet auch gegenüber dem Verantwortlichen und dem Auftragsverarbeiter.

Schwerpunktthema Nr. 5 – Befugnisse der Aufsichtsbehörden und Sanktionspraxis

I. Befugnisse

1. Problemaufriss

Die Worte „mit Verarbeitungsvorgängen“ in Art. 58 Abs. 2 lit. b DS-GVO führen zu Problemen bei der Anwendung der Vorschrift. Es gibt in der DS-GVO verschiedene Pflichten, die von einer konkreten Verarbeitung unabhängig sind, wie z. B. die Bestellung eines Datenschutzbeauftragten (Art. 37 DS-GVO) oder Vertreters (Art. 27 DS-GVO) oder die Pflicht zur Führung eines Verarbeitungsverzeichnisses (Art. 30 DS-GVO). Es ist deshalb für die Aufsichtsbehörden fraglich, auf welcher Rechtsgrundlage sie bei derartigen Verstößen eine Verwarnung aussprechen können.

2. Bewertung

Die Grundsätze, denen eine Verarbeitung entsprechen muss, sind in Art. 5 DS-GVO niedergelegt und in weiteren Vorschriften der DS-GVO genauer aufgeführt. Es gibt in der DS-GVO Pflichten, die von diesen Verarbeitungsgrundsätzen unabhängig sind. Zumindest für die Bestellung eines Datenschutzbeauftragten oder Vertreters oder für die Pflicht zur Führung eines Verarbeitungsverzeichnisses ist nicht ersichtlich, dass sie einen der in Art. 5 DS-GVO niedergelegten Grundsätze der Verarbeitung ausfüllen. Daher wird durch die Verletzung der genannten Pflichten die einzelne Verarbeitung nicht unzulässig. Es besteht aber ein praktischer Bedarf, auch bei derartigen Verstößen eine Verwarnung aussprechen zu können. Zur Vermeidung von Wertungswidersprüchen sollte diese Möglichkeit bei allen Verstößen gegen die Verordnung bestehen.

Zum Vergleich: Auch die Sanktionen in Art. 83 DS-GVO knüpfen nicht an Verarbeitungsvorgänge, sondern lediglich an „Verstöße gegen diese Verordnung“ (Abs. 1) bzw. „Verstöße gegen die folgenden Bestimmungen“ (Abs. 4, 5) an.

3. Änderungsvorschläge

Keine Beschränkung der Befugnisse nach Art. 58 Abs. 2 DS-GVO auf Verarbeitungsvorgänge.

Art. 58

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass ~~beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,~~ er voraussichtlich gegen diese Verordnung verstoßen wird,

b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er ~~mit Verarbeitungsvorgängen~~ gegen diese Verordnung verstoßen hat,

d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, Maßnahmen oder die Erfüllung von Pflichten gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,

II. Art. 83 Abs. 5 lit. e DS-GVO – Sanktionen, Tatbestand für Verstöße gegen Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 1 lit. a DS-GVO

1. Problemaufriss

Gemäß Art. 58 Abs. 1 lit. a DS-GVO kann der Verantwortliche / Auftragsverarbeiter von der Aufsichtsbehörde angewiesen werden, „alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind." Dieser behördliche Auskunftsanspruch verpflichtet den Adressaten, auf Anforderung der Behörde zuzuarbeiten.

Nach Art. 58 Abs. 1 lit. e DS-GVO hat die Aufsichtsbehörde darüber hinaus die Befugnis, „Zugang zu allen personenbezogenen Daten und Informationen zu erhalten, die zur Erfüllung ihrer Aufgabe notwendig sind." Das Zugangsrecht erlaubt der Aufsichtsbehörde, über die bereitgestellten Informationen hinaus in interne Unterlagen, Datenbanken und Verfahren Einsicht zu nehmen (z. B. Ehmann/ Selmayr, Datenschutzgrundverordnung Art. 58 RN 16). Nach dieser Abgrenzung muss die Nichtbereitstellung von Informationen oder die Auskunftsverweigerung des Adressaten unter Art. 58 Abs. 1 lit. a DS-GVO subsumiert werden.

