Städteverband Schleswig-Holstein

Die neue EU-Datenschutz-Grundverordnung – was ändert sich bei der Datenverarbeitung durch Kommunen?

Teil 1: Einordnung der DSGVO, Rechtsgrundlagen der Datenverarbeitung

Die *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkeh und zur Aufhebung der Richtlinie 95/46/EG* (Datenschutz-Grundverordnung – DSGVO) ist derzeit in aller Munde. Sie hat, neben einschlägigen Skandalen um soziale Netzwerke, dazu geführt, dass das Thema Datenschutz in den Fokus gerückt ist. In der Tat entdecken manche Stellen bei dieser Gelegenheit Rechtspflichten, die bereits nach altem Recht und damit schon seit vielen Jahren galten. Ein großer Teil der Aufmerksamkeit wird von mehr oder weniger seriösen, häufig selbst ernannten Experten erzeugt, die durch die Lande ziehen und jenen öffentlichen und privaten Stellen den baldigen Untergang voraussagen, die sich nicht für deftige Honorare beraten lassen. Befeuert wird das Ganze durch die hohen Bußgelder, die nach der DSGVO von den Datenschutz-Aufsichtsbehörden künftig verhängt werden können: bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes. Das Bundesdatenschutzgesetz hatte bisher als maximales Bußgeld 300.000 Euro vorgesehen. Aus dem Umstand, dass der neue Höchstbetrag das sechsundsechzigfache des alten beträgt, wurde schon abgeleitet, dass die Aufsichtsbehörden jetzt alle Bußgelder mal 66 nehmen müssten; wo frühe 1.000 Euro verhängt wurden, sollten nun 66.000 Euro verhängt werden.

Abseits von solchen abwegigen Vorstellungen soll in diesem Beitrag herausgearbeitet werden, welche Änderungen durch die DSGVO tatsächlich auf öffentliche Stellen und namentlich auf Kommunen zukommen. Dabei wird die DSGVO zunächst in ihren rechtlichen Kontext eingeordnet. Nach einem kurzen Blick auf den Anwendungsbereich ein paar Begriffe wenden wir uns schließlich den Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten zu, die für öffentliche Stellen künftig gelten und werfen am Ende dieses ersten Teils noch einen Blick auf die Vorschriften zur Zweckänderung bei der Datenverarbeitung. Im zweiten Teil wird es um die Rechte der Betroffenen, die organisatorischen Pflichten der Verantwortlichen sowie um die aufsichtsbehördlichen Maßnahmen und den Rechtsschutz dagegen gehen.

1. Geschichte:

Bereits seit 1995 gibt es eine europäische Regelung zum Datenschutz: die *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. Diese Richtlinie stammt aus einer Zeit vor dem Internet, Smartphones, Facebook und Tinder. Es wurde schnell offenbar, dass eine neue Regelung des Datenschutzes im Internetzeitalter geboten war. Zudem hatte es in der Zwischenzeit auch rechtliche Entwicklungen auf Ebene des EU-Rechts gegeben. Bekanntlich hatte das Bundesverfassungsgericht im Jahr 1983 ein neues Grundrecht entdeckt: das informationelle Selbstbestimmungsrecht. Allerdings ist dieses für den Laien im Grundgesetz kaum auffindbar, der Begriff Datenschutz findet sich dort nicht ausdrücklich. Anders im sog. Primärrecht der EU (den die EU konstituierenden Rechtsnormen): Mit dem Vertrag von Lissabon wurde die Europäische Grundrechtecharta Teil des EU-Rechts. In Art. 8 findet sich nicht nur das Recht auf Datenschutz für alle Bürger der EU, sondern auch einige der wichtigsten Grundsätze des Datenschutzes:

Gesetzgebung der EU in diesem Bereich. Diese Kompetenz hat die EU mit der DSGVO wahrgenommen.

Die Arbeiten an der DSGVO begannen schon vor 2010 und zogen sich über einen selbst für die EU-Gesetzgebung erstaunlich langen Zeitraum hin. Dies hatte nicht zuletzt damit zu tun, dass interessierte Lobbygruppen intensiv daran arbeiteten, effektivere datenschutzrechtliche Vorschriften zu verwässern. Es ist nicht zuletzt dem langen Atem des Grüne-Abgeordneten im EU-Parlament Jan-Philip Albrecht (dem künftigen Umweltminister in Schleswig-Holstein) zu verdanken, dass das Gesetzeswerk schließlich erfolgreich verabschiedet wurde.

