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

Teil 2: Rechte der Betroffenen, organisatorische Vorgaben, Aufsichtsbehörden

Im ersten Teil fanden sich Ausführungen zur Einordnung der EU-Datenschutz-Grundverordnung (DSGVO) in den Kontext des europäischen und deutschen Datenschutzrechts. Außerdem wurden die Rechtsgrundlagen für die Datenverarbeitung durch öffentliche Stellen beleuchtet.

In diesem zweiten Teil werden kurz die Rechte der Betroffenen vorgestellt und einige der organisatorischen Vorgaben genannt. Abschließend wird ein Blick auf die Befugnisse der Aufsichtsbehörden und die dagegen möglichen Rechtsmittel geworfen.

Im ersten Teil wurde schon erwähnt, dass der Rechtsanwender den Blick zwischen der DSGVO und dem nationalen Recht, welches die Öffnungsklauseln ausfüllt, hin und her wandern lassen muss. Für die Kommunen in Schleswig-Holstein finden sich die wichtigsten Vorschriften des nationalen Rechts im neuen Landesdatenschutzgesetz (LDSG), das zum Zeitpunkt der Abfassung des ersten Teils noch nicht verkündet worden war. Es kann nun vermeldet werden, dass das *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 2. Mai 2018* im Gesetz- und Verordnungsblatt für Schleswig-Holstein, Ausgabe 8/2018 vom 17. Mai 20, S. 162, veröffentlicht wurde (uldsh.de/ldsg). Es trat mit der DSGVO zusammen am 25. Mai in Kraft. In Artikel 1 des Gesetzes findet sich das neue LDSG. Artikel 2 ist das Gesetz zur Errichtung eines Unabhängigen Landeszentrums für Datenschutz. In den insgesamt 41 Artikeln werden weitere Fachgesetze an die DSGVO angepasst. Im Folgenden sind alle zitierten Artikel solche der DSGVO, soweit nicht andere Rechtsquellen ausdrücklich genannt werden.

1. Rechte der Betroffenen

Die meisten der Betroffenenrechte sind im Grunde alte Bekannte; sie gab es schon in der Richtlinie 95/46/EG und den dazu erlassenen nationalen Vorschriften. Einige wenige Rechte sind neu hinzugekommen. Die Rechte der Betroffenen selbst ergeben sich aus der DSGVO direkt. Allerdings erlaubt eine Öffnungsklausel in Art. 23 dem nationalen Gesetzgeber, die Rechte für bestimmte Zwecke einzuschränken. Daher muss, wie schon erwähnt, auch hier der Blick des Rechtsanwenders zwischen den Art. 12 bis 22, die die Rechte selbst enthalten, und den §§ 8 bis 11 LDSG mit den Einschränkungen hin und her schweifen.

Es kann hier nicht auf alle Rechte im Detail eingegangen werden. Von Bedeutung ist zunächst Art. 12, der selbst kein Recht enthält, sondern die Modalitäten bei der Ausübung der Rechte behandelt. Nach Abs. 1 der Vorschrift hat der Verantwortliche geeignete Maßnahmen zu treffen, um den Verpflichtungen in diesem Kapitel der DSGVO nachkommen zu können. Diese Maßnahmen sollten Bestandteile eines Datenschutz-Managementsystems sein, bei dem durch Zuweisung von Aufgaben und Festlegung von Verfahren im Voraus definiert wird, wie z.B. mit Auskunftsersuchen der Betroffenen umgegangen wird. Art. 12 verlangt weiter, dass den Betroffenen alle Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ übermittelt werden. Diese Vorgabe steht in einem gewissen Spannungsverhältnis zu den z.T. recht detailliert beschriebenen Pflichtinformationen nach Art. 13 und Art. 14, dazu sogleich. Es besteht keine Pflicht, die Informationen in einer anderen als der Landessprache des jeweiligen Mitgliedstaats zur Verfügung zu stellen.

Machen die Betroffenen ihre Rechte gegenüber dem Verantwortlichen geltend, so gilt neuerdings eine Frist von einem Monat, innerhalb der der Verantwortliche regieren muss (Art. 12 Abs. 3). Bei Komplexität der Angelegenheit oder bei einer großen Zahl von Anträgen kann der Verantwortliche dem Betroffenen mitteilen, dass er die Frist auf weitere zwei Monate verlängern möchte.