Gemäß Art. 83 Abs. 5 lit. e DS-GVO kann nach dem Wortlaut nur das Nichtbefolgen einer Anweisung nach Art. 58 Abs. 2 DS-GVO oder die Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 DS-GVO mit einem Bußgeld geahndet werden. Demgegenüber können Verstöße gegen die Zusammenarbeitspflichten, z. B. die Auskunftsverweigerung nach Art. 83 Abs. 4 lit. a i. V. m. Art. 31 DS-GVO geahndet werden.

2. Bewertung

Diese Verortung der fehlenden Informationsbereitstellung oder der Auskunftsverweigerung ist unter den Aufsichtsbehörden umstritten. Zum einen wird Art. 31 DS-GVO von zumindest einem Teil der Kommentarliteratur so verstanden, dass die Zusammenarbeitsverpflichtung von einer Anfrage der Aufsichtsbehörde ausgelöst wird, welche keine Verwaltungsaktqualität haben muss, also eher in Voruntersuchungen zur Sachverhaltsermittlung stattfindet. Eine solche Sachverhaltsermittlung ist jedoch von einer förmlichen Geltendmachung des behördlichen Auskunftsanspruches nach Art. 58 Abs. 1 lit. a DS-GVO zu unterscheiden und in der Folge sind Verstöße gegen die Verpflichtungen auch unterschiedlich zu ahnden.

Zum anderen wird die Inkonsistenz des Auslegungsergebnisses beklagt, da Art. 83 Abs. 4 lit. a DS-GVO i. V. m. Art. 31 DS-GVO einen erheblich niedrigeren Bußgeldrahmen aufweist, als z. B. die Nichtgewährung des Zuganges nach Art. 83 Abs. 5 lit. e DS-GVO i.V.m. Art. 58 Abs. 1 DS-GVO.

Verstöße gegen Art. 58 Abs. 1 lit. a DS-GVO sollten daher wie die Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 lit. e oder f DS-GVO gleichmäßig geahndet werden. Daher ist im Rahmen des Art. 83 Abs. 5 lit. e DS-GVO ein Tatbestand für Verstöße gegen eine Anweisung nach Art. 58 Abs. 1 lit. a DS-GVO zu schaffen.

3. Änderungsvorschlag

Änderung des Art. 83 Abs. 5 lit. e DS-GVO:

Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Abs. 2,

Nichtbefolgung einer Anweisung, Informationen bereit zu stellen oder Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 Buchstaben a, e und f.

Schwerpunktthema Nr. 6 – Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz

I. Art. 46 Abs. 4 i. V. m. Art. 64 Abs. 2 DS-GVO

1. Problemaufriss

Es wird aus dem Gesetzestext nicht klar deutlich, ob bei jeder Verwaltungsvereinbarung, die als Grundlage für internationalen Datentransfer dienen soll und der zuständigen Aufsichtsbehörde gemäß Art. 46 Abs. 3 lit. b DS-GVO zur Genehmigung vorgelegt wird, ein Kohärenzverfahren durchgeführt werden muss. Art. 46 Abs. 4 DS-GVO sieht dies für alle Fälle des Absatzes 3 vor. Art. 64 Abs. 1 DS-GVO erwähnt in lit. e aber nur die Genehmigung von Vertragsklauseln nach Art. 46 Abs. 3 lit. a DS-GVO.

Hintergrund: Seine Stellungnahme zur ESMA/IOSCO Verwaltungsvereinbarung hat der EDSA gemäß Art. 64 Abs. 2 DS-GVO abgegeben. Ob dieses Verfahren in Zukunft für alle Verwaltungsvereinbarungen oder nur für multilaterale Vereinbarungen Anwendung finden soll, wird in der ITES und der COOPESG streitig diskutiert.

2. Bewertung

Es bedarf tatsächlich der Klarstellung, ob auch Verwaltungsvereinbarungen nach Art. 46 Abs. 3 lit. b DS-GVO dem Ausschuss vorgelegt werden müssen. Aus deutscher Sicht ist das der Fall. Allerdings soll hier das Kohärenzverfahren nach Art. 64 Abs. 2 DS-GVO angewendet werden, um dem Ausschuss die Möglichkeit zu geben, bei Verwaltungsvereinbarungen, die nicht die Voraussetzungen des Art. 64 Abs. 2 DS-GVO (Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat) erfüllen, den Antrag auf Stellungnahme abzulehnen.