Die DSGVO wurde am 4.5.2016 im Amtsblatt der EU verkündet. Art. 99 der DSGVO besagt, dass sie am 20. Tag nach der Verkündung in Kraft tritt und ab dem 25.5.2018 gilt. Es soll hier nicht untersucht werden, wie eine Rechtsvorschrift gleichzeitig in Kraft sein und (noch) nicht gelten kann (diese Konstellation erinnert den Autor an Schrödingers Katze, die gleichzeitig lebendig und tot ist). Hinzuweisen ist aber darauf, dass die neuen rechtlichen Vorgaben seit gut zwei Jahren bekannt sind. Daher wird es bei der Umsetzung auch keine weitere Karenzzeit geben (wiewohl dies schon von manchen Stellen gefordert wurde).

2. Einordnung der DSGVO in den Kontext alter und neuer Datenschutzvorschriften

In der deutschen Diskussion wird die DSGVO meist mit den geltenden Vorschriften zum Datenschutz im Bundesdatenschutzgesetz (BDSG) und in den Landesdatenschutzgesetzen (LDSG) verglichen. Dieser Vergleich hinkt allerdings. Richtiger wäre es, die DSGVO mit ihrer europäischen Vorgängervorschrift zu vergleichen, der Richtlinie 95/46/EG. Ein solcher Vergleich zeigt, dass viele Regelungen der DSGVO bereits Entsprechungen in der 95er-Richtlinie haben und lediglich weiterentwickelt wurden. Dies gilt z.B. für die meisten Grundsätze in Art. 5 Abs. 1 DSGVO (wie z.B. die Verarbeitung nach Treu und Glauben und auf rechtmäßige Weise), die sich schon in Art. 6 der 95er-Richtlinie finden. Der entscheidende Unterschied ist die Wahl des Regelungsinstruments durch die EU. Die Richtlinie 95/46/EG war wie jede EU-Richtlinie an die Mitgliedstaaten adressiert und machte diesen Vorgaben dazu, welche Vorschriften zum Datenschutz zu erlassen sind. Die Mitgliedstaaten setzten die Richtlinie oft verzögert um und nahmen sich dabei einige Freiheiten. Die DSGVO ist eine EU-Verordnung und gilt somit unmittelbar. Der deutsche Gesetzgeber verzichtete bei der Umsetzung der 95er-Richtlinie aus guten Gründen darauf, den Grundsatz der Verarbeitung nach Treu und Glauben in deutsches Recht zu übernehmen. Gerade für öffentliche Stellen in Deutschland ergibt sich die Bindung an Recht und Gesetz schon aus Art. 20 Abs. 2 GG. Für den zivilrechtlichen Begriff „Treu und Glauben" ist daneben im öffentlichen Recht kein Raum. Unter der DSGVO gilt dieses Prinzip jetzt jedoch unmittelbar nach Art. 5 Abs. 1 DSGVO. Auf der Ebene des EU-Rechts hat sich damit im Vergleich zur 95er-Richtlinie nicht viel geändert. Auf Ebene des deutschen öffentlichen Rechts ist allerdings nicht klar, wie die jetzt unmittelbar geltende Verpflichtung auf Treu und Glauben in die Rechtsanwendung zu integrieren ist. Das Beispiel soll zeigen, dass manche Fragen und Probleme bei der Rechtsanwendung aus der spezifischen Konstellation herrühren, dass ein Rechtsbereich, der bisher durch EU-Recht überformt, aber durch nationales Recht geregelt war, nun durch unmittelbar anzuwendendes EU-Recht geregelt wird.

Namentlich für den öffentlichen Bereich wird die Lage allerdings dadurch entschärft, dass die DSGVO eine Reihe von Öffnungsklauseln enthält. Diese erlauben es dem nationalen Gesetzgeber, eigene Regelungen zu treffen, z.T. schreiben sie solche Regelungen auf Ebene der Mitgliedstaaten vor. An diesen Stellen wirkt die DSGVO eher wie eine Richtlinie, die einen gewissen Spielraum für die

Mitgliedstaaten lässt. Allerdings führen diese Öffnungsklauseln dazu, dass es nicht ausreicht, in die DSGVO zu schauen, um die Rechtslage zu beurteilen. Zusätzlich ist der Blick in das nationale Recht geboten, welches die Öffnungsklauseln ausfüllt. Dieses findet sich wie schon bisher in allgemeinen Datenschutzgesetzen (auf Bundesebene das BDSG, auf Landesebene die LDSG) sowie in bereichsspezifischen Vorschriften, d.h. Fachgesetzen, die (auch) Vorgaben zur Verarbeitung von personenbezogenen Daten enthalten.