Alle Informationen und Mitteilungen im Kontext der Ausübung der Rechte der Betroffenen werden unentgeltlich zu Verfügung gestellt. Nur bei offenkundig unbegründeten oder exzessiven Anträgen kann der Verantwortliche doch ein Entgelt verlangen oder den Antrag ignorieren. Die Beweislast liegt aber beim Verantwortlichen, d.h. Exzessivität oder offenkundige Unbegründetheit sind zu dokumentieren.

An verschiedenen Stellen in Art. 12 wird deutlich, dass der Verantwortliche die Pflicht hat, die Identität des Antragstellers zu prüfen, bevor er dem Antrag nachkommt. Das ist in der Praxis vor allem bei der Wahrnehmung des Auskunftsrechts von Bedeutung. Hier genügt es keinesfalls, dass die Anfrage per E-Mail mit einer namentlich passenden E-Mail-Adresse gesendet wurde. In der Regel wird die Vorlage des Personalausweises oder eine Kopie desselben als ausreichender Nachweis der Identität angesehen werden können. Ausweiskopien sollten nicht gespeichert werden; vielmehr genügt ein Aktenvermerk mit dem Inhalt, dass die Ausweiskopie vorgelegen hat und die Identität geprüft wurde.

„Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch.“ (Art. 12 Abs. 1 Satz 2). Wegen der bekannten Vertraulichkeitsprobleme bei E-Mails kommt jedoch z.B. die Übersendung eines Auszugs aller gespeicherten Daten an den Betroffenen nur per verschlüsselte E-Mail in Betracht. Reine Verfahrensmitteilungen, wie z.B. die Verlängerung der Bearbeitungsfrist, können auch durch einfache E-Mail versendet werden.

Das Recht, das derzeit wohl am meisten im Fokus steht, ist in der DSGVO als Pflicht des Verantwortlichen formuliert: die Pflicht zur Information des Betroffenen. Diese ergibt sich in zwei Ausprägungen: Art. 13 enthält die Pflicht zur Information im Falle der Erhebung beim Betroffenen, Art. 14 die Informationspflicht, wenn die Daten bei Dritten erhoben werden. Diese Informationspflichten waren schon in der Vorläufervorschrift, der Richtlinie 95/46/EG, enthalten und durch § 26 LDSG-alt in Landesrecht umgesetzt worden. Zwar erweitert die DSGVO den Katalog der Angaben, die dem Betroffenen zur Verfügung gestellt werden müssen. Gleichwohl überrascht die Aufregung, die jetzt durch die vermeintlich neuen Informationspflichten hervorgerufen wird.

Art. 13 wie auch Art. 14 teilen die Informationen, die den Betroffenen zu geben sind, jeweils zwischen Absatz 1 und Absatz 2 auf, wobei nach „Absatz 2 folgende weitere Informationen zur

Verfügung (gestellt werden), die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten“. Die Gelehrten rätseln noch, was das bedeuten soll. Denn unbestritten dienen die Angaben nach dem jeweiligen Absatz 1 auch der Transparenz. Für die praktische Umsetzung ist zu empfehlen, stets alle Angaben nach Absatz 1 und 2 zu machen, jedenfalls soweit einschlägig. Gibt es z.B. keine automatisierte Entscheidungsfindung, so entfällt natürlich die Information nach Art. 13 Abs. 2 Buchstabe f). Weiterhin fällt auf, dass es in Art. 13 Abs. 1 und in Art. 14 Abs. 1 heißt, der Verantwortliche „teilt mit“, während im jeweiligen Absatz 2 nur verlangt wird, dass der Verantwortliche die Informationen „zur Verfügung stellt“. Hierbei handelt es sich jedoch um einen Übersetzungsfehler. In der englischen und der französischen Sprachfassung wird jeweils in Absatz 1 und Absatz 2 derselbe Begriff verwendet (im Englischen: „to provide“, dass dem „zur Verfügung stellen“ entspricht). Alle Informationen müssen also nur zur Verfügung gestellt werden.