3. Änderungsvorschlag

Neufassung des Artikels 46 Absatz 4 DS-GVO

(4) In Fällen gemäß Absatz 3 Buchstabe a wendet die Aufsichtsbehörde das Kohärenzverfahren nach Art. 64 Abs. 1 Satz 2 Buchstabe e an, in Fällen gemäß Absatz 3 Buchstabe b das Kohärenzverfahren nach Artikel 64 Absatz 2.“

II. Erfahrungen mit Anwendung und Wirkungsweise der Vorschriften zu Kapitel V und Kapitel VII

1. Problemaufriss

Als gemäß Art. 97 DS-GVO gesetztes Thema sind die Erfahrungen mit Anwendung und Wirkungsweise der Vorschriften zu Kapitel V und Kapitel VII zu behandeln. Konkret stellen sich hier u. a. die Fragen, ob längere Fristen erforderlich sind.

2. Bewertung

Die in der DS-GVO festgelegten Fristen konnten bisher nicht vollumfänglich in der Praxis getestet werden.

Nichtsdestotrotz wurde bereits bei den Anträgen auf Stellungnahme nach Art. 64 Abs. 2 DS-GVO festgestellt, dass eine sachgerechte Behandlung und Diskussion umfangreicherer Themen und schwieriger Einzelfälle durch die Fristen erschwert wird.

3. Änderungsvorschlag

Die Frist des Art. 64 Abs. 3 DS-GVO sollte von acht Wochen auf drei Monate und die Frist des Art. 66 Abs. 4 DS-GVO von zwei auf vier Wochen verlängert werden. Entsprechend müsste dann auch geprüft werden, ob die Geltungsdauer einstweiliger Maßnahmen (Art. 66 Abs. 1 DS-GVO) verlängert wird. Mindestens aber sollte im Kooperations- und Kohärenzverfahren eine Verlängerung aller Fristen um 50 % in Betracht gezogen werden.

III. Art. 64 Abs. 7 DS-GVO

1. Problemaufriss

Die DS-GVO schreibt in Art. 64 Abs. 7 DS-GVO bisher lediglich vor, dass die zuständige Aufsichtsbehörde dem EDSA aufgrund dessen Stellungnahme einen geänderten Beschlussentwurf zur Verfügung stellt (oder mitteilt, dass sie den Beschluss nicht ändern wird). Darauf ist aber keine weitere Rückmeldung des EDSA an die federführende Aufsichtsbehörde mehr vorgesehen.

Zuerst identifiziert wurde dieses Thema im Zusammenhang mit den Kohärenzverfahren zu DSFA-Listen (Art. 64 Abs. 1 lit. a DS-GVO). Vielen Anwendern dieser DSFA-Listen war nicht klar, ob diese nun verbindlichen Charakter haben, nachdem sie gemäß Art. 64 Abs. 7 DS-GVO an die Stellungnahme des EDSA angepasst wurden. Mittlerweile äußert es sich als großes Problem bei Kohärenzverfahren zu BCR (Binding Corporate Rules), da dort auch Externe (die antragstellenden Unternehmen) betroffen sind. Fällt also eine Stellungnahme des EDSA zunächst negativ aus bzw. werden dort Änderungsbedarfe aufgeführt und ändert das Unternehmen daraufhin seine BCR-Unterlagen (Teil des Genehmigungsentwurfs der federführenden Behörde), erhalten federführende Behörde und Unternehmen keine abschließende Rückmeldung mehr, ob damit den Bedenken des EDSA Genüge getan wurde und ob in der Folge der geänderte Beschlussentwurf verbindlich geworden ist.

Dies ist mittlerweile ein erheblicher Diskussionspunkt mit dem EDSA-Sekretariat. Daher wäre hier eine ergänzende Regelung in Art. 64 DS-GVO für einen vollständigen Abschluss von Kohärenzverfahren erforderlich.

2. Bewertung

Es scheint in der Tat eine Regelungslücke zu bestehen, welches Verfahren ein geänderter Beschlussentwurf nach sich zieht.

3. Änderungsvorschlag

Ergänzung eines zweiten Satzes in Art. 64 Abs. 7 DS-GVO:

Der Ausschuss gibt binnen vier Wochen eine Stellungnahme zu dem geänderten Beschlussentwurf ab.

Äußert sich der Ausschuss nicht binnen vier Wochen, so gilt dies als Zustimmung.