Der Blick des Rechtsanwenders muss also zwischen der DSGVO und dem nationalen Recht hin und her schweifen. Leider aber ist die Lage noch komplexer. Zeitgleich mit der DSGVO wurde im EU-Amtsblatt eine weitere Rechtsvorschrift veröffentlicht: die *Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates* (JI-Richtlinie). Aus bestimmten Gründen hatte die EU sich entschlossen, die Datenschutzvorschriften für diesen Bereich in einem separaten Regelungsinstrument zusammenzufassen und dafür das Instrument einer Richtlinie zu wählen. Offensichtlich gelten diese Richtlinie bzw. die zu ihrer Umsetzung erlassenen nationalen Vorschriften für den Bereich der Strafverfolgung durch die Polizei und die Justiz sowie der Gefahrenabwehr durch die Polizei. Wegen der Nähe zur Strafverfolgung fällt allerdings auch die Verfolgung von Ordnungswidrigkeiten unter die Richtlinie. Dies ist von Bedeutung für alle Bußgeldverfahren, die von den Kommunen betrieben werden. Namentlich im Bereich der Verfolgung von Verkehrsordnungswidrigkeiten, wo es in den Fachgesetzen an konkreten Vorgaben zur Verarbeitung personenbezogener Daten fehlt, werden die Vorschriften zur Umsetzung der JI-Richtlinie zur Anwendung kommen. Bei der Gefahrenabwehr, die durch die kommunalen Ordnungsbehörden betrieben wird, bleibt es bei der Anwendung der DSGVO und der ergänzenden mitgliedstaatlichen Regelungen.

Zur Wahrnehmung der Öffnungsklauseln der DSGVO und zur Umsetzung der JI-Richtlinie hatte der Bundesgesetzgeber schon frühzeitig mit den Vorarbeiten begonnen, so dass ein neues BDSG bereits im Juni 2017 verabschiedet werden konnte – noch vor der Bundestagswahl 2017. Auf Landesebene begannen die Vorarbeiten später, so dass ein Gesetzentwurf für ein neues LDSG erst im Januar 2018 in den Landtag eingebracht wurde. Wie auf Bundesebene finden sich hier die Ausfüllung der Öffnungsklauseln der DSGVO und die Umsetzung der JI-Richtlinie zusammengefasst in einem Gesetz (in einigen anderen Bundesländern soll dies in zwei unterschiedliche Gesetze aufgespalten werden). Aufgrund mangelnder Abstimmung bei der Erstellung des Gesetzentwurfs waren noch einige Änderungen im parlamentarischen Prozess nötig, um einen halbwegs konsistenten Entwurf zu erzeugen. Dieser wurde am 27. April 2018 vom Schleswig-Holsteinischen Landtag verabschiedet, so dass das neue LDSG rechtzeitig zum 25. Mai 2018 in Kraft treten kann. Zum Zeitpunkt der Abfassung dieses Beitrags war das neue LDSG noch nicht verkündet worden, so dass hier für den vollständigen Text nur auf die letzte Landtagsdrucksache dazu (19/664) verwiesen werden kann.

> Die Grafik versucht, die relevanten Rechtsgrundlagen darzustellen. Eine Kommune in Schleswig-Holstein (eingekreist) muss bei der Rechtsanwendung die DSGVO selbst sowie den 2. Teil des LDSG berücksichtigen, der die Öffnungsklauseln der DSSGVO umsetzt. Soweit Ordnungswidrigkeitsverfahren betrieben werden, ist auch der 3. Teil des LDSG zu berücksichtigen. Nicht berücksichtigt sind hier bereichsspezifische Vorschriften. [Grafik in PPT-Folie]