Für die Praxis ist bedeutsam, wie dieses Zur-Verfügung-Stellen konkret aussehen muss. Dabei geht es vor allem in Art. 13 auch um das Wann. Der Wortlaut spricht vom „Zeitpunkt der Erhebung dieser Daten“. Die Datenschutz-Aufsichtsbehörden sind Befürchtungen entgegengetreten, dass nun z.B. schon im Vorwege telefonischer Kontaktaufnahme den Anrufern zunächst die Pflichtinformationen vorgelesen werden müssten. Das ULD gibt Hinweise zur Umsetzung in Heft 4 der Praxis-Reihe (abzurufen unter uldsh.de/dsgvo). So empfiehlt es sich bei der Gestaltung von Formularen, die Pflichtinformationen in diesen unterzubringen. Hier kann auch auf das bewährte Konzept der gestuften Datenschutzinformation zurückgegriffen werden. Das Formular kann erste Informationen in der geforderten einfachen Sprache enthalten, für weitere, detailliertere Angaben aber z.B. auf die Homepage der Organisation verweisen. Nicht ausreichend wäre es, zwar Informationsblätter mit den Pflichtangaben vorzuhalten, diese aber erst auf Nachfrage herauszugeben. Denn der Verantwortliche hat die Pflicht, die Angaben zur Verfügung zu stellen. Dazu gehört, dass zumindest ein Hinweis auf diese Angaben dem Betroffenen „aufgedrängt“ wird, z.B. durch ein gut lesbares Hinweisschild auf dem Tresen des Bürgerbüros. Nur so werden die Informationen auch denjenigen zur Verfügung gestellt, die nicht wissen, wonach sie fragen sollen.

Werden die Daten nicht beim Betroffenen, sondern bei einem Dritten erhoben, so kommt die Informationspflicht nach Art. 14 zu Anwendung. Hier ist zusätzlich zu den Pflichtangaben nach Art. 13 auch die Information erforderlich, welche Kategorien von Daten verarbeitet werden und aus welcher Quelle die Daten stammen. Der Zeitpunkt der Information ist hier fallweise gestuft: die Information ist fällig spätestens einen Monat nach Erhebung. Kommt es zuvor zu einer Übermittlung, dann muss zum Zeitpunkt der Übermittlung der Betroffene informiert werden. Sollen die Daten vor Ablauf der Monatsfrist für eine Kommunikation mit dem Betroffenem verwendet werden (also z.B. zur Anhörung im Verwaltungsverfahren, § 87 LVwG), so muss die Pflichtinformation zusammen mit dieser Kommunikation erfolgen.

Bei Art. 13 und Art. 14 entfällt die Mitteilungspflicht, wenn und soweit der Betroffene schon über die Information verfügt. Dass dies der Fall ist, muss im Zweifel durch den Verantwortlichen nachgewiesen werden. Nach Art. 14 Abs. 5 Buchstaben b)-c) entfällt die Mitteilungspflicht außerdem, wenn sie unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert (z.B., wenn die Kommunikationsdaten nicht bekannt und nur sehr aufwendig zur ermitteln sind), wenn die Datenerhebung ausdrücklich gesetzlich geregelt ist oder wenn die Daten einem Berufsgeheimnis unterliegen. Gerade der Fall des Buchstaben c) (Erhebung bzw. Übermittlung ist durch Rechtsvorschrift vorgesehen, die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht) ist im öffentlichen Bereich die Regel. So handelt es sich z.B. bei Abrufen von Daten aus dem Melderegister um Erhebung bei Dritten im Sinne von Art. 14. Sind diese Abrufe speziell im Gesetz geregelt, so entfällt die Informationspflicht. Ein Beispiel

ist die Übermittlung von bestimmten Daten aus den Melderegistern an das Landesamt für soziale Dienste zur Erfüllung von dessen Aufgaben nach § 6 Landesmeldegesetz. Hier ist die Übermittlung von Daten für bestimmte Aufgaben vorgesehen. Daher muss das LAsD keine Mitteilung nach Art. 14 machen.

Zum Auskunftsrecht nach Art. 15 sei außer der oben angesprochenen Monatsfrist nur auf Folgendes hingewiesen: Inhalt des Rechts ist auch die Negativauskunft (es sind keine Daten über den Anfragenden gespeichert). Werden Daten über den Anfragenenden gespeichert, so sind die Angaben nach Abs. 1 und 2 zu machen. Von besonderer Bedeutung ist freilich die Kopie der gespeicherten Daten nach Abs. 3, die den eigentlichen Wesenskern der Auskunft ausmachen. Dabei ist die erste Kopie kostenfrei, für alle weiteren kann ein angemessenes Entgelt verlangt werden.