Schwerpunktthema Nr. 7 – Direktwerbung

1. Problemaufriss

Mit der DS-GVO sind konkrete Regelungen im nationalen Recht entfallen, die insbesondere Gewichtungen von Interessen vorgesehen haben. Die DS-GVO gibt nur im ErwG 47 DS-GVO einen Anhaltspunkt für die Abwägung: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden." In der Praxis stellen sich Fragen, die mit konkreteren Vorgaben des Gesetzgebers besser lösbar wären, z. B.:

Ist die Weitergabe von Kundendaten an Dritte zu Werbezwecken zulässig?

Ist es zulässig, listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen-, oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken (keine Telefon- und Faxnummern, E-Mail-Adresse, Geburtsdatum) für Werbezwecke vorzuhalten und zu nutzen?

Ist die Werbung für wohltätige Zwecke im Ergebnis anders zu bewerten als für wirtschaftliche Zwecke?

2. Bewertung

Direktwerbung betrifft viele Wirtschaftsbereiche und viele betroffene Personen.

Die Traditionen in den Mitgliedstaaten sind unterschiedlich, so dass auch die Erwartungen der Betroffenen, die bei der Interessenabwägung zu berücksichtigen sind, unterschiedlich sein können. Für eine europaweit einheitliche Anwendung sollte der Gesetzgeber deshalb detailliertere Regelungen schaffen.

3. Änderungsvorschlag

Für Direktwerbung sollte der europäische Gesetzgeber in der DS-GVO gesetzliche Vorgaben schaffen, die zumindest die grundsätzliche Gewichtung von Interessen vorsehen.

Schwerpunktthema Nr. 8 – Profiling

1. Problemaufriss

Die Bildung von persönlichen Profilen und deren – kommerzielle und politische – Auswertung sind eine der zentralen datenschutzpolitischen Herausforderungen unserer Zeit. Die Werkzeuge der Datenverarbeitung ermöglichen das Anlegen, die Auswertung und Analyse ungeheurer Datenmengen aus verschiedensten Kontexten. Verbunden mit immer weiter verfeinerten Möglichkeiten des Einsatzes selbstlernender Mechanismen eröffnet dies vielfältige Möglichkeiten, Verhalten von Einzelnen (vermeintlich) vorherzusagen und ggf. zu steuern. Obwohl diese Entwicklung diverse datenschutzrechtliche Grundprinzipien herausfordert – z. B. das Gebot der Datenminimierung oder die Zweckbindung – bleibt die DS-GVO gerade in diesem Punkt vage und weitgehend auf dem Stand von 1995. Bei den Verhandlungen zur Schaffung der DS-GVO war es nicht gelungen, die Bildung von Profilen und das Scoring einer detaillierten modernen europäischen Regelung zuzuführen.

Die DS-GVO enthält zwar in Art. 4 Nr. 4 DS-GVO eine Definition des Profiling und der Begriff wird in verschiedenen Erwägungsgründen und Artikeln erwähnt (beispielsweise ErwG 60 DS-GVO, Art. 21, Art. 22, Art. 13 und 14 DS-GVO). Die Profilbildung als solche wird jedoch von den meisten dieser Normen nicht erfasst. Einschränkende Kernregelung ist vielmehr das Verbot der automatisierten Einzelentscheidung mit Erlaubnisvorbehalt (Art. 22 DS-GVO). Das Profiling an sich ist nach geltendem Recht daher vielfach nach den allgemeinen Tatbeständen des Art. 6 DS-GVO zu beurteilen. Beispielsweise wird Profilerstellung auf Grundlage von Internet- Kommunikationsinhalten und Metadaten u. a. für Werbezwecke von den Unternehmen oftmals nicht als automatisierte Entscheidung angesehen, mit der Folge, dass diese Profilbildung nicht vom grundsätzlichen Verbot des Art. 22 DS-GVO umfasst ist.

