Überblick zur EU-Datenschutz-Grundverordnung (DS-GVO) sowie wesentliche Entwicklungen im Landesdatenschutzrecht Sachsen-Anhalt

Von Katrin Riep, Magdeburg

Zusammenfassung
Die gründliche Befassung mit der DS-GVO ist in allen Bereichen erforderlich, die mit personenbezogenen Daten arbeiten.
Speziell unter Berücksichtigung der Verpflichtungen durch die Betroffenenrechte, kurzfristig erforderlicher Sofortmaßnahmen und der neu eingeführten Rechenschaftspflicht des Verantwortlichen sollte die DS-GVO zwingend dazu führen, dass der Datenschutz und das damit verbundene Datenschutzmanagementsystem dauerhaft in Unternehmen wie Behörden integriert wird.

1 Allgemeine Hinweise zum Geltungsbereich der DS-GVO

Dieser Beitrag gibt die persönliche Auffassung der Autorin wieder und soll insbesondere im behördlichen Bereich die systematische Arbeit mit der Rechtsmaterie erleichtern.

Die DS-GVO (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 Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 04.05.2016 S. 1 ff., L 314 vom 22.11.2016, S. 72, ABl. L 127 vom 23.05.2018, S. 2 ff.) ist seit Mai 2016 in Kraft und gilt nach dem zweijährigen Übergangszeitraum seit dem 25. Mai 2018 in allen Mitgliedsstaaten der EU gleichzeitig, unmittelbar und einheitlich (Art. 99 DS-GVO). Sie benötigt aufgrund ihres Rechtscharakters als Grundverordnung keines weiteren mitgliedschaftlichen Umsetzungsaktes. Bereits die Vorgängerregelung (RL 95/46/EG) war vollharmonisierend angelegt, konnte jedoch aufgrund der in der Zwischenzeit nach Inkrafttreten im Alltag und der Lebenswirklichkeit eingetretenen technischen Neuerungen (und u. a. daraus ergebenden Umgehungsmöglichkeiten), insbesondere für die großen Online-Unternehmen wie Google, Facebook etc. nur unzureichende Regelungen, v. a. eingrenzende Sanktionen, treffen.

Die DS-GVO ist in Abgrenzung und zugleich engem Zusammenhang mit der zeitgleich verabschiedeten sogenannten JI-RL (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, ABl. L 119 vom 04.05.2016, S. 89 ff.) zu betrachten. Um den sachlichen Anwendungsbereich der JI-RL von der DS-GVO abzugrenzen, ist die Regelung des Art. 2 Abs. 2 d DS-GVO in Verbindung mit den Erwägungsgründen (EG) Nr. 19 wesentlich. Für den behördlichen Bereich ist zum Verständnis wichtig, dass die Abgrenzung von der DS-GVO zur JI-RL nicht auf die Behördenzuständigkeit als Kriterium abstellt, sondern eine aufgabenbezogene

Betrachtung erfolgt. Aus systematischen Gründen erfolgen zu diesem wesentlichen Aspekt nähere Ausführungen unter dem Punkt I.1 (Entwicklungen im Landesdatenschutzrecht Sachsen-Anhalt).

Aus dem oben genannten Rechtscharakter der DS-GVO als Grundverordnung ergibt sich zudem, dass entgegenstehendes und prinzipiell auch gleichlautendes Recht generell im Sinne der DS-GVO auszulegen und anzuwenden ist.

Die Rechtsnatur der 173 Erwägungsgründe der DS-GVO soll an dieser Stelle für den Anwender in der Praxis kurz verdeutlicht werden. Erwägungsgründe (EG) befinden sich zwar außerhalb des eigentlichen Normtextes, dienen jedoch als fester Bestandteil einer Rechtsquelle als Auslegungskriterium der Praxis, da sie Rückschlüsse über Zielsetzungen und Hintergründe für den Erlass des Rechtsaktes und der politischen Einigung vorab geben. Sie entfalten insofern im Ergebnis zwar keine direkte Bindungswirkung, stellen jedoch wichtige Orientierungshilfen im Rahmen der Auslegung dar [Paal, Pauly 2018, Einleitung RN 10].

Im Folgenden werden die wesentlichsten (in der behördlichen Praxis häufig relevanten) neuen bzw. modifizierten Regelungen inhaltlich kurz vorgestellt:

1) Erweiterung des räumlichen Anwendungsbereichs

Der räumliche Anwendungsbereich der DS-GVO wird erheblich ausgedehnt auf datenverarbeitende Stellen auch außerhalb der EU, soweit sie personenbezogene Daten von in der Union befindlichen Personen verarbeiten und Waren oder Dienstleistungen entgeltlich oder unentgeltlich in der EU anbieten (Art. 3 Abs. 2 lit. a DS-GVO) oder eine Verhaltensbeobachtung nach Art. 3 Abs. 2 lit. b DS-GVO stattfindet. Das sogenannte „Marktortprinzip" nach Art. 3 Abs. 2 DS-GVO soll für gleiche Wettbewerbsbedingungen für alle in- und ausländischen Unternehmen sorgen, die auf dem europäischen Binnenmarkt tätig sind. Abzuwarten bleibt, ob in der zukünftigen Rechtspraxis durch diese beabsichtigte Schaffung einheitlicher Wettbewerbsbedingungen z. B. im Bereich der IT-Wirtschaft die Stärkung nationaler oder europäischer Unternehmen gegenüber den Marktgiganten (Facebook, Google etc.) erreicht wird. [Albrecht 2018, Teil 8].

2) Geschützte Rechte natürlicher Personen, neuer Verarbeitungsbegriff

Regelungsziel der DS-GVO ist der Schutz personenbezogener Daten natürlicher Personen (Art. 1 DS-GVO). Der gewährte Schutz soll nicht auf die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen erweitert werden (s. a. EG 14 DS-GVO). Daten der Organe juristischer Personen sind zwar im Ergebnis wieder Daten von natürlichen Personen (Organe der Gesellschaft wie Gesellschafter, Geschäftsführer, Aufsichtsrat), jedoch haben diese Personen die Datenverarbeitung bei unmittelbarem Bezug zur juristischen Person als Daten der juristischen Person hinzunehmen (s. a. BGH vom 24.06.2003, VI ZR 3/03 und nun insoweit stringent: EG 14 Satz 2 DS-GVO).

Der weit gefasste sachliche Anwendungsbereich (Art. 2 Abs. 1 DS-GVO) gibt vor, dass die DS-GVO neben der ganz oder teilweise automatisierten Datenverarbeitung auch für die nicht automatisierte Verarbeitung personenbezogener Daten gilt, sofern diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Unter Berücksichtigung des Wortlautes EG 15 wird deutlich, dass dieser extensive Anwendungsbereich u. a. in der behördlichen Praxis zu einer deutlichen Sensibilisierung im Sinne des Schutzzweckes der DS-GVO beitragen sollte.

Sofern im bisherigen fachspezifischen Datenschutzrecht mit der Nennung der sogenannten Trias „Erheben, Verarbeiten und Nutzen" umfassend alle datenbezogenen Vorgänge gemeint waren, wird nun lediglich der Begriff „Verarbeiten" unter Bezug auf Art. 4 Nr. 2 DS-GVO verwandt. Der bisher geltende engere Begriff „Verarbeiten" wurde grundsätzlich durch die nicht abschließend aufgezählten Unterfälle (Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung) ersetzt. Im Grunde sind damit alle Formen des Umgangs mit Daten angesprochen, um durch die extensive, nicht abschließende Aufzählung bewusst einen sehr weiten, zukunftstauglichen Schutzbereich zu schaffen.

Neu ist der erweiterte Verarbeitungsbegriff nach Art. 4 Nr. 2 DS-GVO; die nicht abschließende Aufzählung möglicher Nutzungsvorgänge erfasst im Ergebnis jeden Umgang mit Daten (mit oder ohne Hilfe automatisierter Verfahren).

Besondere Kategorien personenbezogener Daten sind nach Art. 9 Abs. 1 DS-GVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 Abs. 1 DS-GVO). Die rechtmäßige Verarbeitung dieser besonders sensiblen Daten erfordert stets besondere Prüfungen (u. a. Art. 9 Abs. 2 und 35 DS-GVO).

Nach Artikel 6 Abs. 1 DS-GVO gilt das bereits bekannte Grundmodell des Verbotes der Datenverarbeitung unter dem Vorbehalt einer gesetzlichen oder gewillkürten Erlaubnis.

Jede Verarbeitung muss neben den grundsätzlichen Voraussetzungen (Art. 5 DS-GVO) auch mindestens einer der in Art. 6 Abs. 1 DS-GVO genannten Rechtsgrundlagen genügen.

Zur Rechtmäßigkeit der Datenverarbeitung benennt Art. 6 Abs. 1 DS-GVO sechs Rechtsgrundlagen.

Auf die Einwilligung nach Art. 6 Abs. 1 lit. a (hierzu s. a. Art. 4 Nr. 11 DS-GVO) wird der behördliche Bereich aufgrund der typischerweise fehlenden Freiwilligkeit im Über-/Unterordnungsverhältnis zwischen Behörde und Bürger unter Beachtung des EG 43 DS-GVO eher selten zurückgreifen können. Im Einzelfall muss im Bereich der Einwilligung stets Art. 7 DS-GVO beachtet werden, d. h. erforderlich ist eine eindeutige, bestätigende Handlung, wobei bereits angekreuzte Kästchen oder die reine Untätigkeit nicht mehr ausreichend sein dürften. Insbesondere vorformulierte Einwilligungserklärungen müssen nach Art. 7 Abs. 2 DS-GVO in verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache verfasst sein und klar unterscheidbar von anderen Erklärungen erfolgen. Auf die jederzeitige Widerrufsmöglichkeit nach Art. 7 Abs. 3 DS-GVO sowie die Rechtswirkungen eines Widerrufs ist hinzuweisen. Nach EG 32 DS-GVO ist grundsätzlich zwar auch eine elektronische und mündliche Form der Einwilligung zulässig, jedoch wird die Praxis aufgrund der sich stellenden Nachweisproblematik im Einzelfall (Art. 7 Abs. 1 DS-GVO und EG 42) hiervon eher absehen. Inwiefern die alten – vor Inkrafttreten der DS-GVO, also auf der Basis der Richtlinie 95/46 EG – erteilten Einwilligungen ggf. im Einzelfall neu eingeholt werden müssen, ist anhand EG 171 DS-GVO zu prüfen.

Voraussetzungen einer wirksamen Einwilligung nach Art. 6 Abs. 1 lit. a, Art. 4 Nr. 11, Art. 7 f. DS-GVO ist u. a. das Merkmal der „Freiwilligkeit", das im behördlichen Verhältnis zum Bürger nicht in jedem Fall zu bejahen ist (s. a. EG 43).

Rechtsgrundlagen im behördlichen Bereich sind insbesondere Art. 6 Abs. 1 lit. c bzw. e jeweils in Verbindung mit Art. 6 Abs. 2, 3 DS-GVO (spezialgesetzlicher Grundlage).

Im Rahmen der öffentlichen Verwaltung dürften v. a. Art 6 Abs. 1 lit. c in Verbindung mit Art. 6 Abs. 2 und 3 DS-GVO (Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen) oder aber Art. 6 Abs. 1 lit. e in Verbindung mit Art. 6 Abs. 2 und 3 DS-GVO (Wahrnehmung öffentlicher Interessen und Ausübung öffentlicher Gewalt) als Rechtsgrundlagen einschlägig sein. Der Verweis auf die Absätze 2 und 3 des Art. 6 DS-GVO verdeutlicht, dass als ausreichende Rechtsgrundlage stets die spezifischen zumeist landes- bzw. bundesrechtlichen Rechtsnormen mit aufzuführen sind. Daneben ist bei beiden Rechtsgrundlagen das Merkmal der „Erforderlichkeit" ausdrücklich benannt.

Die allgemein bekannten und weiterhin geltenden Grundsätze im Datenschutzrecht wie z. B. Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Integrität und Vertraulichkeit finden sich in Art. 5 Abs. 1 DS-GVO. Wesentlich neu ist die in Art. 5 Abs. 2 DS-GVO geregelte Rechenschaftspflicht des Verantwortlichen.

Nichts prinzipiell Neues regelt Art. 5 Abs. 1 lit. a bis f mit den dort ausgeführten allgemeinen Grundsätzen, wie z. B. der Transparenz, Datenminimierung, Richtigkeit, Integrität und Vertraulichkeit. Der in Art. 5 Abs. 1 lit. b aufgestellte Grundsatz der Zweckbindung ist im Hinblick auf eine möglicherweise zulässige Zweckänderung stets mit Halbsatz 2 und zumeist Art. 6 Abs. 4 DS-GVO, der die Kriterien für die Beurteilung der Vereinbarkeit einer Zweckänderung vorgibt, zu prüfen.

Die in Art. 5 Abs. 2 DS-GVO neu geregelte Rechenschaftspflicht des Verantwortlichen (insofern zur Legaldefinition des „Verantwortlichen" s. a. Art. 4 lit. 7 DS-GVO) sollte im Sinne der insgesamt nach DS-GVO neu geregelten Pflichten zu einem verstärkten Datenschutzmanagement führen, dass entsprechend der vorgegebenen Dokumentationspflichten entsprechende Maßnahmen nach Art. 24 f. DS-GVO stringent umsetzt, um so selbst im Falle einer Verletzung des Schutzes personenbezogener Daten die Befreiung von der Haftung nach Art. 83 Abs. 3, 33 Abs. 5 DS-GVO ermöglicht.

Insbesondere die Rechte betroffener Personen (zum Begriff der „betroffenen Person" s. a. Art. 4 Nr. 1 DS-GVO) werden durch einen Katalog der Informationen, die dem Betroffenen zur Verfügung gestellt werden müssen, erheblich erweitert.

Art. 13 DS-GVO trifft Regelungen zur Informationspflicht bei der Erhebung von personenbezogenen Daten direkt bei der betroffenen Person, wohingegen Art. 14 DS-GVO diejenigen Vorgaben aufzeigt, die im Hinblick auf die Informationspflicht einzuhalten sind, wenn die Erhebung personenbezogener Daten nicht direkt bei der betroffenen Person erfolgt.

Die wichtigsten Legaldefinitionen zu den verwendeten Begriffen finden sich in Art. 4 DS-GVO.

Neben Pflichtinformationen (systematisch jeweils Abs. 1 der Art. 13 und Art. 14 DS-GVO), die immer zu geben sind, müssen weitere Informationen mitgeteilt werden, wenn sie für eine transparente Datenverarbeitung erforderlich sind (systematisch jeweils Abs. 2 der Art. 13 und Art. 14 DS-GVO). Bei Änderungen des Erhebungszweckes im Rahmen der Verarbeitung sind nach Art. 13 Abs. 3 und Art. 14 Abs. 4 DS-GVO weitere Angaben zur Verfügung zu stellen. Ob daneben grundsätzlich die allgemeinen Abwägungskriterien des Art. 6 Abs. 4 DS-GVO zur Einschätzung der Vereinbarung der Zweckänderung bei Datenverarbeitung für Sekundärzwecke zu beachten sind, scheint in der aktuellen Literatur noch nicht endgültig geklärt (bejahend: Knyrim in: [Ehmann, Selmayr 2017], Art. 13 RN 56, a. A. Paal/Hennemann in: [Paal, Pauly 2018], Art. 13 RN 33). Wichtig ist aber, dass bereits die Absicht der Weiterverarbeitung nach Art. 13 Abs. 3 DS-GVO bzw. Art. 14 Abs. 4 DS-GVO zu denjenigen Informationen zählt, die der Verantwortliche dem Betroffenen bei Erhebung, d. h. bereits ohne beabsichtigte Zweckänderung mitteilen muss [Schneider 2017, S. 66].

Art. 13 Abs. 4 bzw. Art 14 Abs. 5 lit. a DS-GVO schließen die Informationspflichten aus, wenn und soweit die betroffene Person bereits über die betreffenden Informa-

tionen verfügt, wobei hier positive Kenntnis erforderlich ist. Praxisrelevante Fallkonstellation ist der häufige Fall, dass ein Bürger seine Kontaktdaten mit der Bitte um konkrete behördliche Maßnahmen direkt an die örtlich und sachlich zuständige Behörde gibt. Solange und soweit diese im Rahmen ihres originären Aufgabenbereichs das Bürgeranliegen intern klären kann und keine Weitergabe z. B. an Behörden außerhalb des Zuständigkeitsbereiches sowie keine Aufnahme der Daten z. B. in einen E-Mail-Verteiler erfolgt (hierfür wäre Art. 4 Nr. 2 DS-GVO einschlägig), darf aufgrund der ausdrücklichen Bitte des Bürgers davon ausgegangen werden, dass er über positive Kenntnis zur Verarbeitung seiner Daten verfügt und daher die Informationspflichten nach Art. 13 Abs. 4 DS-GVO entfallen.

Weitere Betroffenenrechte sind neben dem Auskunftsrecht (Art. 15 DS-GVO) das Recht auf Berichtigung nach Art. 16 DS-GVO sowie das Recht auf Löschung und auf Vergessenwerden nach Art. 17 DS-GVO. Mit dem „Recht auf Vergessenwerden“ bei Veröffentlichung in Art. 17 Abs. 2 DS-GVO soll sichergestellt werden, dass Unternehmen, die Daten öffentlich gemacht haben, das Löschungsverlangen des Betroffenen an Dritte weiterleiten müssen, wenn diese auf die Veröffentlichung verweisen sowie auch allen sonstigen Dritten, welchen es die Daten weitergeleitet hatte, das Löschungsbegehren mitteilen (Kamann/Braun in: [Ehmann, Selmayr 2017], Art. 17 RN 38 ff.). Art. 17 Abs. 1 DS-GVO führt neben den allgemeinen Gründen (v. a. Widerruf der Einwilligung, Widerspruch gegen die Verarbeitung und unrechtmäßige Verarbeitung) einen speziellen Löschungsgrund mittels Buchstabe f ein, wenn Daten über Kinder von Internetanbietern erhoben worden sind, die sich direkt an Kinder (in Bezug auf Dienste der Informationsgesellschaft) wenden. Zur Altersgrenze bei Minderjährigen geht Art. 8 DS-GVO i. V. m. Art. 6 Abs. 1 lit. a DS-GVO von einer eigenen Einsichtsfähigkeit im Hinblick auf die Einwilligung im Alter zwischen vollendetem 13. Lebensjahr (s. a. Öffnungsklausel des Art. 8 Abs. 1 Satz 3 DS-GVO für abweichende mitgliedsstaatliche Regelungen) und 16. Lebensjahr bei einem Angebot von Diensten der Informationsgesellschaft, das direkt gegenüber dem Kind offeriert wird, aus. Damit ist für den Rechtsanwender in diesen speziellen Fällen zu beachten, dass im Falle von Jugendlichen unter dem vollendeten 16. Lebensjahr die Träger elterlicher Verantwortung selbst einwilligen müssen oder aber der Einwilligung des Jugendlichen zustimmen müssen (Frenzel in: [Paal, Pauly 2018], Art. 8 RN 11).

Mit den neuen Betroffenenrechten, insbesondere den Art. 13, 14, 15, 16, 17 DS-GVO unter Beachtung der allgemeinen Regelungen des Art. 12 DS-GVO sollte sich Jeder, der personenbezogene Daten verarbeitet, vertraut machen.

Art. 21 DS-GVO regelt ein Widerspruchsrecht bei der Verarbeitung nach Art. 6 Abs. 1 lit. e oder lit. f DS-GVO und ein besonderes Widerspruchsrecht bei der Datenverarbeitung zum Zwecke des Direktmarketings (Art. 21 Abs. 2, 3 DS-GVO). Der ausdrückliche Hinweis für den Betroffenen auf das Widerspruchsrecht in verständlicher Form und getrennt von jeglicher anderer Information (Art. 21 Abs. 4 DS-GVO) ist systemkonform und präzisiert die allgemeinen Anforderungen nach Art. 12 Abs. 1 und Art. 13 bzw. 14 DS-GVO (Martini in: [Paal, Pauly 2018], Art. 21 RN 64 ff.).

Durch Art. 20 DS-GVO ist ein Recht auf Datenübertragbarkeit (sog. Daten-Portabilität) eingefügt worden. Unter den dort genannten Voraussetzungen erhält der Betroffene damit das Recht, eine Kopie der von ihm zur Verfügung gestellten Daten zu erhalten und diese zu einem anderen Anbieter zu übermitteln (Art. 20 DS-GVO). Darüber hinaus kann er nach Art. 20 Abs. 2 DS-GVO unter der Prämisse der technischen Möglichkeiten die direkte Übermittlung vom alten Verantwortlichen (Provider) an den neu vom Betroffenen gewünschten Verantwortlichen (Folgeprovider) verlangen.

Dieser Rechtsanspruch auf Datenübertragbarkeit soll es in der Praxis erleichtern, Profile bei sozialen Netzwerken oder E-Mail-Konten auf datenschutzfreundlichere Netzwerke/Technologien zu übertragen und ist damit auch als Wettbewerbsgedanke zur Förderung datenschutzfreundlicher Technologien zu bewerten (Martini in: [Paal, Pauly 2018], Art. 20 RN 5). Die Einschränkungen des Anspruchs nach Art. 20 Abs. 3 Satz 2 DS-GVO gilt grundsätzlich u. a. für den behördlichen Bereich (Kamann/Braun in: [Ehmann, Selmayr 2017], Art. 20 RN 30).

Die DS-GVO belässt den Mitgliedsstaaten in sogenannten Öffnungsklauseln Spielräume für eigenständige nationale Regelungen. Wesentliche Öffnungsklauseln sind z. B. Art. 6 Abs. 2 und Abs. 3, Art. 9 Abs. 4, Art. 23, Art. 88 DS-GVO.

Weitreichende Beschränkungsmöglichkeiten im Hinblick auf die Betroffenenrechte eröffnet Art. 23 DS-GVO den Mitgliedsstaaten. Art. 23 DS-GVO erfordert zur wirksamen Beschränkung der Betroffenenrechte Normen, die den detaillierten Vorgaben des Art. 23 Abs. 1 und Abs. 2 DS-GVO entsprechen müssen und inhaltlich konkrete, begründete Beschränkungen vorgeben.

Die DS-GVO enthält zahlreiche Öffnungsklauseln, die den Mitgliedsstaaten in engen Grenzen einen Umsetzungsspielraum einräumen (sog. fakultative Öffnungsklauseln) oder zwingende Regelungsaufträge an die nationalen Gesetzgeber vorgeben (sog. obligatorische Öffnungsklauseln). Eine wesentliche Aufgabe der Rechtsanwender wird zukünftig die kritische Prüfung im Hinblick auf die rechtlich zulässige Nutzung eingeräumter Spielräume durch Öffnungsklauseln sein. Zu beachten ist an dieser Stelle der grundsätzliche Anwendungsvorrang des höherrangigen Rechts, d. h. der unmittelbar geltenden DS-GVO [Kühling, Sackmann 2018, S. 682].

Der Vollständigkeit halber soll Art. 12 DS-GVO nicht unerwähnt bleiben. Art. 12 Abs. 1 DS-GVO kann als „Generalklausel" im Hinblick auf die Transparenzvorgaben zur Information der betroffenen Person bezeichnet werden (Paal/Hennemann in: [Paal, Pauly 2018], Art. 12 RN 1).