In Wahrnehmung der Öffnungsklausel in Art. 23 beschränkt das LDSG die Rechte aus Art. 13 bis 15 auch in anderen Fällen, z.B. für den Fall, dass die „Erteilung der Information die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes schwere Nachteile bereiten würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen“ oder dass „die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind“. Hieraus, sowie aus Art. 15 Abs. 4 ergibt sich, dass bei der Gewährung der Auskunft in der Regel die Daten Dritter, die mit den Daten des Antragstellers verbunden sind, zu schwärzen oder in anderer Weise unkenntlich zu machen sind. Dies betrifft insbesondere die Daten von Behördeninformanten, wie das Bundesverwaltungsgericht in ständiger Rechtsprechung urteilt (BVerwG, Urteil vom 04.09.2003, 5 C 48/02).

Das dem Namen nach neue „Recht auf Vergessenwerden“ (Art. 17) entspricht dem bisherigen Recht auf Löschung, wenn die Daten nicht länger benötigt werden. Neu dabei ist die Pflicht des Verantwortlichen bei Daten, die er (im Internet) veröffentlicht hat, anlässlich der Löschung im eigenen System darauf hinzuwirken, dass diese Daten auch in Systemen anderer Verantwortlicher gelöscht werden und von Suchmaschinen nicht mehr angeboten werden. Wegen des offenen Wortlauts herrscht noch einige Unklarheit über den genauen Inhalt des Rechts nach Art. 17 Abs. 2.

Ein weiteres neues Betroffenenrecht ist das Recht auf Datenübertragbarkeit (Art. 20). Dieses ist jedoch beschränkt auf Verarbeitungen, die auf der Grundlage einer Einwilligung oder eines Vertrages stattfinden und dürfte daher im öffentlichen Bereich kaum relevant werden (außer freilich bei den Beschäftigtendaten).

2. Organisatorische Vorgaben

Im Kapitel IV der DSGVO findet sich sodann eine Reihe von organisatorischen Vorgaben, von denen einige im Folgenden beleuchtet werden sollen.

Art. 24 Abs. 1 verpflichtet den Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Umsetzung der Vorgaben der DSGVO sicherzustellen und auch den Nachweis hierüber zu erbringen. Letztlich beinhaltet dies die Pflicht, ein Datenschutz-Managementsystem zu installieren, siehe oben zu Art. 12. Aus Art. 24 zusammen mit Art. 5 Abs. 2 ergibt sich auch die Pflicht zur Dokumentation der getroffenen Maßnahmen, dazu sogleich mehr.

Nach Art. 25 hat der Verantwortliche für „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ zu sorgen. Namentlich der erste Aspekt, geregelt in Abs. 1 der Vorschrift und meist englisch als „Privacy by Design“ bezeichnet, kann im öffentlichen Bereich eine Rolle spielen, und zwar bei Beschaffungsentscheidungen. Dabei müssen Grundsätze wie der der Datenminimierung bereits bei Ausschreibungen in das Pflichtenheft aufgenommen werden. Bei vergleichbarer Preisgestaltung ist das datenschutzfreundlichere Produkt zu beschaffen.

Wegen der erheblichen praktischen Bedeutung sei auf Art. 30 hingewiesen, der die Verantwortlichen verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Diese Pflicht trifft unabhängig vom Verantwortlichen nun auch den Auftragsverarbeiter. Es gilt nicht mehr nur für automatisierte Verfahren, sondern auch für Aktenbestände in Papierform. Anders als das frühere Verfahrensverzeichnis nach § 7 LDSG-alt gibt es keinen allgemeinen Anspruch auf Einsicht in das Verzeichnis unmittelbar aus den datenschutzrechtlichen Vorschriften. Allerdings wird meist ein Antrag nach dem Informationszugangsgesetz zu identischen Ergebnissen führen. Wie oben erwähnt bringt die DSGVO mit der Pflicht, die Einhaltung der Vorschriften nachweisen zu können, zusätzliche Dokumentationspflichten mit sich. Das ULD hat hierzu eine Hilfestellung veröffentlicht, die es ermöglichen soll, eine vollständige Dokumentation zu erstellen (uldsh.de/doku). Dabei sind mehr Angaben erforderlich als nach Art. 30 für das Verzeichnis der Verarbeitungstätigkeiten gefordert. So kann die Rechtmäßigkeit der Verarbeitung nur nachgewiesen werden, wenn auch die Rechtsgrundlage für die Verarbeitung dokumentiert wird – eine Angabe, die in Art. 30 nicht genannt wird, aber in dem Muster des ULD enthalten ist. Bereits bisher bestand für öffentliche Stellen nach der Schleswig-Holsteinischen Datenschutzverordnung (DSVO) eine recht weitgehende Dokumentationspflicht. Stellen, die diese Vorgaben eingehalten haben, werden es leichter haben, den Dokumentationsanforderungen der DSGVO zu genügen. Die DSVO gilt als Landesverordnung bis Ende 2018; es ist zu erwarten, dass eine Nachfolge-Vorschrift auf der Ermächtigungsgrundlage in § 7 Abs. 2 LDSG-neu erlassen wird.

