Datenschutzreform 2018 – Auswirkungen auf die kommunale Praxis

Dr. Dominik Lück, Potsdam*

Am 25.5.2018 endet die zweijährige Vorbereitungsfrist, die Unternehmen und öffentliche Institutionen für die Vorbereitung auf das neue Datenschutzrecht haben. Dann gilt die Datenschutzgrundverordnung (DSGVO) europaweit, einheitlich und unmittelbar. Das „neue Datenschutzrecht" nach der DSGVO ist daher derzeit in aller Munde. In der kommunalen Praxis wird das Stichwort DSGVO, obwohl die Neuregelungen schon seit Mai 2016 bekannt sind, häufig noch immer als Schreckgespenst wahrgenommen. Diese Unsicherheit resultiert jedoch vielfach daraus, dass dem Führungs- und Fachpersonal von Gemeinden, Landkreisen und Zweckverbänden zwar der Bedeutungsgewinn des Datenschutzrechts insgesamt bewusst ist, die konkreten praktischen Auswirkungen der DSGVO für die tägliche Arbeit der Kommunalverwaltung aber nicht selten überhaupt nicht klar sind.

Der nachstehende Beitrag fasst deshalb die wesentlichen Änderungen, die die DSGVO für die kommunale Praxis mit sich bringt, zusammen und weist auf die Aufgaben hin, die bis zum Wirksamwerden der DSGVO, von den Kommunalverwaltungen umzusetzen sind.

* Der Autor ist Rechtsanwalt und Fachanwalt für Verwaltungsrecht in der Partnerschaft Dombert Rechtsanwälte mbB in Potsdam. Neben dem Kommunalrecht bildet das Datenschutzrecht einen Schwerpunkt seiner Tätigkeit. Herrn *Joshua Moir*, LL.B. dankt er für die umsichtige Unterstützung.

I. Zukünftiger datenschutzrechtlicher Regelungsrahmen

Die DSGVO wird am 25.5.2018[1, 2] ohne weitere Umsetzungsakte Bestandteil der deutschen Rechtsordnung[3]. Ihr kommt Anwendungsvorrang gegenüber dem nationalen Recht zu[4]. Soweit bestehendes deutsches Datenschutzrecht in Widerspruch zur DSGVO steht, darf es deshalb ab deren Geltungsbeginn nicht mehr zur Anwendung kommen. Es ist an die DSGVO anzupassen.

Die DSGVO verdrängt das nationale Datenschutzrecht aber nicht vollständig. Sie sieht zahlreiche Öffnungsklauseln vor, die dem nationalen Gesetzgeber einen Gestaltungsspielraum für abweichende Regelungen eröffnen, sofern sie inhaltlich

1 Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

2 Art. 99 II DSGVO.

3 Vgl. *Schaffland/Holthaus*, in: *Schaffland/Wiltfang*, DS-GVO, Lfg. 2/17, Synopse BDSG/DS-GVO, Kennzahl 0190.

4 *Sydow*, in: Europäische Datenschutzgrundverordnung, 2017, Einl. Rn. 36.

mit dem Schutzziel der Öffnungsklauseln übereinstimmen.[5] Die Mehrzahl der Öffnungsklauseln betreffen dabei die Datenverarbeitung durch öffentliche Stellen.[6]

Der Bundesgesetzgeber hat bereits reagiert. Er hat am 30.6.2017 ein neues Bundesdatenschutzgesetz beschlossen, das zum Geltungsbeginn der DSGVO am 25.5.2018 in Kraft treten wird.[7] Auch die Mehrzahl der Länder hat zwischenzeitlich Entwürfe an die DSGVO angepasster Landesdatenschutzgesetze vorgelegt.[8]

Für die kommunale Praxis zeigt sich dabei bereits jetzt eines deutlich: Das Datenschutzrecht wird unübersichtlicher. Der Vollharmonisierungsanspruch der DSGVO[9] ist im öffentlichen Bereich vor dem Hintergrund entsprechender Abweichungen durch die Landesgesetze eingeschränkt. Zukünftig werden von öffentlichen Stellen immer die DSGVO und die jeweiligen Landesdatenschutzgesetze parallel herangezogen werden müssen. Denn die Landesgesetzgeber machen von den Gestaltungsmöglichkeiten durch die Öffnungsklauseln, angesichts der vorliegenden Entwürfe, umfassend Gebrauch.

III. Neuerungen nach der DSGVO

Für das deutsche Datenschutzrecht stellen die durch die DSGVO hervorgerufenen Änderungen eine Evolution aber keine Revolution dar.

So erfasst etwa die Definition des zentralen Begriffs der personenbezogenen Daten nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wobei eine natürliche Person identifizierbar ist, die direkt oder indirekt, insbesondere mittels Zuordnung zu Identifizierungsmerkmalen identifiziert werden kann und entspricht damit dem gängigen Begriffsverständnis des deutschen Datenschutzrechts.[10]

Auch die Tatsache, dass Art. 4 Nr. 2 DSGVO praktisch alle mögliche Nutzungsvorgänge zentral unter den Begriff der „Verarbeitung" fasst, stellt eine für die Praxis eher unbedeutende Änderung dar. Denn die Definition des nun auch unter den Begriff der Verarbeitung fallende Erheben und Nutzen personenbezogener Daten ändert sich dadurch nicht.[11]

1. Verantwortlicher, Art 4 Nr. 7 DSGVO

Eine für die kommunale Praxis wichtige Klarstellung ergibt sich hingegen aus dem Begriff des Verantwortlichen.

Der Verantwortliche ist Adressat der materiellen Regelungen der DSGVO. Er wird nach Art. 4 Nr. 7 DSGVO als „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet" definiert.

Für den Datenschutz in der Kommunalverwaltung ist insoweit entscheidend, dass die Behörde und nicht Abteilungen, Referate, Dezernate und Sachgebiete von Behörden als Verantwortliche benannt werden. Als verantwortliche Stelle für die Behörde handelt die Behördenleitung. Sie trägt damit die Verantwortung für den Datenschutz in ihrem Zuständigkeitsbereich[12] und nicht der einzelne Sachbearbeiter oder Referent.

2. Datenschutzbeauftragter, Art. 37 DSGVO

Änderungen ergeben sich auch in Bezug auf den Datenschutzbeauftragten.

a) Pflicht zu Bestellung

Während bislang eine Pflicht zur Benennung eines Datenschutzbeauftragten europarechtlich lediglich für öffentliche Stellen des Bundes sowie subsidiär für öffentliche Stellen der Länder gefordert war, ist nach Art. 37 I a DSGVO nun auf jeden Fall ein Datenschutzbeauftragter zu benennen, wenn die Datenverarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird.

Dies führt dazu, dass auch in den Ländern Sachsen und Schleswig-Holstein auf kommunaler Ebene nun zwingend ein Datenschutzbeauftragter zu bestellen ist[13].

b) Gemeinsame externe Datenschutzbeauftragte

Art. 37 DSGVO verlangt indes nicht, dass jede einzelne Behörde oder öffentliche Stelle über einen eigenen Datenschutzbeauftragten verfügt. Unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe können mehrere Behörden oder Stellen nach Art. 37 III DSGVO einen gemeinsamen Datenschutzbeauftragten benennen. Die bestehenden Voraussetzungen werden in der Praxis aber häufig ins Leere laufen, denn Behörden werden ohnehin nur dann einen gemeinsamen Datenschutzbeauftragten benennen, wenn sie gleiche oder ähnliche Aufgaben haben und deshalb bereits eng zusammenarbeiten[14].

Während eine gemeinsame Benennung eines Datenschutzbeauftragten durch mehrere Behörden oder Ämter derselben Organisationsstruktur schon bislang möglich war[15], ist es nach der Neuregelung des Art. 37 III, VI DSGVO auch zulässig, dass der Datenschutzbeauftragte seine Aufgaben auf Grundlage eines Dienstleistungsvertrages erfüllt[16]. Damit sind zukünftig

5 Bsp. für Öffnungsklausen sind: Art. 4 Nr.7, Art. 26 I, Art. 37 IV sowie Art. 83 VII DSGVO.
6 Vgl. *Kühling/Martini*, EuZW 2016, 448 (448) m.w.N.
7 BGBl. 2017 I S. 2132.
8 Entwürfe mit Stand vom 12.2.2018: Rheinland-Pfalz vom 23.1.2018, Thüringen vom 17.1.2018, Schleswig-Holstein vom 10.1.2018, Hessen vom 9.1.2018, Nordrhein-Westfalen vom 14.12.2017, Baden-Württemberg vom 14.12.2017, Bayern vom 12.12.2017, Sachsen vom 29.09.2017, Brandenburg vom 15.9.2017, Sachsen-Anhalt vom 15.8.2017 sowie Mecklenburg-Vorpommern (Referentenentwurf).
9 Erwägungsgrund Nr. 10 ff. VO (EU) 2016/679.
10 § 3 I BDSG.
11 *Ernst*, in: *Paal/Pauly*, DSGVO, 2. Aufl. (2018), Art. 4 Rn. 20.
12 Vgl. *Schild*, in: BeckOK DatenschutzR, DS-GVO, 22. Ed. 5/2017, Art. 4 Rn. 89; *Schaffland/Holthaus*, in: Schaffland/Wildfang, DSGVO, Lfg. 2/17, Art. 4 Rn. 150.
13 Bislang war gemäß § 11 I SächsDSG und § 10 LDSG S-H die Bestellung eines Datenschutzbeauftragten im kommunalen Bereich nicht zwingend. Anderes gilt aber bereits nach geltendem Recht gemäß § 7a I BbgDSG, § 19a I BlnDSG, § 10a I ThürDSG; § 20 I MVDSG; § 14a I SachsAnhDSG; § 8a NDSG.
14 *Schaffland/Holthaus* (o.Fußn. 12), Art. 37 Rn. 18.
15 So etwa § 4 f II 4 BDSG.
16 *Paal*, in: *Paal/Pauly*, DSGVO, 2. Aufl. (2018), Art. 37 Rn. 14.

sowohl gemeinsame interne als auch gemeinsame externe Datenschutzbeauftragte möglich[17].

Diese Alternative führt für die kommunale Praxis dazu, dass eine deutlich größere personelle Flexibilität als bislang besteht. Schließlich kann durch die Beauftragung eines externen Datenschutzbeauftragten die Überwachung der Einhaltung der DSGVO komplett ausgegliedert werden.

c) Eignung der Person des Datenschutzbeauftragten

Nach Art. 37 V DSGVO muss der Datenschutzbeauftragte eine ausreichende Qualifizierung für seine Tätigkeit vorweisen. Denn seine Benennung erfolgt auf Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt.

Jenseits dieser weichen Kriterien formuliert die DSGVO dagegen keine weiteren Anforderungen.[18] Damit ist weder die Ablegung einer gesonderten Prüfung noch die nachgewiesene Teilnahme an Schulungen ausdrückliche Voraussetzung für die Benennung einer Person als Datenschutzbeauftragter.

Anerkannt ist allerdings, dass nur Personen Datenschutzbeauftragter werden dürfen, die persönlich für die Aufgabe geeignet sind. Personen, die selbst in der Vergangenheit Daten missbraucht haben, scheiden deshalb von vornherein aus. Nicht zum Datenschutzbeauftragten bestellt werden dürfen auch Personen, die durch die Tätigkeit als Datenschutzbeauftragter in ihrer Arbeit beeinträchtigt würden.[19] Praktisch bedeutet dies, dass etwa Behördenleiter, Personalleiter, oder aber auch Leiter der IT-Abteilung auf Grund eines angenommenen Interessenkonfliktes mit ihrer Haupttätigkeit nicht zum Datenschutzbeauftragten bestellt werden können[20]. Entsprechende Zuwiderhandlungen sind bereits in der Vergangenheit mit Bußgeldern geahndet worden[21].

d) Stellung und Aufgaben des Datenschutzbeauftragten

Im Hinblick auf die Stellung des Datenschutzbeauftragten stellt Art. 38 I DSGVO ausdrücklich klar, dass er von der Behördenleitung ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden ist. Der Datenschutzbeauftragte ist darüber hinaus in Bezug auf die Ausübung seiner Aufgaben gegenüber der Behördenleitung ausdrücklich nicht weisungsgebunden, Art. 38 III 1 DSGVO.[22] Hierdurch sollen Datenschutzbeauftragte vor unbilligen Beeinflussungsversuchen der Behördenleitung geschützt werden, deren Interessen den Zielen eines umfassenden Schutzes personenbezogener Daten zuwiderlaufen könnten.[23]

Eine wesentliche Änderung ergibt sich in Bezug auf die Aufgaben des Datenschutzbeauftragten. Bislang war die Aufgabe des Datenschutzbeauftragten im BDSG und in den Landesdatenschutzgesetzen durch die Unterstützung der Behörde und ein Hinwirken auf die Einhaltung des Datenschutzes umschrieben.[24] Art. 39 I b DSGVO formuliert demgegenüber ausdrücklich, dass es Aufgabe des Datenschutzbeauftragten ist, die Einhaltung der DSGVO zu „überwachen".[25]

Die Überwachungspflicht schließt nach dem Wortlaut („einschließlich") von Art. 39 I b DSGVO die Zuweisung von Zuständigkeiten, die Sensibilisierung und Schulung der Verfahrensvorgänge beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen mit ein. Der Datenschutzbeauftragte hat damit die Befugnis, im Hinblick auf die Überwachung Zuständigkeiten im Rahmen des Überwachungsprozesses festzulegen und einzelnen Mitarbeitern zuzuweisen.[26] Für den Teilbereich des Datenschutzes ist der Datenschutzbeauftragte damit Mitarbeitern, die in der Behördenstruktur normalerweise ihm gegenüber weisungsbefugt sind, selbst weisungsbefugt.

Darüber hinaus hat der Datenschutzbeauftragte die Beschäftigten zu beraten, die Datenverarbeitungen vornehmen, Beratungen im Zusammenhang mit der Datenschutzfolgeabschätzung vorzunehmen und mit der zuständigen Aufsichtsbehörde zusammenzuarbeiten, Art. 39 I d DSGVO.

3. Einwilligung, Art. 6 I 1 a, Art. 4 Nr. 11 DSGVO

Auch nach der DSGVO bleibt die Verarbeitung personenbezogener Daten grundsätzlich unzulässig, wenn kein ausdrücklicher Erlaubnistatbestand besteht. Mögliche Erlaubnistatbestände werden von Art. 6 I DSGVO benannt. Die Öffnungsklausel des Art. 6 II DSGVO eröffnet den Ländern zu dem weiteren Spielraum.

Erhebliche praktische Bedeutung für zulässige Datenverarbeitungen hat die Einwilligung der betroffenen Person gemäß Art. 6 I 1 a DSGVO. Für Datenverarbeitungen von Kommunalverwaltungen ist diese Bedeutung aber eingeschränkt, denn nach der Definition des Art. 4 Nr. 11 DSGVO ist eine „Einwilligung der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist."

---

17 Vgl. nur BT-Dr 18/11325, S. 82 sowie *Paal* (o.Fußn. 16), Art. 37 Rn. 14.
18 Vgl. *von dem Busche*, in: *Plath*, BDSG/DSGVO, 2. Aufl. (2016), Art. 37 Rn. 11.
19 *Niklas/Faas*, NZA 2017, 1091.
20 Vgl. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Die Datenschutzbeauftragten in Behörde und Betrieb – Info 4, 12. Aufl. (2017), S. 15.
21 So im Fall eines Unternehmens in Bayern, das sich weigerte eine andere Person als den „IT-Manager" zum Datenschutzbeauftragten zu bestellen (vgl. Pressemitteilung des Bayerischen Landesamts für Datenschutzaufsicht vom 20.10.2016, online abrufbar unter URL: https://www.lda.bayern.de/media/pm2016_08.pdf, zuletzt abgerufen am 12.2.2018).
22 Nach Erwägungsgrund Nr. 97 VO (EU) 2016/679 sollen Datenschutzbeauftragte ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können. Das gleichlautend in der RL 95/46/EG enthaltene Erfordernis „völligen Unabhängigkeit" hat der EuGH zumindest in Bezug auf die staatlichen Datenschutzaufsichtsbehörden derart interpretiert, dass es jegliche Einflussnahme von außen, sei sie unmittelbar oder mittelbar verbiete, EuGH, MMR 2010, 352, weshalb *Moos*, in: BeckOK DatenschutzR, DS-GVO, 22. Edition, Stand: 1.5.2017, Art. 38 Rn. 10, davon ausgeht, dass dies auch im Hinblick auf Datenschutzbeauftragte gelten muss.
23 *Paal* (o.Fußn. 16), Art. 38 Rn. 9.
24 Vgl. etwa § 4 g I BDSG; § 14 a SachsAnhDSG; § 7a V BbgDSG; § 10a II ThürDSG; § 11 IV SächsDSG.
25 Denkbar ist daher, dass der Datenschutzbeauftragte damit auch als Überwachungsgarant im straf-und ordnungswidrigkeitenrechtlichen Sinne fungiert. So *Wybitul*, ZD, 2016, 203 (205); ablehnend zur früheren Rechtslage *Marschall*, ZD 2014, 66 (68).
26 *Paal* (o.Fußn. 16), Art. 39 Rn. 6a.

a) Voraussetzungen einer wirksamen Einwilligung

Zunächst setzt damit jede Einwilligung eine freiwillige Entscheidung des Betroffenen voraus. Nach der DSGVO kann eine Willensbekundung nur dann freiwillig sein, wenn die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einlegung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden".[27]

Grundsätzlich können deshalb auch Verarbeitungen durch öffentliche Stellen aufgrund einer Einwilligung rechtmäßig sein. Hier ist freilich das Merkmal der Freiwilligkeit besonders sorgfältig zu prüfen, denn öffentliche Stellen haben nicht selten durch ihre gesetzlichen Befugnisse die Möglichkeit, Rechtsverhältnisse mit den Bürgerinnen und Bürger einseitig zu regeln.[28]

Wirksam wird eine Einwilligung in der kommunalen Praxis deshalb immer nur in solchen Fällen sein, in denen der Betroffene eine echte Wahl hat, ob er der Verwaltung entsprechende personenbezogene Daten zur Verfügung stellt. Denkbar ist dies etwa im Hinblick auf die Veröffentlichung von Fotos aus Kindergärten oder bei der Veröffentlichung von Jubiläums- oder Standesamtsdaten in Gemeindebriefen oder Amtsblättern.

Soweit die Definition verlangt, dass die betroffene Person ihre Einwilligung „in informierter Weise" erteilt, setzt diese Anforderung voraus, dass die Person weiß, wer der Verantwortliche ist und für welchen Zweck ihre Daten verarbeitet werden sollen.[29] Sie muss wissen, dass und in welchem Umfang sie ihre Einwilligung erteilt.[30]

Vor dem Hintergrund des Zweckbindungsgrundsatzes nach Art. 5 I b DSGVO kann eine Einwilligung weiterhin nur „für einen oder mehrere bestimmte Zwecke" erteilt werden. Aus der Einwilligungserklärung muss damit ersichtlich sein, für welche Zwecke die personenbezogenen Daten eingesetzt werden sollen.

Ferner muss sich die Einwilligung auf eine bestimmte Verarbeitung von Daten beziehen. Blanko-Einwilligungen sind deshalb auch weiterhin nicht möglich.

Schließlich muss die betroffene Person die Einwilligung unmissverständlich zum Ausdruck gebracht haben. Dies kann in Form einer ausdrücklichen Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung erfolgen. Untätigkeit ist dabei keine unmissverständliche bestätigende Handlung.[31] In der Folge liegt bei elektronisch abgegebenen Einwilligungserklärungen eine eindeutige bestätigende Handlung vor, wenn die betroffene Person beim Besuch einer Internetseite selbst ein Kästchen auf einer Internetseite anklickt. Dagegen liegt keine eindeutige Erklärung vor, wenn das Kästchen bereits systemseitig angekreuzt ist und die betroffene Person das Kreuzchen nicht herausnimmt.[32]

b) Nachweispflicht

Anders als bislang im deutschen Datenschutzrecht üblich[33] fordert die DSGVO für die Einwilligung keine Schriftform. Jedoch muss gemäß Art. 7 I DSGVO der Verantwortliche nachweisen können, dass die betroffene Person eine Einwilligung erklärt hat. Diese Nachweispflicht führt damit dazu, dass in der Praxis auch ohne strikt vorgeschriebene Schriftform eine formularmäßige, schriftliche Einwilligung zu empfehlen ist.

c) Fortgeltung bisher erteilter Einwilligungen?

In der Praxis stellt sich die Frage, wie mit bereits erteilten Einwilligungen Betroffener nach dem 25.5.2018 umzugehen ist. Behalten Sie Gültigkeit, oder sind sie neu einzuholen?

Die DSGVO selbst stellt in Erwägungsgrund 171 klar, dass die Verantwortlichen in vielen Fällen die Verarbeitung aufgrund einer bereits vor Geltung der DSGVO eingeholten Einlegung fortsetzen können. Voraussetzung ist aber, dass die „Art der bereits erteilten Einwilligung" den Bedingungen der DSGVO entspricht.[34]

Als problematisch erweist sich insoweit, dass Art. 13 DSGVO umfassende Informationspflichten der betroffenen Person bei Erhebung von personenbezogenen Daten vorsieht, die so nach dem bisherigen deutschen Datenschutzrecht nicht galten, und damit auch nicht Bestandteil bestehender Einwilligungen sind. Allerdings haben für den Datenschutz im nicht-öffentlichen Bereich die deutschen Aufsichtsbehörden beschlossen,[35] dass die Pflichten des Art. 13 DSGVO für bisher erteilter Einwilligungen nicht erfüllt sein müssen, da sie keine Bedingungen im Sinne des Erwägungsgrund 171 darstellen.

Für Einwilligungen im öffentlichen Bereich kann nichts anderes gelten, weshalb bereits erteilte Einwilligungen regelmäßig wirksam bleiben dürften.

4. Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO

Auch im Hinblick auf die Dokumentation von Datenverarbeitungsvorgängen ergeben sich aus der DSGVO Änderungen, die von den Kommunalverwaltungen beachtet werden müssen.

Nach den bislang geltenden Landesdatenschutzgesetzen musste die datenverarbeitende Stelle für automatisierte Verarbeitungen ein Verfahrensverzeichnis führen.[36] Zukünftig haben Kommu-

27 Erwägungsgrund Nr. 5 der VO (EU) 2016/679.
28 Erwägungsgrund Nr. 43 der VO (EU) 2016/679, wonach die Einwilligung in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern können soll.
29 Die Frage nach der Informiertheit hat aktuell Bedeutung erlangt im Zusammenhang mit der Überprüfung der Privatsphäre- und Datenschutzeinstellungen von Facebook, LG Berlin, Urt. v. 16.1.2018 – 16 O 341/15.
30 Erwägungsgrund Nr. 42 der VO (EU) 2016/679.
31 Erwägungsgrund Nr. 32 der VO (EU) 2016/679.
32 Vgl. nur *Schild*, in: BeckOK DatenschutzR, DS-GVO, 22. Ed. 5/2017, Art. 4 Rn. 124.
33 Vgl. etwa § 4a I 3 BDSG; § 4 II BbgDSG; § 4 II SachsAnhDSG; § 8 I MVDSG; § 4 III ThürDSG.
34 in Erwägungsgrund Nr. 171 der VO (EU) 2016/679 heißt es insoweit: Beruhen die Verarbeitung auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihrer Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorstehenden Verordnung fortsetzen kann.
35 Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Düsseldorfer Kreis am 13./14.9.2016, abrufbar unter URL: https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/FortgeltungBisherErteilterEinwilligungen.html;jsessionid=6D61D02D93DE0C5A14FBC6003E72B5B3.2_cid354?nn=5217016 (zuletzt abgerufen am: 12.2.2018).
36 Vgl. nur § 8 I BbgDSG; § 10 I ThürDSG; § 14 III SachsAnhDSG sowie § 10 I SächsDSG.

nalverwaltungen gem. Art. 30 DSGVO ein sog. Verzeichnis von Verarbeitungstätigkeiten (VVT) für „alle" Verarbeitungstätigkeiten zu führen.

Dagegen ist eine Vorabmeldung einer Verarbeitungstätigkeit bei der zuständigen Aufsichtsbehörde nicht mehr notwendig.[37] Die entsprechenden Informationen sind indes nunmehr geordnet vorzuhalten, sodass sie auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt werden können.[38]

a) Formelle Anforderungen an das VVT

Das VVT ist im Gegensatz zum bisherigen Verfahrensverzeichnis nicht vom jeweiligen Datenschutzbeauftragten, sondern unmittelbar vom Verantwortlichen zu führen. Allerdings kann es gleichwohl sinnvoll sein, das Verzeichnis zentral in der Kommunalverwaltung zu führen. Auch insoweit bleibt aber die Verantwortung beim Behördenleiter.

Das Verzeichnis kann gemäß Art. 30 III DSGVO ausdrücklich auch in elektronischer Form geführt werden.

b) Inhalt des VVT

Inhaltlich ist VVT nicht als Auflistung einzelner Verarbeitungen, sondern als prozessorientierte Übersicht der Verarbeitungen zu verstehen. Ziel ist, dass über das VVT der einzelne Datenverarbeitungsprozess identifiziert werden kann. Die Mindestinhalte des VVT sind in Art. 30 I a bis g DSGVO benannt.[39]

c) Ausnahmen

Soweit Art. 30 V DSGVO eine Ausnahme von der Pflicht zur Führung eines V VT regelt, greift diese im Hinblick auf die kommunale Praxis nicht.

Danach müssen Einrichtungen kein VVT führen, die weniger als 250 Mitarbeiter beschäftigen. Diese Ausnahme ist aber auf Einrichtungen beschränkt, bei denen die Verarbeitung personenbezogener Daten nur „gelegentlich" erfolgt.[40] Dies kann bei Kommunalverwaltungen nicht angenommen werden.

5. Datenschutzfolgeabschätzung, Art. 35 DSGVO

Bei der Datenschutzfolgenabschätzung (DSFA) nach Art. 35 DSGVO handelt es sich um ein durch die DSGVO neugeschaffenes Instrument, das das Ziel verfolgt die Risiken der Betroffenen unabhängig von den sonstigen Voraussetzungen für die Datenverarbeitung durch geeignete Abhilfemaßnahmen einzudämmen.

Für die kommunale Praxis wird die DSFA insbesondere im Hinblick auf Videoüberwachung öffentlich zugänglicher Bereiche Bedeutung erlangen.

a) Anforderungen an die DSFA

Mindestinhalte einer DSFA sind nach Art. 35 VII DSGVO Informationen darüber, welche Datenverarbeitungsvorgänge geplant sind, wie deren Verhältnismäßigkeit eingeschätzt wird, welche möglichen Risiken von den Verarbeitungsvorgang für die Bürgerrechte betroffener Personen ausgehen sowie mögliche Abhilfemaßnahmen.

Da der Verordnungstext über diese Mindestangaben hinaus keine Anforderungen formuliert und verbindliche Aussagen der Aufsichtsbehörden zu den konkreten formalen Anforderungen an die Durchführung einer DSFA bislang fehlen, ist im Einzelnen noch vieles unklar.[41] Wie mit dem Instrument der DSGVO praktisch umzugehen ist, wird deshalb erst die Rechtspraxis nach dem 25.5.2018 zeigen.

b) Erforderlichkeit einer DSFA

Art. 35 III DSGVO nennt die Fälle, in denen eine DSFA insbesondere erforderlich ist. Von Relevanz für die kommunale Praxis ist dabei die Regelung des Art. 35 III c DSGVO, wonach im Vorfeld einer geplanten systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche eine DSFA durchzuführen ist. Die Pflicht soll insoweit der strukturellen Gefährdung des Persönlichkeitsrechts Rechnung tragen, die von systematischen Beobachtungen menschlichen Verhaltens durch Videomaßnahmen ausgeht.[42]

Des Weiteren sind nach Art. 35 IV DSGVO die Aufsichtsbehörden verpflichtet, eine Liste der Verarbeitungsvorgänge für die eine DSFA durchzuführen ist, zu veröffentlichen. Bislang bestehen derartige Positivlisten der Aufsichtsbehörden – soweit erkennbar – indes noch nicht. Darüber hinaus stellt Art. 35 V DSGVO die Erstellung einer Negativliste für Arten von Verarbeitungsvorgängen, für die keine Datenschutzfolgeabschätzung erforderlich ist, ausdrücklich in das Ermessen der Aufsichtsbehörden.

6. Bußgelder, Art. 83 DSGVO

In der öffentlichen Debatte über die DSGVO stehen die massiv erhöhten Bußgelder im Falle von Verstößen gegen die Vorgaben der DSGVO – als wesentliches Instrument zur Durchsetzung des materiellen Datenschutzrechts – im Mittelpunkt. Für den Datenschutz in der kommunalen Praxis spielen die Bußgelder aber wohl keine große Rolle.

So sieht Art. 83 VII DSGVO im Hinblick auf die Erhebung von Bußgeldern gegenüber öffentlichen Stellen eine Öffnungsklausel vor. Danach kann jeder vor Mitgliedsstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

---

37 *Spoerr*, in: BeckOK DatenschutzR, DS-GVO, 22. Ed. 5/2017, Art. 30 Rn. 27.
38 Vgl. Erwägungsgrund Nr. 89 der VO (EU) 2016/679.
39 Ein Muster für ein VVT stellt die Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) zur Verfügung unter URL: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf (zuletzt abgerufen am 12.2.2018).
40 Zwar tritt nach dem Wortlaut des Art. 30 V die Privilegierung nur ein, sofern „die Verarbeitung nicht nur gelegentlich", also regelmäßig erfolgt. Nach *Martini* (o. Fußn. 16), Art. 30 Rn. 33 ist jedoch das Gegenteil gemeint gewesen und die Konstruktion der doppelten Verneinung durch das Raster der redaktionellen Kontrolle gefallen. A.A. wohl *Spoerr* (o.Fußn. 37), Art. 30 Rn. 24.
41 Das Forum Privatheit hat ein sog. Whitepaper zur Umsetzung der DSFA mit umfassender Einleitung, Anforderungen und prozessorientierten Datenschutzmaßnahmen entworfen. Dieses ist online abrufbar unter URL: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf, zuletzt abgerufen am 12.2.18.
42 Erwägungsgrund Nr. 91 der VO (EU) 2016/679.

Hiervon hat jedenfalls der Bundesgesetzgeber in Art. 43 III BDSG (2018) bereits Gebrauch gemacht und festgelegt, dass gegen Behörden und sonstige öffentliche Stellen keine Geldbußen verhängt werden.

Entsprechende Regelungen treffen nach dem aktuellen Entwurfstand auch die Landesdatenschutzgesetze öffentliche Stellen der Länder.[43] Der Ausschluss von Bußgeldern soll jedoch nicht uneingeschränkt gelten. So sieht etwa Art. 22 BayDSG-E vor, dass gegen öffentliche Stellen Geldbußen nach Art. 83 DSGVO verhängt werden dürfen, soweit diese als Unternehmen am Wettbewerb teilnehmen.[44]

IV. Zusammenfassung

Auch die Kommunalverwaltungen sind gezwungen sich bis zum 25.5.2018 auf das „neue" Datenschutzrecht einzustellen. Ein Grund zur Panik besteht aber nicht.

Die größte Herausforderung besteht für den kommunalen Rechtsanwender darin, dass ihm zukünftig kein einheitliches datenschutzrechtliches Regelungswerk mehr zur Verfügung steht, sondern er sich aus der DSGVO und dem jeweils geltenden Landesdatenschutzgesetz die für die konkrete Fragestellung geltenden Vorgaben „zusammensuchen" muss.

Verantwortlich für die Einhaltung des Datenschutzes ist immer der Behördenleiter. Kommunale Datenschutzbeauftragte sind ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Zukünftig können Kommunalverwaltungen auch gemeinsam mit anderen Verwaltungen externe Beauftragte bestellen

Mit dem Instrument der Einwilligung zur Rechtfertigung der Datenverarbeitung durch die Kommunalverwaltung ist – wie bislang auch schon – vorsichtig zu verfahren. Es ist stets zu prüfen, ob der Betroffene die Einlegung freiwillig erteilt. Bisherige Einwilligungen sind auf ihre Vereinbarkeit mit den Vorgaben der DSGVO zu überprüfen.

Bei der Dokumentation der Verarbeitungstätigkeiten ist auf die neue Rechtslage abzustellen. Bestehende Verfahrensverzeichnisse müssen an die Anforderungen des Art. 30 DSGVO angepasst werden.

Auch kommunale Behörden werden prüfen müssen, ob und inwieweit im Einzelfall die Durchführung einer Datenschutzfolgenabschätzung notwendig ist. Da klare Vorgaben zur Durchführung einer Datenschutzfolgeabschätzung bislang fehlen, sollte insoweit Rücksprache mit der zuständigen Aufsichtsbehörde gehalten werden, die ohnehin gehalten ist entsprechende Positivlisten zu erstellen.

Kommunalverwaltungen werden sich keinen Bußgeldern durch die Aufsichtsbehörden ausgesetzt sehen, da die Landesgesetzgeber – soweit bislang bekannt – insoweit von der Öffnungsklausel des Art. 83 VII DSGVO Gebrauch machen werden, und Bußgelder für Stellen ausschließen.

---

43 Vgl. nur § 31 III BbgDSG-E; § 23 III DSG MV-E; § 61 IV ThürDSG-E; anders etwa in § 22 II SächsDSG-E, wo vorgesehen ist, dass Mitarbeiter der öffentlichen Stellen haftbar sind (vgl. auch LT-Dr 6/10918, S. 72).

44 so auch bspw. in § 61 IV ThürDSG-E.