3. Anwendungsbereich, Begriffe

Die DSGVO unterscheidet nicht zwischen öffentlichen und nicht-öffentlichen Stellen, wie es das deutsche Datenschutzrecht traditionell tut. Allerdings ist der nationale Gesetzgeber auch nicht gehindert, eine solche Unterscheidung einzuführen, solange diese nicht mit den verbindlichen Vorgaben der DSGVO kollidiert. Das LDSG-neu regelt grundsätzlich im Bereich der Öffnungsklausen der DSGVO für die öffentlichen Stellen des Landes. Wie schon bisher sind dies die „Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung" (§ 2 Abs. 1 LDSG-neu). Allerdings gibt es eine wichtige Ausnahme: Nach § 1 Abs.4 LDSG-neu soll das Gesetz keine Anwendung finden, „soweit öffentliche Stellen nach Absatz 1 am Wettbewerb teilnehmen und personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten." Dann soll für den Bereich der Wettbewerbsteilnahme das BDSG gelten. Als Beispiel nennt die Gesetzesbegründung das UKSH (und andere von öffentlich-rechtlichen Trägern geführte Krankenhäuser), soweit die Patientenversorgung betroffen ist. Auch im kommunalen Bereich kann es solche Konstellationen geben, z.B. wenn eine Gemeinde einen Eigenbetrieb unterhält, der in einem der Bereiche aktiv ist, die dem Wettbewerb unterfallen (z.B. Strom- und Gasversorgung). Entsprechendes gilt für Verkauf von Holz aus kommunalen Wäldern. Hier unterfällt die Verarbeitung der Kundendaten dem BDSG, aber alle andere kommunalen Verarbeitungen und namentlich die der Beschäftigtendaten dem LDSG.

In Art. 4 finden sich ausführliche Definitionen der zentralen Begriffe. Manche davon sind neu, andere weichen von der bisherigen Definition ab.

„Personenbezogene Daten" liegen nicht nur dann vor, wenn eine Klarname genannt wird. Es genügt, dass der Betroffene individualisiert werden, d.h. ein Eins-zu-Eins-Bezug zwischen den Daten und einer Person hergestellt werden kann. Damit sind auch z.B. Autonummern oder IP-Adressen personenbezogen.

„Verarbeitung" ist nach wie vor jede Aktivität, die an oder mit personenbezogenen Daten ausgeführt wird. In der Definition werden eine Vielzahl von Beispielen genannt, unter anderem „Offenlegung durch Übermittlung" wo bisher nur von Übermittlung die Rede war. Eine Rechtsänderung durch den etwas verunglückten Begriff ergibt sich nicht.

Die „datenverarbeitende Stelle" des LDSG-alt wird nun zum „Verantwortlichen". Verantwortlicher ist, „wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Dabei ist es nicht erforderlich, dass der Verantwortliche selbst die Daten verarbeitet. So kann auch eine Stelle, die lediglich die Infrastruktur vorgibt, zum Verantwortlichen werden. Meist wird es sich dann bei dieser Stelle und den Stellen, die die praktisch mit den Daten umgehen, um gemeinsam für die Verarbeitung Verantwortliche im Sinne von Art. 26 DSGVO handeln. Der Verantwortliche ist Adressat der meisten zentralen Pflichten in der DSGVO.

Die bisher als Auftragsdatenverarbeiter bezeichnete Rolle heißt nunmehr vereinfacht „Auftragsverarbeiter".

Neuerdings definiert werden „genetische Daten", „biometrische Daten" und „Gesundheitsdaten", alle gehören zu den sensiblen Daten nach Art. 9 Abs. 1 DSGVO (siehe unten).

4. Rechtsgrundlagen für die Datenverarbeitung

4.1 Allgemeines

Wie schon bisher gilt für die Verarbeitung ein Verbot mit Erlaubnisvorbehalt: Die Verarbeitung ist nicht zulässig, es sei denn, eine Rechtsgrundlage erlaubt sie ausdrücklich. Dabei macht die DSGVO zunächst keine Unterscheidung zwischen der Datenverarbeitung durch öffentliche bzw. durch private („nicht-öffentliche") Stellen. Diese im deutschen Datenschutzrecht hergebrachte Differenzierung ist dem europäischen Datenschutzrecht fremd. Allerdings finden sich dann in einzelnen Vorschriften der DSGVO doch Öffnungsklauseln und Vorgaben, die es dem deutschen Gesetzgeber erlauben, bei der hierzulande hergebrachten unterschiedlichen Regelung für den privaten und den öffentlichen Bereich zu bleiben.