Art. 12 Abs. 2, 3 DS-GVO regeln daneben konkrete Verpflichtungen des Verantwortlichen im Hinblick auf die erleichterte Wahrnehmung der Betroffenenrechte. Insbesondere die gesetzlich vorgegebene Frist auf Auskunft innerhalb eines Monats nach Eingang des Antrags (Art. 12 Abs. 3 Satz 1 DS-GVO) im Normalfall verdeutlicht, dass es durchaus bedeutsam ist, innerhalb kurzer Zeit einen Gesamtüberblick über die vorhandenen personenbezogenen Daten im Verantwortungsbereich zu bekommen. Diese übliche Aufgabe eines Datenmanagements ist mittels eines aktuellen, vollständigen und aussagefähigen sog. Verzeichnisses über Verarbeitungstätigkeiten (Art. 30 DS-GVO, genaueres hierzu unter Punkt 8) zu bewältigen. Zugleich wird an dieser Stelle bereits deutlich, dass die Anforderungen der DS-GVO gleichsam aufeinander aufbauen und als dauerhafte Aufgabe die aktuelle Integration des Datenschutzmanagements im Alltag und die Einbindung aller (behördlichen) Bereiche erfordern.

3) Betonung des technischen und organisatorischen Datenschutzkonzeptes, insbesondere durch Art. 24 f., 32, 35 f., 5 Abs. 1 lit. d und Art. 5 Abs. 2 DS-GVO

Aufgrund des risikobasierten Ansatzes der DS-GVO sind die zu erfüllenden technischen und organisatorischen Datenschutzkonzepte immer am Schutzzweck (Worst-Case-Szenario) ausgerichtet und auf dem aktuellen Stand der Technik unter Nutzung datenschutzfreundlicher Technikgestaltung sowie Voreinstellung zu orientieren. Der Umfang zu treffender Vorsorgemaßnahmen ist mittels einer Gesamtabwägung, die in Art. 25 DS-GVO dargestellt ist, zu treffen. Insbesondere aufgrund der 2. Berichtigung der DS-GVO (Berichtigung des Europäischen Rates vom 19.04.2018, ABl.

L 127/2 vom 23.05.2018) mittels der u. a. im Art. 25 Abs. 2 DS-GVO das möglicherweise einschränkende Wort „grundsätzlich" gestrichen wurde, bleibt zu vermuten, dass dem uneingeschränkten neuen Wortlaut nach der Verantwortliche die geeigneten und organisatorischen Maßnahmen treffen soll, die sicherstellen, dass entsprechende datenschutzfreundliche Voreinstellungen vorgenommen werden. Das Gebot des Art. 25 Abs. 2 Satz 1 DS-GVO ist damit im Umkehrschluss nicht mehr unter dem Vorbehalt der Angemessenheit zu würdigen (so noch für die Textfassung vor 2. Berichtigung der DS-GVO vertreten: Martini in: [Paal, Pauly 2018], Art. 25 RN 47). Damit wurde das im Rahmen der DS-GVO dargestellte Konzept Datenschutz durch Technik („privacy by design", Abs. 25 Abs. 1) und datenschutzfreundliche Voreinstellungen („privacy by default") konsequent noch verstärkt. Dies ist systemkonform auch unter Berücksichtigung der neu eingeführten Rechenschaftspflicht des Verantwortlichen nach Art 5 Abs. 2 DS-GVO als wesentliche Kernaussage der DS-GVO zu betrachten. Umsetzungsinstrumente in der Praxis sind u. a. das Verarbeitungsverzeichnis (Art. 30 DS-GVO) und die Datenschutz-Folgeabschätzung (Art. 35 DS-GVO).

Im Rahmen der Regelungen wird der wesentliche Bedeutungszuwachs technischer und organisatorischer Maßnahmen unter Berücksichtigung des risikobasierten Ansatzes und der Aktualisierungsverpflichtung sowie Beachtung der Einführung einer Rechenschaftspflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO deutlich.

Prüfungs-und Aktualisierungspflicht (Art 24 DS-GVO) sind daher bei Maßnahmen stets als dynamischer Prozess (s. a. Art. 5 Abs. 1 d DS-GVO) auszugestalten. Wesentliche Grundaussagen bei der Risikobetrachtung ergeben sich für den Rechtsanwender auch aus EG 75.

Künftig werden die vorgesehenen Selbstregulierungs- und Zertifizierungsmechanismen (s. a. Art. 40 ff. DS-GVO, Art. 28 Abs. 5 DS-GVO) sicher an Bedeutung gewinnen und in der Praxis – ähnlich einem Datenschutzaudit – genutzt werden [Schantz 2016, S. 1841ff (1846)].

4) Aufsichtsstärkung Art. 51 ff. DS-GVO

Wesentliche Intention der DS-GVO war es, die Datenschutzaufsicht innerhalb der EU insgesamt zu stärken. Art. 52 DS-GVO betont die Unabhängigkeit der Aufsichtsbehörden und richtet mittels Art. 52 Abs. 3 DS-GVO den ausdrücklichen Auftrag an die Mitgliedsstaaten, die Aufsichtsbehörden umfassend im Hinblick auf eine effektive Aufgabenwahrnehmung mit personellen, technischen, finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen auszustatten.

Im Land Sachsen-Anhalt ist die organisationsrechtliche Umsetzung mittels des am 25.01.2018 vom Landtag beschlossenen Gesetzes zur Organisationsfortentwicklung des Landesbeauftragten für den Datenschutz und zur Änderung des Informationszugangsgesetzes Sachsen-Anhalt vom 21. Februar 2018 (GVBl. LSA S. 10, Datum des Inkrafttretens 06.05.2018) erfolgt.

Hiernach ist der Landesbeauftragte für den Datenschutz (LfD) in der Verfassung als persönlich Verantwortlicher für den Datenschutz (Artikel 63 der Landesverfassung) weiterhin verankert. Der LfD wird nach Artikel 59 DS-GVO verpflichtet, einen Jahresbericht über seine Tätigkeit zu erstellen, den er sowohl dem Landtag als auch der Landesregierung übermittelt. Damit wird die Form des bisherigen Tätigkeitsberichtes, der bislang zwei Berichtsjahre erfasste, entbehrlich. Im Rahmen der bisherigen Tätigkeitsberichte fungierte der LfD mindestens für den öffentlichen Bereich lediglich als Eingabe- und Beschwerdestelle und konnte insofern informelle Beanstandungen aussprechen. Nach Art. 58 DS-GVO kann der LfD gegenüber allen Landesbehörden – also auch im öffentlichen Bereich – Beanstan-

dungen in der Form eines Verwaltungsakts aussprechen, der justiziabel ist. Insofern werden die nach der DS-GVO vorgegebenen Berichte deutlich mehr den Charakter von Rechenschaftsberichten erhalten.

Im öffentlichen Bereich wird die Aufsichtsbehörde weitreichende Befugnisse erhalten, die sie bisher nicht hatte. Sie wird u. a. auch gegenüber Behörden Anordnungen erlassen können, um z. B. eine rechtswidrige Datenverarbeitung zu unterbinden, die Löschung personenbezogener Daten zu erwirken oder eine Datenübermittlung in Drittstaaten zu untersagen.

Datenschutzbehörden werden damit zu spezifischen Rechtsaufsichtsbehörden auch gegenüber Behörden.

Der Landesbeauftragte wird durch eine entsprechende Regelung in § 21 DSG LSA (neu) sowohl Aufsichtsbehörde im Sinne der DS-GVO als auch Aufsichtsbehörde für den Bereich von Polizei und Justiz bis hin zur Strafvollstreckung im Sinne der JI-RL.

Die bislang nach § 21 Abs. 3 Satz 1 DSG LSA beim Präsidenten des Landtags angesiedelte Geschäftsstelle des LfD wird rechtlich verselbständigt. Zukünftig steht der LfD der nur ihm ausschließlich zugeordneten Geschäftsstelle vor. Die Verselbständigung wird haushaltsrechtlich umgesetzt, indem der LfD ab dem Haushaltsjahr 2018 einen eigenen Einzelplan erhält.

Der Anspruch auf wirksamen gerichtlichen Rechtsschutz wird durch die Neuregelung des § 31b DSG LSA umgesetzt. Hiernach werden dem Verwaltungsgericht Magdeburg für die Bezirke aller Verwaltungsgerichte die Rechtsstreitigkeiten nach Art. 78 Abs. 1 und 2 DS-GVO und Art. 53 Abs. 1 und 2 der JI-RL mit Ausnahme der Straf- und Bußgeldverfahren zugewiesen. Ein Vorverfahren ist nicht vorgesehen.

Im nicht-öffentlichen Bereich sind die Befugnisse der Aufsicht (Art. 58 DS-GVO) mit der ehemals geltenden Rechtslage vergleichbar.

Erleichterungen für die Betroffenen bringt bei grenzüberschreitenden Datenverarbeitungen im Ergebnis der sogenannte „One-Stop-Shop-Mechanismus“. Hiernach ist grundsätzlich federführend die Datenschutzbehörde am Hauptsitz bzw. Sitz der Hauptniederlassung des Verantwortlichen (zentraler Ansprechpartner Art. 56 DS-GVO). Es gilt nach Art. 77 Abs. 1 DS-GVO allgemein, dass der Betroffene sich mit Beschwerden immer an die Datenschutzaufsichtsbehörde seines Wohnsitzes wenden kann (Art. 77 Abs. 1 DS-GVO).

5) Datenschutz-Folgeabschätzung Art. 35 f. DS-GVO

Die Datenschutz-Folgeabschätzung ist ein Mittel zur Erfüllung der Dokumentationspflichten nach Art. 24 DS-GVO und nicht auf automatisierte Verarbeitungen beschränkt. Die in Art. 35 f. DS-GVO aufgezählten Kriterien zur Risikoeinschätzung sind nicht abschließend, lassen aber deutlich werden, dass auch hier der risikobasierte Ansatz der DS-GVO im Grundsatz gilt. Systematisch konsequent ist die Regelung, dass im Gegensatz zur Vorgängernorm keine generelle Meldepflicht mehr gefordert wird, sondern der Fokus auf denjenigen Arten von Verarbeitungsvorgängen liegt, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen mit sich bringen. Insbesondere bei Nutzung neuer Technologien ohne bisherige Folgenabschätzung und umfangreichen Verarbeitungsvorgängen ist im Zweifel schon dem Wortlaut nach vorab eine Datenschutz-Folgeabschätzung durch den Verantwortlichen vorzunehmen.

Da die Datenschutz-Folgeabschätzung ein übliches Instrument im Datenschutzmanagement ist, um Risiken für Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten zu beschreiben, zu bewerten und im Ergebnis einzudämmen, sind beim Verantwortlichen stets möglichst früh Maßnahmen, Garantien und Verfahren zur Risikoeindämmung durch Einfügung verfügbarer Technologien und Implementierungskosten zu prüfen. Dies sollte bei der Auftragsverarbeitung unter Einbeziehung bzw. mit Unterstützung des Auftragsverarbeiters erfolgen. Die Konsultation der Aufsichtsbehörde wird mittels Art. 36 DS-GVO, s. a. EG 94 nunmehr stark risikobasiert geregelt.

Die Datenschutz-Folgenabschätzung erfordert grundsätzlich eine risikobasierte Selbsteinschätzung durch den Verantwortlichen auf erster Prüfungsstufe.

Art. 33 f. DS-GVO regeln die Pflichten bei Datenschutzverstößen. Hiernach muss grundsätzlich das verantwortliche Unternehmen der Aufsichtsbehörde jede Datenschutzverletzung unverzüglich, möglichst innerhalb 72 Stunden nach Kenntnis des Verantwortlichen melden. Die in Art. 33 Abs. 1, Satz 1, 2. Halbsatz geregelte Ausnahme zielt ersichtlich wieder auf eine risikoorientierte Betrachtung ab. Die gegensätzlichen Sachverhalte (Benachrichtigungspflicht der betroffenen Person bei voraussichtlich hoher Risikobewertung) regelt Art. 34 DS-GVO.

Den Umfang der Informationen, die mit einer Meldung nach Art. 33 DS-GVO den Aufsichtsbehörden mitzuteilen sind, gibt Art. 33 Abs. 3 DS-GVO ggf. in Verbindung mit Art. 34 Abs. 2 DS-GVO vor.

Für den Rechtsanwender bleibt zu hoffen, dass die Aufsichtsbehörden zeitnah von der ihnen eingeräumten Möglichkeit (s. a. Art. 35 Abs. 4 DS-GVO) zur Erstellung einer Positivliste, d. h. einer Liste solcher Verarbeitungsvorgänge, die regelmäßig eine Datenschutz-Folgeabschätzung nach sich ziehen, veröffentlichen. Derzeit liegen als Orientierungshilfe die von der Art. 29-Datenschutzgruppe bereits im April 2017 erstellten Leitlinien zum Begriff des hohen Risikos und zur Datenschutz-Folgeabschätzung vor, die allerdings noch unter Geltung der Vorgängerrichtlinie erstellt wurden. Es bleibt den Aufsichtsbehörden nach Art. 35 Abs. 5 DS-GVO fakultativ unbenommen, praktisch spiegelbildlich zu Art. 35 Abs. 4 DS-GVO eine Negativliste zu erstellen und zu veröffentlichen, in der diejenigen Verarbeitungsvorgänge aufgeführt werden, die keine Datenschutz-Folgeabschätzung erforderlich machen.

Bezogen auf den behördlichen Bereich wäre darüber hinaus wünschenswert, wenn die Mitgliedsstaaten bzw. die Union selbst beim zukünftigen Erlass von Rechtsgrundlagen in geeigneten Fällen nach ihrem Ermessen eine Gesetzesfolgenabschätzung bereits im Rahmen des Gesetzgebungsverfahrens durchführen, die es nach Art. 35 Abs. 10 DS-GVO den Anwendern ermöglicht, von der eigenen Datenschutz-Folgeabschätzung abzusehen. Mit Hilfe dieses Verfahrens könnte der Bürokratieaufwand, insbesondere im Bereich des öffentlichen Dienstes, erheblich vermindert werden (Baumgartner in: [Ehmann, Selmayr 2017], Art. 35 RN 51).

6) Bestellungspflichten von Datenschutzbeauftragten und Stellung derselben nach Art. 37 ff. DS-GVO

Die Pflicht zur Bestellung eines Datenschutzbeauftragten regelt Art. 37 Abs. 1 lit. a bis c DS-GVO. Hiernach ist zwingend ein Datenschutzbeauftragter zu bestellen, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme der Gerichte, soweit diese im Rahmen ihrer justiziellen Tätigkeit handeln oder wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund

ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder aber die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 oder Art. 10 DS-GVO besteht. Die Formulierung der Bestellungspflicht für Unternehmen lässt wieder den risikobasierten Grundgedanken der DS-GVO im Hinblick auf Datenverarbeitungsprozesse erkennen. Art. 37 Abs. 1 lit. b DS-GVO spricht von der Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters und macht damit (unter Berücksichtigung der Erläuterung im EG 97) deutlich, dass sich dieser Begriff auf die Haupttätigkeit des Unternehmens beziehen soll und die in der Regelung genannten gesamten Umstände sowohl einzeln als auch kumulativ zur Beantwortung der Frage einer Bestellungspflicht im Unternehmen einfließen sollen. Entsprechend der Intention der DS-GVO wurde die Stellung der Datenschutzbeauftragten deutlich gestärkt. Dies ergibt sich schon aus der Regelung des Art. 38 Abs. 3 Satz 1 (Weisungsfreiheit im Aufgabenbereich), Art. 38 Abs. 3 Satz 2 DS-GVO (funktionsbezogenes Abberufungs- und Benachteiligungsverbot) und Art. 38 Abs. 3 Satz 3 (unmittelbares Berichtsrecht des Datenschutzbeauftragten gegenüber der obersten Managementebene). Den Aufgabenbereich beschreibt Art. 39 Abs. 1 DS-GVO zwar nicht abschließend, aber recht ausführlich. Wesentlichste Aufgaben werden in der Praxis – neben der Beratung und Sensibilisierung Betroffener zu datenschutzrelevanten Fragen – auch die Begleitung und Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung nach Art. 39 Abs. 1 lit. c, 35 Abs. 2 DS-GVO sowie die Zusammenarbeit mit der Aufsichtsbehörde nach Art. 39 Abs. 1 lit d und e DS-GVO darstellen. Die Kontaktdaten des Datenschutzbeauftragten sind nach Art. 37 Abs. 7 DS-GVO zu veröffentlichen, um das Anrufungsrecht Betroffener nach Art. 38 Abs. 4 DS-GVO zu realisieren. Ausreichend dürfte in diesem Zusammenhang die Veröffentlichung auf einer nicht zugangsbeschränkten Internetseite sein [Wybitul, von Gierke 2016, S. 100 ff]. Für die ebenfalls erforderliche Mitteilung an die Aufsichtsbehörde dürften zwischenzeitlich alle Aufsichtsbehörden ein Onlineformular zur Verfügung gestellt haben. Die risikoorientierte Aufgabenerfüllung nach Art. 39 Abs. 2 DS-GVO rundet den Rahmen des insgesamt risikobasierten Ansatzes der DS-GVO ab [Klug 2017, S. 4 ff. (8)].

7) Einführung unionseinheitlicher Sanktionen (Art. 82 ff. DS-GVO)

Die Sanktionsmöglichkeiten sind durch die DS-GVO erheblich verschärft worden. Art. 82 Abs. 1 DS-GVO stellt als eigenständige datenschutzrechtliche Haftungsnorm sowohl auf materielle als auch immaterielle Schäden ab und erweitert die Haftung auf Auftragsverarbeiter neben dem Verantwortlichen [Wybitul, Haß 2018, S. 113 ff.]. Unter zivilrechtlichen Aspekten ist die europarechtliche Norm selbständig neben vertraglichen, deliktischen und sonstigen Ansprüchen zu betrachten. Neu eingeführt wird die Möglichkeit, in Anlehnung einer „Prozessstandschaft“ nach Art. 80 Art. 1 DS-GVO, dass Non-profit-Organisationen unter den aufgeführten Voraussetzungen Betroffene vertreten. Daneben wurde eine Öffnungsklausel für Mitgliedsstaaten geschaffen, um nach Art. 80 Abs. 2 DS-GVO eine Regelung zur Verbandsklage einführen zu können [Schantz 2016, S. 1841 ff.]. Im Hinblick auf die Verhängung von Geldbußen gibt Art. 83 DS-GVO neben den allgemeinen Grundsätzen der Wirksamkeit, Verhältnismäßigkeit und Abschreckung (Art. 83 Abs. 1 DS-GVO) ausführlich mittels Absatz 2 Zumessungskriterien vor, die einzelfallbezogen eine umfassende Würdigung erfordern. Zu berücksichtigen sind neben der Abwägung von Verantwortungsantei-

len unter Berücksichtigung der nach Art. 25, 32 getroffenen technischen Maßnahmen, die Bewertung der Art, Schwere und Dauer des Verstoßes, der Umfang der Maßnahmen zur Schadensbegrenzung, die Zusammenarbeit mit Aufsichtsbehörden, die Kategorien der betroffenen personenbezogenen Daten und anderes mehr.

Im Hinblick auf die Verhängung von Bußgeldern, insbesondere im Bereich klein- und mittelständischer Unternehmen, bestehen derzeit keine Anhaltspunkte, dass die Datenschutzaufsichtsbehörden von ihrer Praxis einer verhältnismäßigen Sanktionierung, die mittlerweile auch durch die o. g. Normen der DS-GVO vorgeschrieben sind, abweichen werden [Bundesregierung 2018, Seite 5].

8) Verzeichnis von Verarbeitungstätigkeiten Art. 30 DS-GVO

Auch die Dokumentationspflicht der Datenverarbeitungsvorgänge in einem Verzeichnis (Verzeichnis von Verarbeitungstätigkeiten) nach Art. 30 DS-GVO ist nicht grundsätzlich neu. Im Zusammenhang mit den neu eingeführten Auskunftsrechten der betroffenen Personen sowie unter Berücksichtigung der neu eingeführten Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO ist das Verzeichnis von Verarbeitungstätigkeiten ein wesentlicher Bestandteil zur Erfüllung dieser gesetzlichen Rechte natürlicher Personen und zugleich auch essentiell im Bereich des Datenschutzmanagements.

Nach Artikel 30 Abs. 1 Satz 1 DS-GVO hat grundsätzlich jeder Verantwortliche, der personenbezogene Daten verarbeitet, ein Verzeichnis aller Verarbeitungstätigkeiten dafür zu erstellen und zu führen. Diese Pflicht trifft ebenfalls den Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO).

Mit einem solchen Verzeichnis stehen geeignete Übersichten zur Verfügung, um die Datenschutzverpflichtungen nach der DS-GVO zu erfüllen, die dann auch auf Anfrage (Art. 30 Abs. 4 DS-GVO) von den Aufsichtsbehörden kontrolliert werden können.

Das Verzeichnis von Verarbeitungstätigkeiten betrifft alle ganz oder teilweise automatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Um einen aktuellen Überblick (Bestandsaufnahme der Prozesse, in denen personenbezogene Daten verarbeitet werden) für den gesamten Verantwortungsbereich zu erhalten, sollten notwendigerweise alle datenverarbeitenden Strukturen regelmäßig sensibilisiert und einbezogen werden, um den Aktualisierungsverpflichtungen nach Art. 24 Abs. 1, 32 Abs. 1, 5 Abs. 1 lit. d DS-GVO auch unter Berücksichtigung der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO genügen zu können.

Die Ausnahme von der Pflicht zur Erstellung und aktuellen Führung eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 5 DS-GVO soll ersichtlich nur kleine und mittelständische Unternehmen betreffen (Beschäftigtenzahl unter 250 Mitarbeiter) soweit „… die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Person birgt, die Verarbeitung nicht nur gelegentlich erfolgt …“ oder aber die Verarbeitung keine besonderen Datenkategorien im Sinne des Art. 9 DS-GVO oder strafrechtliche Verurteilungen und Straftaten nach Art. 10 DS-GVO erfasst. Die Privilegierung nach Art. 30 Abs. 5 DS-GVO benennt zwar nicht ausdrücklich Behörden, sondern spricht hier Unternehmen oder Einrichtungen an,

jedoch ergibt sich aus den kumulativ erforderlichen Gegenausnahmen („… es sei denn ...“), dass ein enger Anwendungsbereich in der Praxis vorliegen wird. Insbesondere die Voraussetzung der nur gelegentlichen Datenverarbeitung ist unter systematischer Betrachtung so auszulegen, dass gerade nicht solche Datenverarbeitungen befreit werden, die als regelmäßige Datenverarbeitungen zum typischen Geschäftsbetrieb gehören. Erfasst werden sollen nur solche Verarbeitungstätigkeiten, die sich abseits des typischen Betriebs bewegen und nur von Zeit zu Zeit in der Praxis vorkommen. Für regelmäßige oder dauerhafte Standardverfahren in Unternehmen wie Behörden (wie z. B. Personalaktenverfahren, Finanzbuchhaltung etc.) bleibt es daher unabhängig von der Mitarbeiterzahl bei der Verpflichtung zur Führung des Verfahrensverzeichnisses (so eindeutig: Martini in: [Paal, Pauly 2018], Art. 30 RN 34).

Der Inhalt des Verarbeitungsverzeichnisses ergibt sich aus Art. 30 Abs. 1 (für den Verantwortlichen) bzw. aus Art. 30 Abs. 2 (betrifft Auftragsverarbeiter bzw. Vertreter).

Mittlerweile haben viele Landesbeauftragte für den Datenschutz und auch die Datenschutzkonferenz des Bundes und der Länder (DSK) Muster und allgemeine Hinweise zur Thematik veröffentlicht (Muster z. B. unter: https://www.lda.bayern.de/de/infoblaetter.html)

Da das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30, 24 f., 5 Abs. 1 d DSGVO auf dem aktuellen Stand zu halten ist, sind Nachträge und gegebenenfalls erforderliche neue Verfahrensvermerke stets bei Änderungen, z. B. Einführung neuer Verfahren oder neuer Sicherheitsstandards, auch zukünftig erforderlich. Dies sollte in der internen Struktur organisatorisch und funktionell abgesichert werden.

Im Ergebnis kann die Pflicht zur Führung des Verfahrensverzeichnisses als „gesetzlich normierte Hilfe zur Selbsthilfe“ [Ehmann, Kranig 2018, S. 199 ff.] gewertet werden. Nur wer sich der internen Bestandsaufnahmefunktion des Verzeichnisses und der insgesamt mit der DS-GVO einhergehenden Verpflichtungen bewusst ist, hat die Möglichkeit, dieses Verzeichnis als Hilfestellung, z. B. bei der Wahrung der Betroffenenrechte und der Meldung von Datenschutzverletzungen – wie ganz allgemein dem internen Datenschutzrisikomanagement – zu würdigen.

9) Gemeinsam Verantwortliche nach Art. 26 DS-GVO sowie Auftragsverarbeitung (Art. 28 DS-GVO)

Die Regelungen des Art. 26 DS-GVO in Verbindung mit Art. 4 Nr. 7 DS-GVO für gemeinsam Verantwortliche zielt darauf, transparente Kriterien festzulegen, um eine klare Zuteilung der Verantwortlichkeiten im Innenverhältnis zwischen den in Betracht kommenden Verantwortlichen zu treffen. Im Außenverhältnis zum Betroffenen ändert dies an der Verantwortlichkeit nichts. Der Betroffene kann nach Art. 26 Abs. 3 DS-GVO gegenüber jedem einzelnen Verantwortlichen seine Rechte nach DS-GVO geltend machen. Diese Erleichterung für den Betroffenen entspricht dem Konstrukt der gesamtschuldnerischen Haftung nach § 421 BGB (Martini in: [Paal, Pauly 2018], Art. 26 RN 36).

Im Hinblick auf die Auftragsverarbeitung (Art. 4 Nr. 8 DS-GVO) trifft Art. 28 Abs. 1 DS-GVO die wesentliche Aussage, dass der Verantwortliche bei Auftragsverarbeitung den Auftragnehmer sorgfältig auswählt und nur mit solchen Auftragsverarbeitern zusammenarbeitet, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen getroffen werden, die gewährleisten, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte betroffener Personen absichert. Die Voraussetzungen an die erforderlichen (zumeist vertraglichen) Regelungen gibt Art. 28 Abs. 3 Satz 2 DS-

GVO vor. Daneben ist der Grundsatz nach Art. 28 Abs. 2 Satz 1 DS-GVO (keine Unterauftragsverarbeitung ohne vorherige schriftliche Genehmigung des Verantwortlichen) zu beachten.

Den Auftragsverarbeiter trifft nach der DS-GVO eine erhöhte Verantwortung. Dementsprechend konsequent wird er in die Pflichten zum Datenschutzmanagement eingebunden (beispielhaft s. a. oben Art. 30 Abs. 2, 32 Abs. 1, 33 Abs. 2 DS-GVO) und kann im Schadensfall gleichfalls für einen durch seine Verarbeitung verursachten Schaden verantwortlich sein s. a. Art. 82 ff. DS-GVO. Hält der Auftragsverarbeiter seinerseits genehmigte Verhaltensregeln (Art. 40 DS-GVO) oder ein genehmigtes Zertifizierungsverfahren (Art. 42 DS-GVO) ein, kann dies als Nachweis geeigneter Garantien nach Art. 28 Abs. 5 DS-GVO zu werten sein. Zukünftig werden genehmigte Standardvertragsklauseln (Art. 28 Abs. 7, 8 DS-GVO), Datenschutzsiegel und Prüfzeichen (Art. 42, Art. 28 Abs. 1 DS-GVO) auch im Bereich der Auftragsverarbeitung zur Vereinheitlichung und Arbeitserleichterung in der Praxis beitragen.

Generell bleibt festzustellen, dass viele offene Fragen erst in den kommenden Jahren durch den Europäischen Gerichtshof geklärt werden. Die Leitlinien des Europäischen Datenschutzausschusses, in denen die nationalen Aufsichtsbehörden mitwirken, werden – insbesondere für diese Übergangszeit – von immenser Bedeutung für die Praxis sein.

2 Entwicklungen im Landesdatenschutzrecht Sachsen-Anhalt

Die im Rahmen der europäischen Rechtssetzung erforderlichen Umsetzungs- und Anpassungsakte sind für den Bereich des Landes Sachsen-Anhalt zum Zeitpunkt der Erstellung dieses Aufsatzes (August 2018) nicht vollständig abgeschlossen worden.

Vor dem 25.05.2018 existierte die grundsätzliche Unterteilung mit der Geltung des BDSG für den nicht-öffentlichen Bereich und der Geltung des DSG LSA im öffentlichen Bereich.

Ab dem 25.05.2018 gilt für den nicht-öffentlichen Bereich die DS-GVO und das neue BDSG (Fassung ab 2017, veröffentlicht im BGBl. I, S. 2097).

Auch im öffentlichen Bereich gilt die DS-GVO unmittelbar und zukünftig i. V. m. dem geplanten Datenschutzausfüllungsgesetz LSA (DSAG) und andererseits der JI-RL i. V. m. dem Datenschutzumsetzungsgesetz LSA (DSUG).

Das Datenschutzausfüllungsgesetz (DSAG) wird das DSG LSA zukünftig ablösen und die im Rahmen der DS-GVO eröffneten Regelungsspielräume für den Landesgesetzgeber ausfüllen und zugleich Anpassungen des allgemeinen Datenschutzrechts in Sachsen-Anhalt vornehmen.

Das geplante Gesetz zur Anpassung des Datenschutzrechts in Sachsen-Anhalt an EU-Recht (DSAnpG EU LSA) beinhaltet als Mantelgesetz im Art. 1 das DSAG.

Für die Interimszeit gilt das DSG LSA in der Fassung der Bekanntmachung vom 13. Januar 2016 (GVBl. LSA S. 24) mit der Änderung, die es durch das Gesetz zur Organisationsfortentwicklung des Landesbeauftragten für den Datenschutz und zur Änderung des Informationszugangsgesetzes Sachsen-Anhalt vom 21. Februar 2018 (GVBl. LSA S. 10) bekommen hat.

Das BDSG und das DSG LSA wurden größtenteils durch die DS-GVO ersetzt. Der DS-GVO entgegenstehendes und prinzipiell auch gleich lautendes Recht ist generell aufzuheben bzw. im Sinne der DS-GVO auszulegen und anzuwenden.

Als typisches Beispiel dieser Systematik ist Art. 4 DS-GVO zu erwähnen, der die Begriffsbestimmungen vorgibt und insofern § 2 DSG LSA entsprechend des o. g. Rechtscharakters der DS-GVO verdrängt.

Die neuen Regelungen und vorgegebenen Instrumente der DS-GVO sind in der Praxis umzusetzen. So sind z. B. Datenverarbeitungsprogramme, die vor dem 25. Mai 2018 bereits betrieben wurden, einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO zu unterziehen, wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen darstellt.

Mit dem ersten Umsetzungsakt im Land Sachsen-Anhalt (s. a. oben unter Punkt 1, 4, d. h. mit dem „Gesetz zur Organisationsfortentwicklung des Landesbeauftragten für den Datenschutz und zur Änderung des Informationszugangsgesetzes Sachsen-Anhalt“, in Kraft seit 06.06.2018) wurde u. a. die Organisation des LfD entsprechend den Vorgaben der DS-GVO verselbständigt zur Schaffung einer unabhängigen Aufsichtsbehörde nach Art. 51 ff. DS-GVO.

Derzeit wird ein Gesetz zur Anpassung des Datenschutzrechts in Sachsen-Anhalt an das Recht der EU (DSAnpG EU LSA) erarbeitet, dass in seiner Konzeption im Art. 1 das DSAG beinhaltet.

Die Umsetzung der Richtlinie EU 2016/680, sogenannte JI-RL, erfolgt in Sachsen-Anhalt mittels des Datenschutzrichtlinienumsetzungsgesetzes (DSUG).

Während die DS-GVO nach seiner Rechtsnatur als EU-Verordnung unmittelbar geltendes Recht ab dem 25.05.2018 ist, bedarf die ebenfalls am 27.04.2016 verkündete JI-RL als „Datenschutz-Richtlinie“ der nationalen gesetzgeberischen Umsetzung, die im Land Sachsen-Anhalt mittels des Datenschutzrichtlinienumsetzungsgesetzes (DSUG) erfolgt.

Wichtig ist, dass die Abgrenzung zwischen dem zukünftigen DSAG und dem zukünftigen DSUG nicht behördenbezogen erfolgen kann, sondern sich an der jeweiligen Aufgabe orientiert.

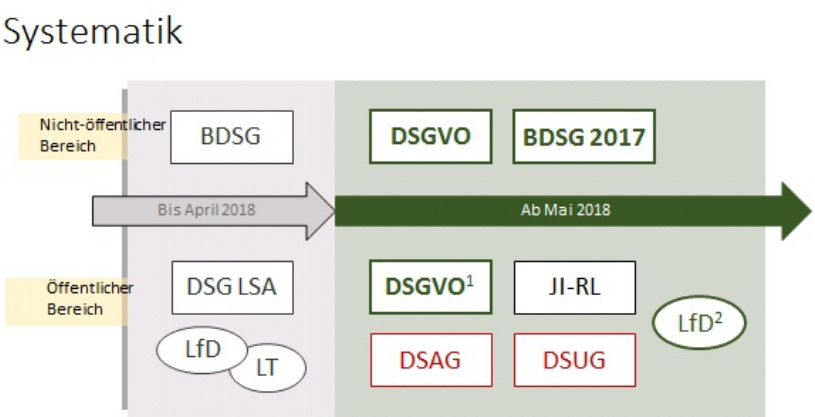
Die Abgrenzung zwischen dem zukünftigen Datenschutzausfüllungsgesetz und dem zukünftigen Datenschutzumsetzungsgesetz erfolgt nicht behördenbezogen, sondern aufgabenbezogen.

Als Hintergrund zum Verständnis ist Folgendes wichtig: die Abgrenzung zwischen den beiden Rechtsakten der Europäischen Union (DS-GVO und JI-RL) erfolgt nicht nach der Zuständigkeit der Behörden, sondern die Abgrenzung erfolgt aufgabenbezogen (s. a. Art. 2 Abs. 2 d DS-GVO). Insoweit wird u. a. auch die kommunale Ebene, die mit ihrer Verwaltungstätigkeit grundsätzlich der unmittelbar geltenden Datenschutz-Grundverordnung unterfällt, immer dann die Richtlinie zu berücksichtigen haben, soweit sie im Bereich der Verfolgung von Ordnungswidrigkeiten (konkret: in der Regel mit Einleitung des Ordnungswidrigkeitsverfahrens) tätig wird und diese Tätigkeiten nicht unmittelbar in den Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) fallen. Ursache dieser in der Praxis durchaus komplexen Abgrenzungsfrage ist der Begriff der „Ordnungswidrigkeit“, der innerhalb der EU außer in Deutschland nur noch in Österreich bekannt ist und aus dem europäischen Blickwinkel unter den Begriff der Straftaten subsumiert wird.

Dieses komplexe Mehrebenensystem hat in der Literatur [Kühling, Sackmann 2018, S. 681 ff.] bereits zu erheblicher Kritik geführt. Für den Rechtsanwender sind zukünftig das grundlegende Verständnis und die Befassung mit der Regelungs-systematik unerlässlich.

3 Vereinfachte systematische Darstellung zur Geltung / dem Zusammenspiel der DS-GVO im datenschutzrechtlichen Kontext sowie der derzeit geplanten landesrechtlichen Regelungen

Erläuterung zur vereinfachten Systematik: Die Abkürzung LfD steht für den Landesbeauftragten für den Datenschutz in Sachsen-Anhalt und die weitere Abkürzung (LT) soll den Landtag Sachsen-Anhalts – bzw. im Kontext die Unabhängigkeit des LfD von den dortigen Strukturen (Haushalt, Personal etc.) – verdeutlichen.



[1] v.a. Art. 6 Abs. 1 c, e; Abs. 2, 3 i. V. m. DSAG/DSG LSA [2] Gesetz zur Organisationsfortentwicklung vom 28.02.2018

Katrin Riep *Anschrift der Autorin*
Datenschutzbeauftragte des Ministeriums für Landesentwicklung und Verkehr des Landes Sachsen-Anhalt
Turmschanzenstraße 30
39114 Magdeburg
E-Mail: Datenschutz@mlv.sachsen-anhalt.de

Literaturverzeichnis

Albrecht, J. 2018:
Die EU-Datenschutzgrundverordnung in 10 Punkten,https://www.janalbrecht.eu/2018/03/2018-01-16-weniger-buerokratie

Bundesregierung 2018:
Antwort der Bundesregierung vom 11.06.2018, auf die Kleine Anfrage der Abgeordneten Lindner, Thomae, Theurer u. a. und der Fraktion der FDP, Bundestags-Drucksache 19/2653 vom 11.06.2018

Ehmann, E., Kranig, T. 2018:
„Fünf nach Zwölf im Datenschutz" in : Zeitschrift für Datenschutz (ZD) Heft 5/2018, S. 199 ff.

Ehmann E., Selmayr M. 2017:
Kommentar zur Datenschutz-Grundverordnung, 1. Auflage 2017

Klug, C. 2017:
„Der Datenschutzbeauftragte in der EU - Maßgaben der Datenschutzgrundverordnung" in: Zeitschrift für Datenschutz (ZD) Heft 5/2017, S. 4 ff.

Kühling J., Sackmann F. 2018:
„Datenschutzordnung 2018- nach der Reform ist vor der Reform?!" in: NVwZ Heft 10/2018, S. 681 bis 702

Paal B., Pauly D. 2018:
Kommentar zur Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 2. Auflage 2018

Schantz, P. 2016:
„Die Datenschutz- Grundverordnung- Beginn einer neuen Zeitrechnung im Datenschutzrecht" in: NJW Heft 26/2016, S. 1841ff

Schneider J. 2017:
Datenschutz nach der EU- Datenschutz-Grundverordnung 2017

Wybitul, T., Haß, D., Albrecht J. 2018:
„Abwehr von Schadensersatzansprüchen nach der Datenschutz-Grundverordnung" in: NJW Heft 3/ 2018, S. 113 ff.

Wybitul, T., von Gierke, L. 2016:
„Checklisten zur DSGVO-Teil 2: Pflichten und Stellung des Datenschutzbeauftragten im Unternehmen" in: BB 2016, S. 100 ff