2. Bewertung

Die DSK ist der Auffassung, dass vor dem Hintergrund der dargestellten Probleme Änderungsbedarf an den Regelungen der DS-GVO zum Profiling besteht. Ziel der Neuregelungen sollte eine Verschärfung des geltenden Rechtsrahmens sein, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen. Die betroffenen Personen sollten von einem größeren Maß an Transparenz bezüglich der erstellten Profile profitieren und zugleich eine größere Kontrolle über die Verarbeitung ihrer Daten zur Profilbildung erhalten. Zu diesem Zweck sollte das Verbot der automatisierten Einzelentscheidung in Art. 22 DS-GVO um die Datenverarbeitung zu Zwecken der Profilbildung erweitert werden. Als Rechtsgrundlagen für das Profiling soll – neben einer spezialgesetzlichen Grundlage – allein eine Einwilligung oder ein Vertrag in Betracht kommen. Damit wird sichergestellt, dass ein Profiling nur stattfindet, wenn die betroffene Person sich dessen bewusst ist und damit einverstanden ist.

Die von der Art. 29-Gruppe beschlossenen und vom EDSA bestätigten „Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679“ geben zwar wichtige Hilfestellung für die datenschutzrechtliche Einordnung der Profilbildung in der Praxis. Sie können aber eine gesetzliche Regelung nicht ersetzen.

Schwerpunktthema Nr. 9 – Akkreditierung

1. Problemaufriss

In Deutschland gibt es eine Auseinandersetzung zwischen der deutschen nationalen Akkreditierungsstelle und den Aufsichtsbehörden über die Anwendung von Art. 41 DS-GVO. Die deutsche Akkreditierungsstelle vertritt die Auffassung, dass sie auch an Akkreditierungen nach Art. 41 DS-GVO zu beteiligen sei, während die deutschen Aufsichtsbehörden der Auffassung sind, dass die Akkreditierung im Sinne von Art. 41 DS-GVO ausschließlich von den Aufsichtsbehörden durchzuführen ist. Im Verlaufe der Auseinandersetzung hat die Deutsche Akkreditierungsstelle die Aufsichtsbehörden gebeten, sich für eine Klarstellung des Wortlauts einzusetzen.

2. Bewertung

Die deutsche nationale Akkreditierungsstelle schließt aus der Verordnung (EG) Nr. 765/2008, dass sie allgemein für Akkreditierungen in Deutschland zuständig ist. Daher geht sie bisher davon aus, dass auch für die Akkreditierung nach Art. 41 Abs. 1 DS-GVO ein ähnliches Verfahren wie nach Art. 43 Abs. 1 DS-GVO unter Beteiligung der Aufsichtsbehörden durchgeführt wird. Die deutschen Aufsichtsbehörden weisen demgegenüber darauf hin, dass Art. 41 Abs. 1 DS-GVO ausschließlich die Aufsichtsbehörden als akkreditierende Stelle benennt. Der Wortlaut des Art. 43 Abs. 1 Satz 2 DS-GVO unterscheidet sich wesentlich von dem des Art. 41 Abs. 1 DS-GVO. Auch sind im Hinblick auf die Akkreditierung nach Art. 41 Abs. 1 DS-GVO mit Ausnahme von Art. 57 Abs. 1 lit. p DS-GVO (Abfassen und Veröffentlichen der Kriterien) keine konkreten Aussagen in der – im Übrigen im Vergleich zur VO 765/2008 spezielleren – DS-GVO getroffen worden. Nach Auffassung der deutschen Aufsichtsbehörden ist vielmehr davon auszugehen, dass das Wort „Akkreditierung“ in Art. 41 DS-GVO nicht gleichbedeutend mit Akkreditierung im Sinne von Art. 43 DS-GVO und der Verordnung Nr. 765/2008 zu verstehen ist, sondern eine andere Form der „Anerkennung“ darstellt, für die die Verordnung Nr. 765/2008 nicht anwendbar ist.

3. Änderungsvorschläge

In Art. 41 Abs. 1 DS-GVO soll zur Klarstellung vor den Worten „von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde“ das Wort „ausschließlich“ eingefügt werden.

Zusätzlich soll rein klarstellend das Wort „akkreditiert“ gestrichen und stattdessen das Wort „anerkannt“ eingesetzt werden.