Art. 32 ist die zentrale Vorschrift zur Datensicherheit in der DSGVO. Allerdings sind die Anforderungen wenig konkret und fallen insoweit hinter die Regelungen in den §§ 5 und 6 LDSG-alt und in der Anlage zu § 9 BDSG-alt zurück. Die in der Vorschrift genannten Maßnahmen, die unter Berücksichtigung des Risikos und anderer Faktoren eingesetzt werden sollen, stellen ein Mischung aus konkreten Technologien, Schutzzielen und Verfahren dar, die in jedem Fall weiter spezifiziert werden müssen. Erfreulich ist in diesem Zusammenhang, dass der Landesgesetzgeber das bewährte Konzept von Test und Freigabe (bisher § 7 Abs. 2 LDSG-alt) in § 7 Abs. 1 LDSG-neu übernommen hat. Wie schon erwähnt gilt das auch für die dazu erlassene Landesverordnung, die im Detail regelt, wie der Einsatz von Informationstechnik, die Sicherheitsmaßnahmen und das Vorgehen bei Test und Freigabe zu dokumentieren sind.

Nach Art. 37 Abs. 1 Buchstabe a) haben alle Behörden und öffentlichen Stellen die Pflicht, einen behördlichen Datenschutzbeauftragten (DSB) zu benennen. Aus welchem Grund die DSGVO hier von der in Richtlinie 95/46/EG eingeführten Begrifflichkeit abweicht bleibt unklar. Jedenfalls hat der neue Begriff „benennen“ keine andere Bedeutung als der bisher in § 10 LDSG-alt verwendete Begriff „bestellen“.

Die Pflicht trifft alle Kommunen und die von ihnen gründeten Zweckverbände. Eigenbetriebe und andere rechtlich unselbständigen Einrichtungen zählen als Teil der Kommune. Ein von der Kommune bestellter DSB ist daher auch für den Eigenbetrieb etc. zuständig. Hat die Gemeinde ihre Aufgaben vollständig auf eine Amtsverwaltung übertragen, so ist die Gemeinde nicht mehr Verantwortlicher, wenn sie selbst keine personenbezogenen Daten mehr verarbeitet. Bleiben Teile der Aufgaben bei der amtsangehörigen Gemeinde oder hat die Gemeinde zwar alle Ver-

waltungsaufgaben übertragen, aber einen Eigenbetrieb eingerichtet, der personenbezogene Daten verarbeitet (z.B. der Kurbetrieb bei der Erhebung der Kurabgabe), so bleibt die Gemeinde insoweit Verantwortlicher und unterliegt der Pflicht zur Bestellung eines DSB. Werden Aufgaben auf privatrechtlich konstituierte Träger (z.B. den Kommunen gehörende GmbHs) ausgelagert, so richtet sich die Bestellung einer DSB bei diesen Stellen nach dem Bundesdatenschutzgesetz. Die Benennung erfolgt mit einem formlosen Schreiben, das vom DSB gegengezeichnet werden sollte.