Von dem grundsätzlichen Verbot der Verarbeitung personenbezogener Daten ausgenommen ist die Verarbeitung „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" (Art. 2 Abs. 2 Buchstabe c). Die Reichweite dieser sog. Haushaltsausnahme ist nicht immer ganz klar. Jedenfalls dann, wenn eine Privatperson Daten anderer Personen im Internet veröffentlicht, wird der Anwendungsbereich der Haushaltsausnahme verlassen (EuGH, 06.11.2003 - C-101/01).

In der DSGVO finden sich die Rechtsgrundlagen für die Datenverarbeitung in Kapitel II („Grundsätze"). Die erste Vorschrift hier ist der schon erwähnte Art. 5, der die Grundsätze für die Verarbeitung personenbezogener Daten enthält. Diese sind selbstverständlich einzuhalten und müssen vor allem bei der Gestaltung von neuen Verarbeitungsprozessen beachtet werden. Allerdings stellen die Grundsätze des Art. 5 selbst keine Rechtsgrundlagen dar, auf welche die Verarbeitung gestützt werden kann. Die eigentlichen Erlaubnisnormen, die festlegen, wann personenbezogene Daten verarbeitet werden dürfen, finden sich in Art. 6 Abs. 1 DSGVO.

Wie schon im bisherigen Recht findet sich hier zunächst die Einwilligung (Art. 6 Abs. 1 Buchstabe a). Die Anforderungen an eine wirksame Einwilligung sind in Art. 7 ausgeführt. Schriftform ist nicht erforderlich, allerdings muss der Verantwortliche die Einwilligung nachweisen können. Im öffentlichen Bereich dürfte die Einwilligung eher selten und nur bei Zusatzangeboten zum Einsatz kommen, die außerhalb dessen liegen, was zu den gesetzlichen Aufgaben der öffentlichen Stelle gehört. Zum einen bestehen wegen des im öffentlich-rechtlichen Bereichs im Grundsatz gegebenen Über-Unterordnungsverhältnisses erhebliche Zweifel an der Freiwilligkeit der Einwilligung (Art. 7 Abs. 4). Zum anderen ist es aus verfassungsrechtlichen Gründen für öffentliche Stellen nicht zulässig, auf der Grundlage einer vermeintlichen Einwilligung den ihnen gesetzlich erlaubten Satz von personenbezogenen Daten zu erweitern. So dürfte eine Gemeinde nicht auf Grundlage einer Einwilligung im Melderegister weitere, im BMG nicht genannte Daten speichern.

Art. 6 Abs. 1 enthält weitere Rechtsgrundlagen, die für öffentliche Stellen nicht relevant sind, wie die Verarbeitung zur Erfüllung eines Vertrags (Buchstabe b) oder zur Wahrung berechtigter Interessen des Verantwortlichen (Interessenabwägung, Buchstabe f).

Die für öffentliche Stellen relevante Rechtsgrundlage findet sich in Buchstabe e). Danach ist die Verarbeitung zulässig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen

übertragen wurde. Anders als bei den meisten anderen Varianten in Art. 6 Abs. 1 wirkt Buchstabe e) jedoch nicht selbst als Rechtsgrundlage. Vielmehr bildet die Norm den Rahmen für die Öffnungsklauseln in Art. 6 Abs. 2 und 3. Das Verhältnis von Abs. 2 zu Abs. 3 bleibt schleierhaft, scheinen beide doch das gleiche zu regeln und eine daher verzichtbar (vgl. Reimer, in: Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 6 Rn. 29-30, beck-online). Hier soll auf den leichter lesbaren Abs. 2 abgestellt werden. Dieser lautet:

„Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX."

Diese Öffnungsklausel erlaubt es dem deutschen Gesetzgeber, genauer zu bestimmen, wann die Voraussetzungen von Art. 6 Abs. 1 Buchstabe f) vorliegen, wann also die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem Verantwortlichen übertragen wurde.

Die DSGVO geht hier erkennbar davon aus, dass durch bereichsspezifisches Recht („spezifische Anforderungen", „präziser bestimmen") für bestimmte, konkrete Verarbeitungsvorgänge im öffentlichen Bereich Regelungen erlassen werden. Nun ist dies in Deutschland schon vor vielen Jahren erfolgt, weil deutsches Verfassungsrecht bereichsspezifische Rechtsgrundlagen für die Datenverarbeitung erforderte. Hier erlaubt die DSGVO, dass bestehende Regelungen „beibehalten" werden können. Das ist eine sehr gute Nachricht für die Datenschutzregelungen im öffentlichen Bereich. Zwar trifft den Gesetzgeber auf Bundes- und Länderebene die Pflicht zu prüfen, ob die bereichsspezifischen Gesetze den Anforderungen genügen. Man kann aber getrost davon ausgehen, dass dies in den allermeisten Fällen zu bejahen ist und die zahlreichen bereichsspezifischen Regelungen nicht geändert werden müssen. (Änderungsbedarf ergibt sich z.T. allerdings mit Blick auf die Verarbeitung von „sensiblen Daten", dazu sogleich.)

Allerdings ist der deutsche Gesetzgeber hier noch einen Schritt weitergegangen (und zwar zunächst auf Bundesebene, d.h. beim BDSG, da dieses als erstes Gesetz zur Ausfüllung der Öffnungsklauseln erlassen wurde). Hier wurde, gestützt auf die Öffnungsklausel in Art. 6 Abs. 2 und 3, mit § 3 BDSG auch eine allgemeine Rechtsgrundlage zur Datenverarbeitung durch öffentliche Stellen aufgenommen, die vom Wortlaut praktisch mit Art. 6 Abs. 1 Buchstabe e) identisch ist. Der Gesetzgeber des LDSG Schleswig-Holstein ist diesem Vorbild mit § 3 Abs. 1 LDSG-neu gefolgt. Damit steht eine in der Praxis sehr wichtige Rechtsgrundlage für solche Fälle zur Verfügung, bei denen keine der bereichsspezifischen Regelungen angewendet werden kann. Dem Vernehmen nach sieht man diese Auslegung der Öffnungsklausel bei der EU-Kommission eher kritisch, allerdings hat es wohl noch keine offizielle Kommunikation dazu gegeben.

4.2 Erlaubnis zur Verarbeitung sensibler Daten

Neben der allgemeinen Zulässigkeitsvorschrift in Art. 6 Abs. 1 enthält die DSGVO noch spezielle Vorschriften dazu, wann die Verarbeitung von „besonderen Kategorien personenbezogener Daten" erlaubt ist. Dies umfasst die folgenden Datenkategorien:

Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Eine ähnliche Kategorisierung gab es schon in der 95er-Richtlinie und infolge dessen auch im deutschen Recht. Herkömmlich werden diese Daten oft als „sensible Daten" bezeichnet. Für diese Daten gilt ein besonderes Verbot mit Erlaubnisvorbehalt, wobei die Schwelle für die Zulässigkeit der Verarbeitung hier generell höher sein soll. In welchem Verhältnis stehen nun die Zulässigkeitsnormen nach Art. 9 und Art. 6? Die deutschen Aufsichtsbehörden sind der Auffassung, dass die Vorschriften wie ein doppelter Filter wirken: für sensible Daten müssen zunächst die spezielle Voraussetzungen nach Art. 9 Abs. 2 vorliegen. Ist dies der Fall, so muss auch eine Erlaubnisnorm nach Art. 6 Abs. 1 die Verarbeitung allgemein erlauben. In der Praxis ist dies meist kein Problem, da die strengeren Vorgaben des Art. 9 Abs. 2 meist die weniger strikten des Art. 6 Abs. 1 mitumfassen.

Für die Verarbeitung von sensiblen Datum durch öffentliche Stellen ist vor allem die Erlaubnis nach Art. 9 Abs. 2 Buchstabe g) von Belang. Danach ist die Verarbeitung dann zulässig, wenn sie „auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich" ist. Hier sind drei Elemente von Interesse: Zuerst stellt die Norm durch den Verweis auf das Recht des Mitgliedstaates eine Öffnungsklausel zur Verfügung, der Bereich kann also durch nationales Recht geregelt werden. Weiterhin reicht hier im Gegensatz zu Art. 6 Abs. 2 Buchstabe e nicht ein einfaches öffentliches Interesse, sondern es ist ein „erhebliches" öffentliches Interesse notwendig. Und schließlich muss das nationale Recht „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" vorsehen.