Liste weiterer Änderungsvorschläge

Betroffene Vorschrift der DS-GVO	Änderungsvorschlag mit Kurzbegründung
Art. 4	Eine Definition der Anonymisierung fehlt bisher in der DS-GVO. Sie wäre für die Praxis hilfreich**.** Sie sollte sich an den Vorgaben der „Opinion 05/2014“ zu Anonymisierungsverfahren orientieren.
Art. 13, 14	Die Kataloge der Absätze 2 in Art. 13 und 14 werden aneinander angepasst, indem die Information nach Art. 14 Abs. 2 lit. b DS-GVO auch in Art. 13 DS-GVO nicht in Ansatz 1, sondern in Abs. 2 aufgelistet wird.
Art. 18 Abs. 1	Recht auf Einschränkung der Verarbeitung: Über die unter Art. 18 Abs. 1 lit. a - d DS-GVO aufgezählten Gründe hinaus sollte das Recht auf Einschränkung der Verarbeitung auch in den Fällen bestehen, in denen die an sich gebotene Löschung unterbleibt, weil die Daten gemäß Art. 17 Abs.3 lit. b DS-GVO lediglich zur Einhaltung von Aufbewahrungsfristen vorgehalten werden müssen.
Art. 21 Abs. 2	Widerspruchsrecht bei Direktmarketing: Durch die Einfügung der Worte „neben dem Widerspruchsrecht nach Abs. 1“ sollte klargestellt werden, dass Abs. 2 kein Unterfall von Abs. 1 ist, sondern dass der Anwendungsbereich, anders als bei Abs. 1, auch dann eröffnet ist, wenn die Daten nicht auf der Grundlage von Art. 6 Abs. 1 lit. e und f DS-GVO verarbeitet werden.
Art. 24 Abs. 2	Der Wortlaut von Art. 24 Abs. 2 DS-GVO erscheint missverständlich. Er sollte der englischen Fassung wie folgt angeglichen werden: „Einführung“ statt „Anwendung“ und Datenschutz„regelwerke“ statt Datenschutz„vorkehrungen“.
Art. 27	In Art. 27 DS-GVO sollte eine Pflicht zur Veröffentlichung des Vertreters wie in Art. 37 Abs. 7 DS-GVO (Datenschutzbeauftragter) eingeführt werden, da in vielen Fällen unklar ist, ob der Verantwortliche/Auftragsverarbeiter seiner Bestellpflicht nachgekommen ist und wo der Vertreter seinen Sitz hat.
Art. 40 Abs. 4 , Art. 41 Abs.1 u. 4	Klarstellung durch Änderungen der genannten Regelungen, ob die Einrichtung einer akkreditierten Überwachungsstelle obligatorisch ist (entsprechend der verabschiedeten Leitlinien des EDSA mit Stand vom 12.02.2019) oder nur fakultativ.

Anhang: Hambacher Erklärung zur Künstlichen Intelligenz

Entschließung der 97. Konferenz
der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Hambacher Schloss

3. April 2019

Hambacher Erklärung zur Künstlichen Intelligenz

Sieben datenschutzrechtliche Anforderungen

Systeme der Künstlichen Intelligenz (KI) stellen eine substanzielle Herausforderung für Freiheit und Demokratie in unserer Rechtsordnung dar. Entwicklungen und Anwendungen von KI müssen in demokratisch-rechtsstaatlicher Weise den Grundrechten entsprechen. Nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden. Das gilt in besonderem Maße für den Einsatz von selbstlernenden Systemen, die massenhaft Daten verarbeiten und durch automatisierte Einzelentscheidungen in Rechte und Freiheiten Betroffener eingreifen. Die Wahrung der Grundrechte ist Aufgabe aller staatlichen Instanzen. Wesentliche Rahmenbedingungen für den Einsatz von KI sind vom Gesetzgeber vorzugeben und durch die Aufsichtsbehörden zu vollziehen. Nur wenn der Grundrechtsschutz und der Datenschutz mit dem Prozess der Digitalisierung Schritt halten, ist eine Zukunft möglich, in der am Ende Menschen und nicht Maschinen über Menschen entscheiden.

I. Künstliche Intelligenz und Datenschutz

„Künstliche Intelligenz“ (auch „KI“ oder „Artificial Intelligence“ – „AI“) wird derzeit intensiv diskutiert, da sie neue Wertschöpfung in vielen Bereichen von Wirtschaft und Gesellschaft verspricht. Die Bundesregierung hat eine KI-Strategie veröffentlicht, mit dem Ziel, Deutschland an die Weltspitze der Entwicklung von KI zu bringen. „AI made in Germany“ soll gleichzeitig dafür sorgen, dass auch bei weitreichendem Einsatz Künstlicher Intelligenz die Grundwerte und Freiheitsrechte, die in Deutschland und der EU gelten, weiterhin die prägende Rolle für unser Zusammenleben spielen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßen diesen Ansatz der grundrechtsverträglichen Gestaltung von KI ausdrücklich.

Eine allgemein anerkannte Definition des Begriffs der Künstlichen Intelligenz existiert bisher nicht. Nach dem Verständnis der Bundesregierung geht es bei KI darum, „technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte

Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu „lernen“ […].“[1]

KI-Systeme werden beispielsweise bereits in der Medizin unterstützend in Forschung und Therapie eingesetzt. Schon heute sind neuronale Netze in der Lage, automatisch komplexe Tumorstrukturen zu erkennen. KI-Systeme können auch genutzt werden, um Depressionserkrankungen anhand des Verhaltens in sozialen Netzwerken oder anhand der Stimmmodulation beim Bedienen von Sprachassistenten zu erkennen. In den Händen von Ärzten kann dieses Wissen dem Wohl der Erkrankten dienen. In den falschen Händen jedoch, kann es auch missbraucht werden.

Auch zur Bewertung von Bewerbungsunterlagen wurde bereits ein KI-System eingesetzt, mit dem Ziel, frei von menschlichen Vorurteilen zu entscheiden. Allerdings hatte das Unternehmen bislang überwiegend männliche Bewerber eingestellt und das KI-System mit deren erfolgreichen Bewerbungen trainiert. In der Folge bewertete das KI-System Frauen sehr viel schlechter, obwohl das Geschlecht nicht nur kein vorgegebenes Bewertungskriterium, sondern dem System sogar unbekannt war. Dies offenbart die Gefahr, dass in Trainingsdaten abgebildete Diskriminierungen nicht beseitigt, sondern verfestigt werden.

Anhand dieser Beispiele wird deutlich, dass mit KI-Systemen häufig personenbezogene Daten verarbeitet werden und diese Verarbeitung Risiken für die Rechte und Freiheiten von Menschen birgt. Sie zeigen auch, wie wichtig es ist, Entwicklung und Einsatz von KI-Systemen politisch, gesellschaftlich und rechtlich zu begleiten. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder verstehen die folgenden Anforderungen als einen konstruktiven Beitrag zu diesem zentralen gesellschaftspolitischen Projekt.

II. Datenschutzrechtliche Anforderungen an Künstliche Intelligenz

Für die Entwicklung und den Einsatz von KI-Systemen, in denen personenbezogene Daten verarbeitet werden, beinhaltet die Datenschutz-Grundverordnung (DS-GVO) wichtige rechtliche Vorgaben. Sie dienen dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Auch für KI-Systeme gelten die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO). Diese Grundsätze müssen gemäß Art. 25 DS-GVO durch frühzeitig geplante technische und organisatorische Maßnahmen von den Verantwortlichen umgesetzt werden (Datenschutz durch Technikgestaltung).

1. KI darf Menschen nicht zum Objekt machen

Die Garantie der Würde des Menschen (Art. 1 Abs. 1 GG, Art. 1 GRCh) gebietet, dass insbesondere im Fall staatlichen Handelns mittels KI der Einzelne nicht zum Objekt gemacht wird. Vollständig automatisierte Entscheidungen oder Profiling durch KI-Systeme sind nur eingeschränkt zulässig. Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Art. 22 DS-GVO nicht allein der Maschine überlassen werden. Wenn der Anwendungsbereich des Art. 22 DS-GVO nicht eröffnet ist, greifen die allgemeinen Grundlagen des Art. 5 DS-GVO, die

[1] BT-Drs. 19/1982 zu 1., Die Datenethikkommission der Bundesregierung hebt ergänzend als wichtige Grundlagen für KI die Mustererkennung, das maschinelle Lernen und Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung hervor (Empfehlungen der Datenethikkommission für die Strategie Künstliche Intelligenz der Bundesregierung, 9.10.2018;).

insbesondere mit den Grundsätzen der Rechtmäßigkeit, Zurechenbarkeit und Fairness die Rechte des Einzelnen schützen. Betroffene haben auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person (Intervenierbarkeit), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung.

2. KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben

Auch für KI-Systeme gilt, dass sie nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden dürfen. Zu beachten ist auch der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO). Zweckänderungen sind mit Art. 6 Abs. 4 DS-GVO klare Grenzen gesetzt. Auch bei KI-Systemen müssen erweiterte Verarbeitungszwecke mit dem ursprünglichen Erhebungszweck vereinbar sein. Das gilt auch für die Nutzung personenbezogener Daten zu Trainingszwecken von KI-Systemen.

3. KI muss transparent, nachvollziehbar und erklärbar sein

Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DS-GVO). Dies erfordert insbesondere eine transparente Verarbeitung, bei der die Informationen über den Prozess der Verarbeitung und ggf. auch über die verwendeten Trainingsdaten leicht zugänglich und verständlich sind (Art. 12 DS-GVO). Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, müssen nachvollziehbar und erklärbar sein. Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Nach der DS-GVO ist dafür auch über die involvierte Logik ausreichend aufzuklären. Diese Transparenz-Anforderungen sind fortwährend zu erfüllen, wenn KI-Systeme zur Verarbeitung von personenbezogenen Daten eingesetzt werden. Es gilt die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DS-GVO).

4. KI muss Diskriminierungen vermeiden

Lernende Systeme sind in hohem Maße abhängig von den eingegebenen Daten. Durch unzureichende Datengrundlagen und Konzeptionen kann es zu Ergebnissen kommen, die sich als Diskriminierungen auswirken. Diskriminierende Verarbeitungen stellen eine Verletzung der Rechte und Freiheiten der betroffenen Personen dar. Sie verstoßen u. a. gegen bestimmte Anforderungen der Datenschutz-Grundverordnung, etwa den Grundsatz der Verarbeitung nach Treu und Glauben, die Bindung der Verarbeitung an legitime Zwecke oder die Angemessenheit der Verarbeitung.

Diese Diskriminierungsneigungen sind nicht immer von vornherein erkennbar. Vor dem Einsatz von KI-Systemen müssen deshalb die Risiken für die Rechte und Freiheiten von Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen.

5. Für KI gilt der Grundsatz der Datenminimierung

Für KI-Systeme werden typischerweise große Bestände von Trainingsdaten genutzt. Für personenbezogene Daten gilt dabei auch in KI-Systemen der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO). Die Verarbeitung personenbezogener Daten muss daher stets auf das

notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.

6. KI braucht Verantwortlichkeit

Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung und die Beherrschbarkeit des KI-Systems zu gewährleisten. Der Verantwortliche muss sicherstellen, dass die Grundsätze nach Art. 5 DS-GVO eingehalten werden. Er muss seine Pflichten im Hinblick auf die Betroffenenrechte aus Art. 12 ff DS-GVO erfüllen. Der Verantwortliche muss die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO gewährleisten und somit auch Manipulationen durch Dritte, die sich auf die Ergebnisse der Systeme auswirken, verhindern. Beim Einsatz eines KI-Systems, in dem personenbezogene Daten verarbeitet werden, wird in der Regel eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich sein.

7. KI benötigt technische und organisatorische Standards

Um eine datenschutzgerechte Verarbeitung sicherzustellen, sind für Konzeption und Einsatz von KI-Systemen technische und organisatorische Maßnahmen gemäß Art. 24 und 25 DS-GVO zu treffen, wie z. B. Pseudonymisierung. Diese erfolgt nicht allein dadurch, dass der Einzelne in einer großen Menge personenbezogener Daten scheinbar verschwindet. Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft. Die Datenschutzaufsichtsbehörden werden diesen Prozess aktiv begleiten.

III. Die Entwicklung von KI bedarf der Steuerung

Die Datenschutzaufsichtsbehörden überwachen die Anwendung des Datenschutzrechts, setzen es durch und haben die Aufgabe, bei der Weiterentwicklung für einen effektiven Grundrechtsschutz einzutreten. Angesichts der hohen Dynamik in der Entwicklung der Technologien von künstlicher Intelligenz und der vielfältigen Einsatzfelder zeichnen sich die Grenzen der Entwicklung noch nicht ab. Gleichermaßen sind die Risiken der Verarbeitung personenbezogener Daten in KI-Systemen nicht pauschal einzuschätzen. Auch ethische Grundsätze sind zu beachten. Wissenschaft, Datenschutz-aufsichtsbehörden, die Anwender und besonders die Politik sind gefordert, die Entwicklung von KI zu begleiten und im Sinne des Datenschutzes zu steuern.