Für die Position kommen neben eigenem Personal auch externe DSB in Betracht. Die DSGVO sieht auch vor, dass öffentlichen Stellen einen gemeinsamen DSB benennen können. Soweit Kreise und kreisangehörige Kommunen dies vorhaben, wird in der Regel ein Vorgehen nach § 19a KGZ gewählt. Bei der gemeinsamen Bestellung müssen Organisationsstruktur und Größe der beteiligten Stellen berücksichtigt werden (Art. 37 Abs. 3). In der Praxis bedeutet das vor allem, dass ein realistischer Personalschlüssel zugrunde gelegt wird. Die Bundesbeauftragte für den Datenschutz hat im Hinblick auf die Bundesverwaltung die Einhaltung des Verhältnisses von 1000 Beschäftigen auf eine Vollzeitstelle eines DSB angemahnt. Vor diesem Hintergrund geht das ULD derzeit davon aus, dass auch bei Kommunen eine Obergrenze von 1000 Beschäftigten pro Vollzeitstelle eines DSB gilt. Tatsächlich ließe sich auch eine geringere Beschäftigtenzahl pro volle DSB-Stelle rechtfertigen. Denn die behördlichen DSB bei den Bundesministerien, für die die Vorgabe der Bundesbeauftragten gemacht wurde, betreuen Stellen mit einer homogenen Organisations- und IT-Struktur, die zudem relative wenige Daten der Bürger verarbeiten. Das Gegenteil gilt für die Betreuung einer Vielzahl von Kommunen: Hier finden sich unterschiedliche Organisationsstrukturen und IT-Systeme und dazu eine große Zahl von Daten der Bürger. Konkret bedeutet die genannte Vorgabe z.B. Folgendes: Hat ein Kreis ca. 700 Mitarbeiter, so dürfen die von dem gemeinsam bestellten DSB betreuten Kommunen und Zweckverbände nicht mehr als 300 Mitarbeiter haben. Wird diese Anzahl überschritten, ist die Schaffung einer weiteren (ggfs. anteilsmäßigen) Stelle erforderlich. Bei kleineren öffentlichen Stellen kann der DSB auch mit anderen Aufgaben betraut werden. Diese dürfen jedoch nicht zu einem Interessenkonflikt führen. Damit scheidet die Benennung von leitenden Mitarbeitern der öffentlichen Stelle oder auch der Leitung der IT-Abteilung aus.

Wichtig ist, dass der DSB die notwendige Fachkunde im Datenschutzrecht und in der Praxis besitzt oder sich diese zumindest in kurzer Zeit verschafft. Die DATENSCHUTZAKADEMIE SH bietet Fortbildungen an (siehe: uldsh.de/dsa).

Die Kontaktdaten der DSB sind zu veröffentlichen und der zuständigen Aufsichtsbehörde mitzuteilen. Das ULD stellt hierfür unter uldsh.de/dsb-meld ein Meldeportal zur Verfügung.

Der DSB muss als Stabstellenfunktion eingerichtet sein, die unmittelbar der Leitung der jeweiligen Stelle zugeordnet ist. Der DSB ist in der Ausübung seiner Funktion unabhängig, Anweisungen bezüglich der Ausübung der Aufgaben dürfen nicht erteilt werden. Den DSB müssen die notwendigen Ressourcen zur Verfügung gestellt werden. Dazu gehört, dass die öffentliche Stelle

- ein Einzelbüro zur Nutzung zur Verfügung stellt, um dem DSB die Wahrung der Vertraulichkeit bei der Ausübung der Aufgabe zu ermöglichen;
- eine eigene E-Mail-Adresse einrichtet, die im alleinigen Zugriff des DSB liegt;
- Fortbildungen ermöglicht und finanziert;
- die Teilnahme an Sitzungen mit anderen DSB ermöglicht und Reisekosten übernimmt.

Der DSB muss frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden. Konkret bedeutet dies, dass die Leitung der öffentlichen Stelle den DSB über jeden geplanten neuen Einsatz von IT-Verfahren oder über relevante Änderungen an bestehenden Verfahren informiert. Dies betrifft sowohl die Verarbeitung der personenbezogenen Daten von Bürgerinnen und Bürgern als auch die Verarbeitung von Beschäftigtendaten. Die Betroffenen können sich in allen Fragen der Datenverarbeitung direkt an den DSB wenden. Der DSB ist zum Stillschweigen über die Sachverhalte verpflichtet, die im in dieser Eigenschaft bekannt werden.

Zu den Aufgaben des DSB gehören die Beratung der öffentlichen Stelle und die Schulung der Mitarbeiter sowie die Kontrolle der Einhaltung der Vorschriften über den Datenschutz. Für die Aufsichtsbehörde (dazu sogleich) dient er als Kontaktperson. Es ist wichtig zu betonen, dass der DSB keinesfalls selbst die Verantwortung für die Datenverarbeitung trägt. Diese verbleibt bei der Leitung der öffentlichen Stelle.

Aufsichtsbehörde

Art. 51 verpflichtet die Mitgliedstaaten, unabhängige Datenschutz-Aufsichtsbehörden zu installieren. In § 17 bestimmt das neue LDSG dazu, dass die oder der Landesbeauftragte für Datenschutz in Schleswig-Holstein die Aufsichtsbehörde nach Art. 51 ist. Dies stellt eine Änderung gegenüber der bisherigen Rechtslage dar, wonach das Unabhängige Landeszentrum für Datenschutz (ULD) die Aufsichtsbehörde war. Ein substantieller Wandel ist damit jedoch nicht verbunden. Das im Jahr 2000 als rechtsfähige Anstalt des öffentlichen Rechts konstituierte ULD bleibt bestehen, wobei die Vorschriften über die Errichtung des ULD in ein separates „Gesetz zur Errichtung eines Unabhängigen Landeszentrums für Datenschutz“ (Errichtungsgesetz ULD) ausgelagert wurden. Das ULD ist jetzt sozusagen das Büro der Landesbeauftragten und diese dessen Leiterin. Verwaltungsakte werden von der Landesbeauftragten erlassen, während das ULD z.B. die Verträge mit seinen Mitarbeitern schließt und der Dienstherr seiner Beamten ist. Von Interesse ist hier vielleicht noch, dass die Dauer einer Amtszeit der Landesbeauftragten von fünf auf sechs Jahre und damit auf den Zeitraum von vor 2000 angehoben wurde. Erst vor nicht allzu langer Zeit hatte der Landtag in der sog. „Lex Weichert“ (GVBl. 2014, 105) auch beschlossen, die Sperre der mehr als einmaligen Wiederwahl der oder des Landesbeauftragten aufzuheben. Nun hat der Gesetzgeber seine Meinung wieder geändert und erlaubt erneut nur eine Wiederwahl des Amtsinhabers.

Die Aufgaben und Befugnisse der Datenschutz-Aufsichtsbehörden sind in Art. 57 und Art. 58 geregelt. Von Interesse sind hier vor allem die Untersuchungsbefugnisse nach Art. 58 Abs. 1 und die sog. Abhilfebefugnisse nach Art. 58 Abs. 2. Die Untersuchungsbefugnisse entsprechen im Wesentlichen den bisher in den §§ 39 bis 41 LDSG-alt geregelten Befugnissen. Dazu gehört, Auskunft verlangen zu können, Prüfungen durchzuführen und Zugang zu allen relevanten Daten zu erhalten. Ergänzend regelt § 18 LDSG-neu (wie bisher § 41 LDSG-alt), dass die öffentlichen Stellen die Landesbeauftragte und ihre Beschäftigen bei der Ausübung ihrer Aufgaben zu unterstützen haben. Insbesondere ist Auskunft zu erteilen sowie Zutritt zu Dienst- und Geschäftsräumen und Einsicht in Unterlagen und Daten zu gewähren.

Neu ist allerdings die Qualität der in Art. 58 Abs. 2 enthaltenen Abhilfebefugnisse. Bisher war die schärfste Waffe gegenüber öffentlichen Stellen die Beanstandung. Dies war der Qualität nach eine schriftliche Rüge, die keine direkten Wirkungen hatte, und auch nicht vor Gericht angegriffen werden konnte (OVG Schleswig, Urteil vom 16.09.1991, 1 L 18/91). Nun stehen neben der Warnung (Hinweis auf zukünftig eintretende Rechtswidrigkeit) als aufsichtsbehördliche Mit-

tel auch die Verwarnung, Anordnungen und sogar das Verbot der Datenverarbeitung zur Verfügung. Bei den beiden letzten handelt es sich um die Befugnis, entsprechende Verwaltungsakte gegenüber öffentlichen Stellen zu erlassen. Zwar hat die Verwarnung (wie die frühere Beanstandung) keinen Regelungsgehalt. Sie wird allerdings als feststellender Verwaltungsakt angesehen. Durch EU-Recht, das – wie im 1. Teil des Beitrags angedeutet wurde – keine Rücksicht auf Befindlichkeiten im mitgliedstaatlichen Verwaltungsrecht nimmt, ist also die ungewöhnliche Situation eingetreten, dass die Landesbeauftragte als eine Behörde des Landes gegenüber anderen Behörden Verwaltungsakte erlassen kann.

Nach Art. 78 hat jeder Adressat von aufsichtsbehördlichen Maßnahmen das Recht auf einen wirksamen gerichtlichen Rechtsbehelf. Während sich dies nach deutschen Verfassungsrecht für Privatrechtssubjekte schon aus Art. 19 Abs. 4 GG und für Kommunen im Bereich der kommunalen Selbstverwaltung aus Art. 28 Abs. 2 GG ergibt, eröffnet Art. 78 nun auch allen anderen Behörden und öffentlichen Stellen die Möglichkeit, Rechtsschutz gegen Maßnahmen der Aufsichtsbehörde zu suchen. Ergänzend regelt § 20 BDSG dazu, dass ein Vorverfahren (mangels Devolutiveffekt) nicht stattfindet und dass die Verwaltungsgerichte für die Streitigkeit zuständig sind. Weiterhin ist geregelt, dass die Aufsichtsbehörde nicht die sofortige Vollziehung gegenüber einer Behörde anordnen darf. Ein größeres Problem bei der Durchsetzung der Verwaltungsakte der Aufsichtsbehörde ist allerdings, dass diese gegenüber öffentlichen Stellen nicht vollstreckbar sind. Dazu hätte es wegen § 234 LVwG einer Rechtsvorschrift bedurft, die den Vollzug gegen Träger der öffentlichen Verwaltung erlaubt. An einer solchen Norm fehlt es aber. Es bleibt abzuwarten, wie sich die Durchsetzung der Aufsichtsbefugnisse gegenüber Kommunen und anderen öffentliche Stellen unter der neuen Rechtslage in der Praxis gestaltet.

Im Grundsatz besteht nach Art. 83 für die Datenschutzaufsichtsbehörden auch die Möglichkeit, Bußgelder zu verhängen. Adressat der Geldbuße ist dabei der Verantwortliche als Organisation (also in der Regel als juristische Person) Vor allem die exorbitante Höhe möglicher Geldstrafen (bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes) hat dazu beigetragen, dass die DSGVO ins Gespräch kam. Im Grundsatz können Bußgelder gegen alle Arten von Verantwortlichen verhängt werden. Allerdings findet sich in Art. 83 Abs. 7 eine Öffnungsklausel, die es Mitgliedstaaten erlaubt, Behörden und öffentliche Stellen von Bußgeldern auszunehmen. § 19 Abs. 1 LDSG-neu nimmt die Öffnungsklausel wahr und schließt Bußgelder gegen öffentliche Stellen in Schleswig-Holstein aus. Entsprechend Regelungen finden sich im BDSG und in allen neuen Landesdatenschutzgesetzen. Bisher fand sich in § 44 LDSG-alt noch die Befugnis, Bußgelder gegen Individuen wegen Verstößen gegen das Datenschutzrecht zu erlassen. Dies betraf vor allem Situation, in denen Beschäftigte öffentlicher Stellen ihren Zugang zu Datenbeständen für private Zwecke nutzten. Eine solche Vorschrift fehlt im neuen LDSG; stattdessen gibt es dort eine Strafvorschrift, die in solchen Fällen greifen kann. Diese verlangt allerdings, dass der Täter gegen Entgelt oder in der Absicht gehandelt hat, sich oder einen anderen zu bereichern oder einen anderen zu schädigen. Nach Auffassung des Gesetzgebers war kein Raum für eine Vorschrift wie die frühere, niedrigschwellige Bußgeldnorm, weil keine Öffnungsklausel in der DSGVO zur Verfügung stand. Dies wurde allerdings von anderen Landesgesetzgebern anders gesehen. Es ist allerdings denkbar, dass Verstöße durch Mitarbeiter öffentlicher Stellen künftig gleichwohl verfolgt werden, indem der Täter selbst als Verantwortlicher angesehen wird, der die Daten in unzulässiger Weise verarbeitet.

Abschließend soll noch darauf hingewiesen werden, dass hier aus Platzründen nur ein Teil der Aspekte angesprochen werden konnte, die für Kommunen und andere öffentliche Stellen relevant werden können. Nicht erwähnt werden konnten z.B. die Meldung von Datenschutzverletzungen nach Art. 33 und 34 sowie die eventuell erforderlich werdende Datenschutz-Folgenabschätzung. Hierzu sowie zu vielen anderen Fragen rund um die Umsetzung der DSG-

VO finden sich Hinweise und Muster auf der Homepage des ULD (uldsh.de/dsgvo). Hier sind auch die sog. Kurzpapiere abrufbar, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu einzelnen Themen rund um die DSGVO zusammengestellt hat.

Lukas Gundermann, LL.M. (Edinburgh)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein