Ausarbeitung

Zu Anforderungen des Datenschutzes für Abgeordnete

© 2018 Deutscher Bundestag

Zu Anforderungen des Datenschutzes für Abgeordnete

Aktenzeichen:	WD 3 - 3000 - 047/18
Abschluss der Arbeit:	02.03.2018
Fachbereich:	WD 3: Verfassung und Verwaltung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

1. Fragestellung

Die Ausarbeitung thematisiert mögliche Auswirkungen der Datenschutz-Grundverordnung (DSGVO) und des ab dem 28.05.2018 geltenden Bundesdatenschutzgesetzes (BDSG) auf die Arbeit der Abgeordneten bzw. der Abgeordnetenbüros.

2. Vorbemerkung

Die nachfolgenden Ausführungen erheben nicht den Anspruch der Vollständigkeit. Vielmehr sollen Regelungsbereiche des neuen Datenschutzrechts aufgezeigt werden, die auch auf die Arbeit der Abgeordneten Auswirkungen haben können. Da die jeweilige Arbeit in den Abgeordnetenbüros variiert, können sich neben den dargestellten Fallkonstellationen im Einzelfall auch andere, nicht aufgezeigte datenschutzrechtliche Fragestellungen ergeben.

Die Anwendbarkeit der datenschutzrechtlichen Vorschriften auf die Arbeit der Abgeordneten ist in der Rechtspraxis und der juristischen Literatur bisher nicht abschließend geklärt. So ordnen verschiedene Literaturstimmen den Bundestag auch in seiner Funktion als Legislativorgan als öffentliche Stelle des Bundes ein. Bei diesem handele es sich um eine „andere öffentlich-rechtlich organisierte Einrichtung des Bundes“ im Sinne des § 2 Abs. 1 BDSG.[1] Auch die einzelnen Abgeordneten werden teilweise entsprechend rechtlich verortet.[2] Der Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung hat in seiner 39. Sitzung am 25.04.2017 festgestellt, dass die legislative Arbeit der Parlamente von der datenschutzrechtlichen Kontrolle nach der DSGVO und dem BDSG ausgenommen sei.[3] Die vorliegende Ausarbeitung beinhaltet keine rechtliche Aussage zur Frage der Anwendbarkeit der datenschutzrechtlichen Vorgaben auf die Tätigkeit der Abgeordneten. Entsprechend der zugrunde liegenden Fragestellung wird die Anwendbarkeit von DSGVO und BDSG vielmehr unterstellt.

Nach Art. 2 Abs. 2 lit. a DSGVO findet die DSGVO insbesondere keine Anwendung auf Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen. Im Zusammenhang mit dieser Regelung steht § 1 Abs. 8 BDSG. Demnach finden die DSGVO und die Teile 1 und 2 des BDSG auch dann entsprechend Anwendung, wenn die Datenverarbeitung öffentlicher Stellen nicht in den Anwendungsbereich der DSGVO fällt. Voraussetzung ist dann aber, dass keine abweichende gesetzliche Regelung besteht. Mit der Rückverweisung in § 1 Abs. 8 BDSG soll ausweislich der

---

1 Vgl. etwa: Hanloser, in: Wolff/Brink, Datenschutzrecht, 22. Edition Stand: 01.02.2017, § 2 BDSG Rn. 50; Gola/Klug/Körffer, in: Gola/Schomerus, Bundesdatenschutzgesetz, 12. Aufl., 2015, § 2 BDSG Rn. 14; Schafflang/Wiltfang, Bundesdatenschutzgesetz, Stand: März 2009, § 2 BDSG Rn. 8; Schreiber, in: Plath, BDSG/DSGVO 2. Aufl., 2016, § 2 BDSG Rn. 10;
Bergmann/Möhrle/Herb, Datenschutzrecht, Stand: August 2009, § 2 BDSG Rn. 27; Dammann, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl., 2014, § 2 BDSG Rn. 29 f.

2 Vgl. Dammann, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl., 2014, § 2 Rn. 29, wonach Abgeordnete im Rahmen ihrer Mandatsausübung zumindest als nichtöffentliche Stelle gelten. Eine hierzu abweichende Meinung vertreten: Eßer, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, § 2 BDSG Rn. 10; Schreiber, in: Plath, BDSG DSGVO 2. Aufl. 2016, § 2 BDSG Rn. 10.

3 BT-Drs. 18/12144, S. 2.

Gesetzesbegründung ein einheitliches datenschutzrechtliches Vollregime geschaffen werden.[4] Eine Rückausnahme von dieser Regelung enthält jedoch § 85 Abs. 3 BDSG. Die dort genannten Fälle sind von den Informationspflichten sowie vom Auskunftsanspruch ausgenommen.

3. Allgemeine Anforderungen und Grundsätze des Datenschutzes

Die datenschutzrechtlichen Vorgaben beziehen sich auf Verarbeitungsvorgänge, die personenbezogene Daten zum Gegenstand haben. Begrifflich werden sowohl die personenbezogenen Daten als auch deren Verarbeitung in Art. 4 DSGVO definiert.

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.[5]

Ein **Verarbeitungsvorgang** liegt nach Art. 4 Nr. 2 DSGVO in jedem mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jeder solcher Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Hierzu zählen etwa das Erheben, das 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.[6]

Die allgemeinen rechtlichen Vorgaben für die Rechtmäßigkeit einer Datenverarbeitung enthält Art. 6 DSGVO. Danach ist die Verarbeitung von Daten nur dann zulässig, wenn eine **Einwilligung** der betroffenen Person im Sinne des Art. 7 DSGVO vorliegt oder einer der genannten **Erlaubnistatbestände** greift. Die in Art. 6 Abs. 1 DSGVO genannten Erlaubnistatbestände umfassen:

- Die Verarbeitung von Daten für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist oder die zur Durchführung vorvertraglicher Maßnahmen erforderlich sind;

- eine Verarbeitung auf Antrag der betroffenen Person;

---

4 BT-Drs. 18/11325, S. 80.

5 Vgl. umfassend zur Auslegung dieser Definition: Schild, in: Wolff/Brink Datenschutzrecht, 22. Edition Stand: 01.11.2017, Art. 4 DSGVO Rn. 3 ff.; Ernst, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 Art. 4 DSGVO Rn. 3 ff.

6 Vgl. umfassend zur Auslegung dieser Definition: Schild, in: Wolff/Brink Datenschutzrecht, 22. Edition Stand: 01.11.2017, Art. 4 DSGVO Rn. 29 ff.; Ernst, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 Art. 4 DSGVO Rn. 20 ff.

- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, die der Verantwortliche unterliegt;

- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

- die Verarbeitung ist im öffentlichen Interesse oder zur Erfüllung hoheitlicher Aufgaben erforderlich.

In Art. 5 DSGVO sind zudem **Grundsätze** für die Verarbeitung von personenbezogenen Daten geregelt.

Zu diesen zählt etwa der Grundsatz der **Datensparsamkeit** nach Art. 5 Abs. 1 lit. c DSGVO. Danach muss die Verarbeitung personenbezogener Daten dem Zweck angemessen und sachlich relevant sowie auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein.[7]

Einen weiteren relevanten Grundsatz stellt Art. 5 Abs. 1 lit. b DSGVO auf, wonach für die Datenverarbeitung eine enge **Zweckbindung** besteht. Personenbezogene Daten dürfen demnach nur für festgelegte eindeutige und rechtmäßige Zwecke erhoben werden. Eine Weiterverarbeitung ist nur bei Vereinbarkeit mit dem Verwendungszweck möglich, solange keine entsprechende Ausnahmevorschrift greift.[8]

Art. 5 Abs. 1 lit. f und Art. 32 DSVO enthalten die Gewährleistung der **Datensicherheit** als Grundprinzip des Datenschutzrechts. Danach sind Daten durch geeignete technische und organisatorische Maßnahmen vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung zu schützen. Das Schutzniveau muss angemessen sein. Der Grad der Angemessenheit ergibt sich aus dem Risiko eines unberechtigten Zugriffs, der Art der Verarbeitung sowie aus der Bedeutung der Daten für die Rechte und Interessen der betroffenen Personen.[9]

4. Vorgaben für eine wirksame Einwilligung

Die Verarbeitung personenbezogener Daten setzt regelmäßig eine wirksame Einwilligung der betroffenen Person voraus.[10] In Art. 4 Nr. 11 DSGVO wird die Einwilligung definiert. Danach 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

---

7 Vgl. hierzu umfassend: Schantz, in: Wolff/Brink, Datenschutzrecht, 22. Edition Stand: 01.02.2017 Art. 5 DSGVO Rn. 24 ff.

8 Vgl. Frenzel, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 Art. 5 DSGVO Rn. 29 ff.

9 Schantz, in: Wolff/Brink, Datenschutzrecht, 22. Edition Stand: 01.02.2017 Art. 5 DSGVO Rn. 36.

10 Schild, in: Wolff/Brink, Datenschutzrecht, 22. Edition Stand: 01.11.2017 Art. 4 DSGVO Rn. 123.

ist".[11] Weitere Einzelheiten zur Einwilligung einer betroffenen Person sind Art. 7 DSGVO zu entnehmen. Besondere Vorgaben für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft enthält Art. 8 DSGVO. Allgemein beruhen die Vorgaben für die Einwilligung auf den Grundgedanken der **Ausdrücklichkeit** und **Freiwilligkeit**.[12]

5. Informationspflichten und Auskunftsanspruch

In ihrem 2. Abschnitt (Art. 13 ff. DSGVO) enthält die DSGVO Regelungen, die Informationspflichten des Verantwortlichen sowie Auskunftsansprüche des Betroffenen beinhalten. Diese Pflichten sind im Zusammenhang mit § 85 Abs. 3 BDSG zu lesen, wonach für öffentliche Stellen des Bundes unter bestimmten Voraussetzungen weder Informations- noch Auskunftspflichten bestehen.

Art. 13 und 14 DSGVO enthalten **Informationspflichten**, die danach differenzieren, ob die Daten bei der betroffenen Person selbst (Art. 13 DSGVO) oder anderweitig (Art. 14 DSGVO) erhoben werden. Die Betroffenen sind u.a. über die Kontaktdaten des Verantwortlichen, die Verarbeitungszwecke, die angewandten Rechtsgrundlagen, bei Übermittlung in Drittländer über mögliche Empfänger oder Kategorien von Empfängern sowie über die Dauer der Speicherung bzw. die Kriterien für die Festlegung der Speicherdauer zu informieren. Weiterhin sind die Betroffenen über ihre Rechte zu informieren (Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO).[13]

Nach Art. 15 DSGVO steht den Betroffenen zudem ein **Auskunftsrecht** zu. Danach kann eine betroffene Person Auskunft darüber verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, erstreckt sich der Anspruch darüber hinaus auch auf Auskunft über diese personenbezogenen Daten sowie auf verschiedene in Art. 15 Abs. 1 DSGVO genannte Informationen.[14] Der Auskunftsanspruch besteht nach h.M. grundsätzlich auch dann, wenn ein Anspruchsteller ihn „ins Blaue hinein" geltend macht.[15] Lediglich im Falle von offenkundigem Rechtsmissbrauch kann die Auskunft verweigert werden.[16]

Eine wichtige **Ausnahme** zu den aufgezeigten Informationspflichten bzw. Auskunftsansprüchen enthält § 85 Abs. 3 BDSG. Die Vorschrift stellt eine Ausnahmeregelung zu § 1 Abs. 8 BDSG dar,

---

11 Umfassend zu dieser Definition: Ernst, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018, Art. 4 DSGVO Rn. 61 ff.

12 Vgl. Ernst, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 Art. 7 DSGVO Rn. 2.

13 Weitere Informationen zu den genannten Pflichten sind dem Kurzpapier Nr. 10 zum Thema „Informationspflichten bei Dritt- und Direkterhebung" der Datenschutzkonferenz zu entnehmen. Abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_Informationspflichten.pdf?__blob=publicationFile&v=3 (Stand 27.02.2018).

14 Weitere Informationen zu den genannten Pflichten sind dem Kurzpapier Nr. 6 zum Thema „Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO" der Datenschutzkonferenz zu entnehmen. Abrufbar unter: file://parlament/daten/DP_wd3-1/Buero/Kurzpapier_Auskunftsrecht.pdf (Stand 27.02.2018).

15 Vgl. nur: Dix, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl., 2014, § 34 BDSG Rn. 12; eine einschränkende Sicht vertrat etwa das LAG Hessen, Urt. v. 29.01.2013 - 13 Sa 263/12, ZD 2013, 413.

16 Vgl. Schmidt-Wudy, in: Wolff/Brink, Datenschutzrecht, 22. Edition, Stand: 01.11.2017, § 34 BDSG Rn. 90.

wonach die DSGVO für die Datenverarbeitung öffentlicher Stellen auch außerhalb ihres Anwendungsbereiches gelten soll, wenn keine speziellen Regelungen existieren.[17] Nach § 85 Abs. 3 BDSG gilt dies jedoch nicht für Tätigkeiten öffentlicher Stellen des Bundes, die nicht in den Anwendungsbereich der DSGVO fallen, wenn es sich um Fälle des § 32 Abs. 1 Nr. 1 bis 3 BDSG handelt oder durch ihre Erfüllung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen, und deswegen das Interesse der betroffenen Person an der Erteilung der Information zurücktreten muss (§ 85 Abs. 3 BDSG). Ausweislich der Gesetzesbegründung ist die Regelung erforderlich, um bei Verarbeitungen personenbezogener Daten im Bereich der nationalen Sicherheit und der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung, die nicht spezialgesetzlich geregelt sind, die bisherigen Ausnahmen von den Informationspflichten aus § 19a Absatz 3 i. V. m. § 19 Absatz 4 BDSG a. F. zu erhalten.[18] Darüber hinaus beinhaltet insbesondere der Verweis auf § 32 Abs. 1 Nr.1 BDSG eine Einschränkung zugunsten kleinerer und mittlerer Einrichtungen, die Daten analog verarbeiten.[19]

Eine Einschränkung wäre auch durch Art. 47 S. 1 GG denkbar. Demnach haben Abgeordnete ein Zeugnisverweigerungsrecht. Dieses Recht bezieht sich jedoch nur auf behördliche und gerichtliche Verfahren und würde gerade nicht gegen einen Auskunftsanspruch eines Privaten geltend gemacht werden können.[20]

6. Recht auf Berichtigung und Löschung

Ein Recht auf **Berichtigung** und **Vervollständigung** enthält Art. 16 DSGVO. Eine betroffene Person kann die Berichtigung sowie ggf. die Vervollständigung sie betreffender unzutreffender oder unvollständiger personenbezogener Daten verlangen. Der Anspruch dient vorrangig dem Ziel der Daten-Richtigkeit.[21]

Nach Art. 17 Abs. 1 DSGVO steht einem Betroffenen unter bestimmten Umständen ein **Löschungsanspruch** zu. Dieser besteht insbesondere dann, wenn nach Art. 17 Abs. 1 lit. a DSGVO die erhobenen Daten für den Zweck, für den sie erhoben wurden, nicht mehr erforderlich sind oder eine betroffene Person ihre Einwilligung widerruft (Art. 17 Abs. 1 lit. b DSGVO). Einen besonderen Fall des Löschungsrechts regelt Art. 17 Abs. 2 DSGVO mit dem **„Recht auf**

---

17 Wolff, in: Wolff/Brink, Datenschutzrecht, 22. Edition, Stand: 01.08.2017, § 85 BDSG Rn. 20.

18 Vgl. BT-Drs. 18/11325, S. 121.

19 Zu den Einzelheiten dieser Regelung: Hennemann, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018, § 32 BDSG Rn. 13.

20 Magiera, in: Sachs, 8. Aufl. 2017, Art. 47 GG Rn. 6.

21 Paal, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 Art. 16 DSGVO Rn. 4.

Vergessenwerden“.[22] Dieser Anspruch richtet sich darauf, unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, zu ergreifen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass ein Löschungsantrag vorliegt. Mit dem Anspruch soll einer massenweisen Verbreitung von personenbezogenen Daten im Internet begegnet werden. Es besteht jedoch kein Recht auf einen bestimmten Löschungserfolg, sondern lediglich auf „angemessene Maßnahmen“.[23] Inwieweit diese Regelung praktisch umsetzbar ist, wird in der Literatur durchaus unterschiedlich beurteilt.[24]

7. Technische und organisatorische Maßnahmen

Ein Verantwortlicher muss nach Art. 24 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorgaben sicherzustellen. Diesem Grundsatz folgend beinhaltet Art. 25 DSGVO besondere Regelungen für die **Technikgestaltung** und **datenschutzfreundliche Voreinstellungen**.

Der Datenschutz soll gem. Art. 25 Abs. 1 DSGVO durch die frühzeitige Umsetzung geeigneter **technischer und organisatorischer Maßnahmen** in der Datenverarbeitung sichergestellt werden. Die zu ergreifenden Maßnahmen sollen dabei der Umsetzung der datenschutzrechtlichen Grundsätze (vgl. Art. 5 DSGVO) dienen.[25] Auf technischer Seite sind vor allem Vorkehrungen physischer Natur wie etwa das Verschließen von Datenträgern denkbar oder die Schaffung einer hinreichenden IT-Sicherheit (z.B. Passwortschutz, Verschlüsselung von Daten). Organisatorische Maßnahmen betreffen die Umstände der Datenverarbeitung, wie etwa den zugangsberechtigten Personenkreis.[26] Der Umfang der zu ergreifenden Maßnahmen ist im Rahmen einer Gesamtabwägung zu bestimmen, deren Abwägungsgegenstände Art. 25 Abs. 1 DSGVO näher benennt. Allgemein müssen umfassendere Maßnahmen ergriffen werden, je sensibler die Daten und je höher die Risiken für die betroffenen Personen sind.[27]

Datenschutzfreundliche Voreinstellungen nach Art. 25 Abs. 2 DSGO sollen sicherstellen, dass nur solche personenbezogenen Daten verarbeitet werden, die für den konkreten Verarbeitungszweck erforderlich sind. Dies betrifft den Umfang der Datenverarbeitung, die Menge der Daten,

---

22 Umfassende Informationen zu den genannten Rechten sind dem Kurzpapier Nr. 11 „Recht auf Löschung / „Recht auf Vergessenwerden“ der Datenschutzkonferenz zu entnehmen. Abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_RechtaufVergessenwerden.pdf?__blob=publicationFile&v=2 (Stand 27.02.2018).

23 Paal, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 Art. 17 DSGVO Rn. 32.

24 Vgl. nur m.w.N. Worms, in: Wolff/Brink, Datenschutzrecht, 22. Edition, Stand: 01.08.2017, Art. 17 DSGVO Rn. 61.

25 Martiny, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 Art. 25 DSGVO Rn. 27.

26 Martiny, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 Art. 25 DSGVO Rn. 28.

27 So der Bayrische Landesbeauftragte für den Datenschutz: https://www.datenschutz-bayern.de/datenschutzreform2018/technik_und_sicherheit.html (Stand 27.02.2018).

ihre Speicherfrist und ihre Zugänglichkeit. Damit soll erreicht werden, dass die gespeicherten Daten nicht einer unbestimmten Personenzahl zugänglich gemacht werden.[28]

Ein Nachweis über die Einhaltung der aufgezeigten Anforderungen ist über ein genehmigtes **Zertifizierungsverfahren** möglich. Art. 25 Abs. 3 DSGVO enthält hierfür einen ausdrücklichen Verweis.

Nach Art. 24 Abs. 1 S. 2 DSGVO müssen die ergriffenen Maßnahmen erforderlichenfalls **überprüft** und **aktualisiert** werden. Der Bayrische Landesbeauftragte für den Datenschutz geht hierfür derzeit von einem Zwei- bis Drei-Jahres-Rhythmus aus.[29]

8. Verzeichnisführung

Nach Art. 30 Abs. 1 DSGVO führen jeder Verantwortliche und gegebenenfalls sein Vertreter ein **Verzeichnis aller Verarbeitungstätigkeiten**, die ihrem Zuständigkeitsbereich unterliegen. Die Norm listet sodann Angaben auf, die zwingend in das Verzeichnis aufgenommen werden müssen. Eine Erleichterung von dieser Vorgabe enthält Art. 30 Abs. 5 DSGVO für Unternehmen bzw. Einrichtungen mit weniger als 250 Mitarbeitern. Voraussetzung für diese Ausnahme ist jedoch, dass die Datenverarbeitung keine Risiken für die Rechte und Freiheiten der Betroffenen birgt, nur gelegentlich erfolgt und keine besonders geschützten Daten betroffen sind. Datenverarbeitungen für die Lohnbuchhaltung oder bei der Führung von Personalakten erfolgen in der Regel nicht gelegentlich. In diesen Bereichen dürften daher auch kleinere Einrichtungen weiterhin von der Pflicht zur Verzeichnisführung betroffen sein.[30]

9. Meldepflichten

Im Falle einer Verletzung des Schutzes personenbezogener Daten muss diese nach Art. 33 Abs. 1 DSGVO unverzüglich nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls der zuständigen Aufsichtsbehörde gemeldet werden. Nach Art. 34 DSGVO muss zudem der Betroffene unverzüglich benachrichtigt werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für seine persönlichen Rechte und Freiheiten zur Folge hat. Eine Meldung kann nach Art. 33 Abs. 1 DSGVO unterbleiben, wenn die Verletzung nicht zu einem Risiko für die Rechte und Freiheiten einer betroffenen natürlichen Person führt. Ein solcher Risikoausschluss kann etwa durch die Verschlüsselung von Daten sichergestellt werden und ist im Rahmen einer Prognoseentscheidung zu bestimmen.[31]

---

28 Paulus, in: Wolff/Brink, Datenschutzrecht, 22. Edition, Stand: 01.08.2017, Art. 25 DSGVO Rn. 12.

29 https://www.datenschutz-bayern.de/datenschutzreform2018/technik_und_sicherheit.html (Stand 27.02.2018).

30 Vgl. v. Schenk/Mueller-Stöfen, Die Datenschutz-Grundverordnung: Auswirkungen in der Praxis, GWR 2017, 171 (173).

31 Vgl. Brink, in: Wolff/Brink, Datenschutzrecht, 22. Edition, Stand: 01.11.2017, Art. 33 DSGVO Rn. 34 ff.

10. Datenverarbeitung zu anderen Zwecken durch öffentliche Stellen

In § 23 BDSG sind Voraussetzungen geregelt, nach denen Datenverarbeitungen durch öffentliche Stellen zu anderen Zwecken zulässig sind. Wie oben dargestellt wurde, stellt die Zweckbindung einen Grundsatz der Datenverarbeitung nach Art. 5 Abs. 1 lit. b DSGVO dar. Ausweislich der Gesetzesbegründung beinhaltet die Regelung in § 23 BDSG eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch denselben Verarbeiter zu einem anderen Zweck als zu demjenigen, zu dem er sie ursprünglich erhoben hat (Weiterverarbeitung). Soweit eine der tatbestandlichen Voraussetzungen nach Absatz 1 erfüllt ist, kann die Weiterverarbeitung personenbezogener Daten durch öffentliche Stellen auf diese Vorschrift gestützt werden.[32]

11. Datenübermittlung durch öffentliche Stellen

Nach § 25 BDSG können personenbezogene Daten unter bestimmten Voraussetzungen von öffentlichen Stellen übermittelt werden. Die Vorschrift bildet die Rechtsgrundlage für die Übermittlung personenbezogener Daten durch öffentliche Stellen soweit diese zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, erfolgt.[33]

***

32 BT-Drs. 18/11325, S. 95.

33 BT-Drs. 18/11325, S. 96.