Weitere Öffnungsklauseln mit Relevanz für den öffentlichen Bereich finden sich in Art. 6 Abs. 2 Buchstabe i) für Zwecke des öffentlichen Gesundheitswesens und in Art. 6 Abs. 2 Buchstabe j) für Archivzwecke, wissenschaftliche oder historische Forschungszwecke und statistische Zwecke. Neben der Verhältnismäßigkeit der Rechtsgrundlage wird auch hier jeweils das Vorhandensein von „Maßnahmen" gefordert.

Der Gesetzgeber des BDSG hat versucht, die geforderten angemessenen und spezifischen Maßnahmen zu konkretisieren, siehe § 22 Abs. 2 BDSG-neu. Genannt werden dort neben technisch-organisatorische Maßnahmen allgemein und konkreten Techniken wie Pseudonymisierung und Verschlüsselung auch z.B. die „Sensibilisierung" der Mitarbeiter, gemeint sind wohl Schulungen. Der Landesgesetzgeber ist diesem Vorbild mit § 12 Abs. 2 und 3 LDSG-neu gefolgt. Viel wird mit diesem Ansatz jedoch nicht bewirkt, denn die Pflicht, angemessene technisch-organisatorische Maßnahmen zu treffen ergibt sich schon aus Art. 32 DSGVO, und zwar für alle Kategorien von Daten, nicht nur für sensible.

Wie zu Art. 6 Abs. 1 Buchstabe e) erläutert, kann jedenfalls auch im Hinblick auf die Verarbeitung von sensiblen Daten bereichsspezifisches Recht geschaffen oder beibehalten werden, wenn es die Voraussetzungen erfüllt. Ein Beispiel könnte § 3 Abs. 1 Nr. 11 BMG sein, der die Speicherung der Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft und damit die Verarbeitung von

Daten über religiöse Überzeugungen vorschreibt. Hier wäre nun zu prüfen, ob die Verarbeitung einem „erheblichen öffentlichen Interesse" dient und ob die angemessenen und spezifischen Maßnahmen vorgesehen sind. Soweit ersichtlich, hat der Gesetzgeber des BMG dies allerdings noch nicht getan. Änderungen des BMG im Zusammenhang mit dem Inkrafttreten der DSGVO gab es nicht. Allerdings ist der Prozess von Folgeänderungen auf Bundesebene noch lange nicht abgeschlossen. Zwar gab es schon ein sog. Omnibusgesetz, mit dem eine Reihe von Anpassungen im Fachrecht erfolgte, namentlich in der AO und im SGB (Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17.07.2017, BGBl. 2541). Dem Vernehmen nach sind jedoch noch weitere Omnibusgesetze auf Bundesebene in Vorbereitung, mit denen entsprechende Änderungen im Fachrecht bewirkt werden sollen.

Auf Landesebene finden sich Änderungen im Fachrecht, mit denen eine DSGVO-konforme Rechtsgrundlage zur Verarbeitung von sensiblen Daten geschaffen werden soll, vor allem für Zwecke des öffentlichen Gesundheitswesens. So wurde durch das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 27.04.2018 ein neuer Absatz 6 an § 16 GDG angefügt, der den Trägern des öffentlichen Gesundheitsdienstes die Verarbeitung von sensiblen Daten erlaubt, „soweit dies im Einzelfall zur Erfüllung von Aufgaben nach diesem Gesetz erforderlich ist". Offenbar geht der Gesetzgeber hier davon aus, dass für alle Aufgaben nach dem GDG ein erhebliches öffentliches Interesse besteht. Weiterhin wird über einen Verweis auf § 12 LDSG-neu auch die Geltung der dort beschriebenen angemessenen und spezifischen Maßnahmen angeordnet.

Wie bei der allgemeinen Zulässigkeitsklausel nach Art. 6 Abs. 1 Buchstabe e) haben sowohl der Bundes- als auch der Landesgesetzgeber eine Generalklausel zur Zulässigkeit der Verarbeitung von sensible Daten ins BDSG (§ 22 Abs. 1) bzw. ins LDSG (§ 12 Abs. 1) eingefügt. Auf diese kann wiederum zurückgegriffen werden, sollte sich in den bereichsspezifischen Regelungen der Fachgesetze keine Rechtsgrundlage finden.

5. Zweckbindung, Zweckänderungen

In Art. 5 Abs. 1 Buchstabe b) findet sich der Grundsatz der Zweckbindung: „personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt (...) nicht als unvereinbar mit den ursprünglichen Zwecken".

Interessanterweise kommt es hier zu einer Lockerung des schon aus dem alten Recht bekannten Zweckbindungsgrundsatzes. War bisher von einer Zweckidentität auszugehen („dürfen nur für den Zweck weiterverarbeitet werden, für den sie rechtmäßig erhoben worden sind", § 13 Abs. 2 LDSG-alt), so wird jetzt nur noch Vereinbarkeit der Zwecke verlangt. In Art. 6 Abs. 4 stellte die DSGVO ein paar Kriterien bereit, um festzustellen, ob die Verarbeitung zu dem neuen Zweck mit dem alten vereinbar ist. Dazu gehören u.a.: Verbindung zwischen den Zwecken, Art der personenbezogenen Daten (bei sensiblen Daten eher keine Vereinbarkeit) und das Vorhandensein geeigneter Garantien zum Schutz der Rechte der Betroffenen wie Verschlüsselung oder Pseudonymisierung.

Diese neuen Regelungen machen die Verwendung von einmal erlangten Informationen für ähnliche Zwecke deutlich einfacher. So wird z.B. im Kontext von Vollstreckungen durch kommunale

Vollstreckungsbeamte oft gefragt, ob die in einem Verfahren erlangte Kontoinformation des Schuldners auch für die Vollstreckung in einem anderen Verfahren verwendet werden kann. Nach hiesiger Auffassung wäre dies zu bejahen, wenn es bei beiden Verfahren um gemeindliche Abgaben geht. Eine Verbindung zwischen den Zwecken liegt in der Durchsetzung der kommunalen Abgabenforderungen, zugleich ist die Kontoinformation kein sensibles Datum nach Art. 9 Abs. 1 DSGVO.

Auch der Aspekt der geeigneten Garantien und hier namentlich der Pseudonymisierung kann hilfreich sein. So ist es unter der DSGVO eindeutig, dass auch Pseudonyme personenbezogene Daten sind und dass daher für ihre Verarbeitung eine Rechtsgrundlage erforderlich ist. Bisher half hier § 11 Abs. 6 LDSG-alt, der es erlaubte, pseudonymisierte Daten zu verarbeiten und auch zu übermitteln, wenn der Verantwortliche keinen Zugriff auf die Zuordnungsfunktion, also die Zuordnung der Pseudonyme zu den Klarnamen, hat. Zwar findet sich eine solche Vorschrift jetzt nicht mehr. Allerdings kommt man zu praktisch gleichen Ergebnissen, wenn man die Zweckänderung der Daten unter der Bedingung zulässt, dass diese sicher pseudonymisiert sind.

Darüber hinaus enthält Art. 6 Abs. 4 eine Öffnungsklausel, die es den Mitgliedstaaten erlaubt, für die in Art. 23 Abs. 1 genannten Zwecke weitere ausdrückliche Zweckdurchbrechungen zuzulassen. Diese ist im LDSG-neu in § 4 wahrgenommen worden. In Anlehnung an die entsprechende Norm des BDSG-neu ist die zweckändernde Verarbeitung der Daten z.B. dann erlaubt, wenn dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist. Nach § 4 Abs. 2 LDSG-neu ist die Zweckänderung bei sensiblen Daten allerdings darauf beschränkt, dass die Verarbeitung für den neuen Zweck auf eine Vorschrift gestützt werden kann, die die Verarbeitung sensibler Daten erlaubt.

Neben der Erlaubnis der ausdrücklichen Zweckänderung findet sich in § 3 Abs. 2 noch die Fiktion einer Zweckerstreckung: „Zu dem Zweck der Verarbeitung personenbezogener Daten gehört auch die Verarbeitung zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung, zur Durchführung von Organisationsuntersuchungen und zur Prüfung und Wartung von automatisierten Verfahren. Dies gilt auch für die Verarbeitung personenbezogener Daten zu Aus- und Fortbildungszwecken, soweit nicht schutzwürdige Interessen der betroffenen Person entgegenstehen." Damit wird eine ähnliche Regelung des § 13 Abs. 5 LDSG-alt fortgeführt. Als Öffnungsklausel beruft sich der Gesetzgeber auf die allgemeine Öffnungsklausel für den öffentlichen Bereich in Art. 6 Abs. 2 und 3.

Lukas Gundermann, LL.M. (Edinburgh)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein