Infobrief

Datenschutzrecht für Abgeordnete

Daniel Mundil

Datenschutzrecht für Abgeordnete

Verfasser/in: Regierungsrat Dr. Daniel Mundil
Aktenzeichen: WD 3 - 3010 - 056/18
Abschluss der Arbeit: 20.03.2018
Fachbereich: WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Einleitung

Der Infobrief thematisiert mögliche Auswirkungen der Datenschutz-Grundverordnung (DSGVO)[1] und des ab dem 25.05.2018 geltenden Bundesdatenschutzgesetzes (BDSG)[2] auf die Arbeit der Abgeordneten bzw. Abgeordnetenbüros und Fraktionen im Deutschen Bundestag. Die DSGVO gilt unmittelbar im innerstaatlichen Rechtsraum und verdrängt sämtliche ihr entgegenstehenden nationalen Vorschriften. Sie ist daher Ausgangspunkt für die Prüfung datenschutzrechtlicher Fragestellungen. Das neue BDSG nimmt diesen Regelungsansatz auf und enthält vor allem Ausführungs- bzw. Ergänzungsregelungen zur DSGVO. Für bestehende Regelungsspielräume, die die DSGVO den nationalen Gesetzgebern einräumt, enthält das BDSG zudem eigene gesetzliche Ausgestaltungen.

In den folgenden Ausführungen wird zunächst dargestellt, inwieweit die neuen datenschutzrechtlichen Vorgaben überhaupt Anwendung im parlamentarischen Bereich finden. Darüber hinaus werden einzelne datenschutzrechtliche Regelungsbereiche aufgezeigt, die möglicherweise im parlamentarischen Bereich Anwendung finden könnten. Die Aufzählung ist nicht abschließend zu verstehen. Aufgrund der Unterschiedlichkeit der verschiedenen Arbeitsbereiche und auch der Organisation insbesondere der Abgeordnetenbüros müssen datenschutzrechtliche Anforderungen im Einzelfall ermittelt werden. Die Ausführungen sollen dabei helfen, entsprechende relevante Bereiche zu erkennen und mögliche Problemlagen zu vermeiden.

Bei den Neuregelungen des Datenschutzrechts wird es mangels hinreichender Praxiserfahrungen für eine rechtssichere Organisation der einzelnen Arbeitsbereiche unumgänglich sein, die Entwicklung der Verwaltungspraxis der Aufsichtsbehörden sowie Gerichtsentscheidungen zu beobachten und die Datenverarbeitungsstandards gegebenenfalls anzupassen.

2. Anwendbarkeit der datenschutzrechtlichen Vorgaben

Bei der Anwendbarkeit der datenschutzrechtlichen Vorgaben sind zwei Komplexe zu unterscheiden. Zunächst ist zu bestimmen, inwieweit die datenschutzrechtlichen Regelungen sachlich Anwendung im parlamentarischen Bereich finden. Darauf aufbauend müsste gegebenenfalls geklärt werden, inwieweit für den parlamentarischen Bereich eine mögliche Bereichsausnahme der datenschutzrechtlichen Regelungen besteht.

2.1. Sachlicher Anwendungsbereich der Datenschutz-Grundverordnung

Die zentrale Vorschrift für die sachliche Anwendbarkeit der DSGVO beinhaltet Art. 2. Danach gilt diese für die ganz oder teilweise automatisierte **Verarbeitung personenbezogener Daten** sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Wichtige Bereichsausnahmen enthält Art. 2 Abs. 2 DSGVO. Insbesondere nach Art. 2 Abs. 2 lit. a DSGVO findet die DSGVO keine Anwendung auf

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, ABl. Nr. L 119 vom 04.05.2016 S. 1.

2 BGBl. I Nr. 44 v. 05.07.2017, S. 2097 ff.; soweit in den weiteren Ausführungen das BDSG zitiert wird, ist damit die ab dem 25.05.2018 geltende Fassung gemeint.

die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt. Nicht in den Anwendungsbereich des Unionsrechts fallen insbesondere nach dem 16. Erwägungsgrund zur DSGVO Tätigkeiten, die die nationale Sicherheit betreffen.[3]

Es ließe sich bereits an dieser Stelle durchaus vertreten, dass die Organisation der nationalen Parlamente sowie auch die Ausgestaltung des Abgeordnetenmandats grundsätzlich nicht in den Anwendungsbereich des Unionsrechts fallen, da sich die Grundlagen der parlamentarischen Arbeit allein aus den nationalen verfassungsrechtlichen Regelungen ergeben. Nach Art. 4 Abs. 2 S. 1 des EU-Vertrages (EUV) achtet die Union die nationale Identität, die in ihren grundlegenden politischen und verfassungsmäßigen Strukturen zum Ausdruck kommt. Ordnet man den innerparlamentarischen Datenschutz diesen dem Unionsrecht grundsätzlich entzogenen Strukturen zu, ließe sich auch begründen, dass dieser nicht in den Anwendungsbereich des Unionsrechts fiele. Bei diesem Ansatz würde folglich auch die DSGVO keine Anwendung finden. Dennoch sollte nicht ausgeblendet werden, dass insbesondere in den Fraktionen und von den Abgeordneten auch unionsrechtliche Vorgaben direkt oder mittelbar angewendet werden (etwa im Arbeitsrecht).

Eine fehlende sachliche Anwendbarkeit der Datenschutz-Grundverordnung nach Art. 2 Abs. 2 DSGVO würde aber nicht zu einem zwingenden Ausschluss der Anwendbarkeit führen. Nach § 1 Abs. 8 BDSG finden für Verarbeitungsvorgänge personenbezogener Daten öffentlicher Stellen, die nicht in den Anwendungsbereich der Datenschutz-Grundverordnung fallen, deren Regelungen dennoch Anwendung, soweit im BDSG oder anderen Vorschriften nichts Abweichendes geregelt ist. Der Gesetzgeber wollte durch diesen Rückverweis ein einheitliches datenschutzrechtliches Vollregime schaffen.[4] Soweit man Fraktionen und Abgeordnete daher als öffentliche Stelle im datenschutzrechtlichen Sinne einordnet (dazu sogleich), würden zumindest über den Rückverweis in § 1 Abs. 8 BDSG die Regelungen der Datenschutz-Grundverordnung entsprechend Anwendung finden.

2.2. Bereichsausnahme für den parlamentarischen Bereich?

Es stellt sich daher die Frage, ob die datenschutzrechtlichen Vorgaben für den parlamentarischen Bereich, namentlich auf Fraktionen und Abgeordnete, überhaupt Anwendung finden oder ob möglicherweise von einer entsprechenden **Bereichsausnahme** ausgegangen werden muss. Ausdrückliche Regelungen hierzu enthält weder die Datenschutz-Grundverordnung noch das neue Bundesdatenschutzgesetz. Im Gegensatz hierzu stehen etwa Regelungen der Bundesländer, die für die Landesparlamente entsprechende Bereichsausnahmen geschaffen haben.[5] Der Datenschutz-

---

3 Vgl. auch: Ernst, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 2 DSGVO Rn. 11.

4 Vgl. BT-Drs. 18/11325, S. 80; Ernst, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 § 1 BDSG Rn. 18.

5 Vgl. etwa: § 2 Abs. 2 des Niedersächsischen Datenschutzgesetzes, wo es heißt: „Der Landtag, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten unterliegen nicht den Bestimmungen dieses Gesetzes, soweit sie bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten und dabei die vom Landtag erlassene Datenschutzordnung anzuwenden haben.“ Vgl. zudem: § 2 Abs. 2 des Landesdatenschutzgesetzes Rheinland-Pfalz; vgl. auch: Art. 1 Abs. 1 S. 2 im Entwurf für ein Bayerisches Datenschutzgesetz, LT-Drs. 17/19628, S. 6 u. 31.

Grundverordnung und dem Bundesdatenschutzgesetz können hingegen lediglich Sonderregelungen für die Arbeit der Gerichte entnommen werden (vgl. etwa: Art. 55 Abs. 3 DSGVO; § 9 Abs. 2 BDSG).

In der rechtswissenschaftlichen Literatur ist die Auseinandersetzung mit dieser Frage nicht abschließend geklärt. Die meisten **Literaturstimmen** ordnen den **Bundestag** und seine **Untergliederungen** als öffentlich-rechtlich organisierte Einrichtung des Bundes und damit als öffentliche Stelle ein.[6] Dabei wird zumeist ohne nähere Begründung davon ausgegangen, dass auch **Fraktionen** zu diesen Untergliederungen zu zählen sind.[7] Auch diese würden daher als **öffentliche Stelle** in den Anwendungsbereich der datenschutzrechtlichen Vorgaben fallen.

Nur wenige Literaturstimmen setzen sich hingegen mit der Stellung der **Abgeordneten** auseinander. Vertreten wird dabei zumeist ohne nähere Begründung, dass Abgeordnete **nicht** als **öffentliche Stelle** angesehen werden können.[8] Lediglich vereinzelt wird diese Auffassung auch ausdrücklich erörtert.[9] Dieser Ansatz lässt sich jedoch gerade im Hinblick auf die Einordnung der Fraktionen als öffentliche Stelle nur schwer begründen. Auch das **Abgeordnetenmandat** ist durch **öffentlich-rechtliche Regelungen**, namentlich durch das Verfassungsrecht und die Regelungen im Abgeordnetengesetz, geprägt. Zudem ist auch eine abweichende Einordnung im Vergleich zu den Fraktionen nicht schlüssig. Fraktionen leiten ihren Status aus dem der Abgeordneten her.[10] Ordnet man sie daher als öffentliche Stellen ein, muss dies auch für Abgeordnete gelten. Jedenfalls für die Ausübung der Mandatstätigkeit liegt es daher nahe, Abgeordnete ebenfalls als **öffentliche Stelle** anzusehen. Eine Einordnung der Abgeordneten als nichtöffentliche Stelle hätte zudem auch rechtspraktisch negative Folgen. So würden die Abgeordneten im Einzelfall anderen datenschutzrechtlichen Regelungen unterliegen als die Fraktionen und zudem in den Zuständigkeitsbereich der jeweiligen Landesdatenschutzbeauftragten als Aufsichtsbehörde fallen. Eine Trennung der rechtlichen Regelungen und der Aufsicht von Fraktionen und Abgeordneten erscheint jedoch bereits wegen der engen Verknüpfung der Tätigkeitsbereiche nicht sinnvoll.

Ordnet man Abgeordnete und Fraktionen hingegen als öffentliche Stelle im Sinne des § 2 Abs. 1 BDSG ein, so unterliegen diese den gleichen datenschutzrechtlichen Vorgaben. Nach § 1 Abs. 8 BDSG würden dann auch die Regelungen der Datenschutz-Grundverordnung grundsätzlich entsprechend Anwendung finden.

Denkbar ist über diese Erwägungen hinaus auch, aus dem Grundsatz der Gewaltenteilung eine ungeschriebene Ausnahme vom aufgezeigten Anwendungsbereich der datenschutzrechtlichen Regelungen bzw. zumindest hinsichtlich der datenschutzrechtlichen Aufsicht im parlamentarischen

---

6 Vgl. nur: Gola/Klug/Körffer, in: Gola/Schomerus, 12. Auflage 2015, § 2 BDSG Rn. 17a; Ernst, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 § 2 BDSG Rn. 5; Schreiber, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 2 BDSG Rn. 10; Eßer, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, § 2 BDSG Rn. 10.

7 Vgl. Schreiber, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 2 BDSG Rn. 10; Eßer, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, § 2 BDSG Rn. 10.

8 Vgl. Schreiber, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 2 BDSG Rn. 10; Eßer, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, § 2 BDSG Rn. 10, unter Verweis auf: Dammann, in: Simitis, 8. Aufl. 2014, § 2 BDSG Rn. 30.

9 Dammann, in: Simitis, 8. Aufl. 2014, § 2 BDSG Rn. 30.

10 Vgl. Butzer, in: Epping/Hillgruber, 35. Edition Stand: 15.11.2017, Art. 38 GG Rn. 136.

Bereich herzuleiten. So stellte der **Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung** in seiner 39. Sitzung am 25.04.2017 Folgendes fest:

> „Die DS-GVO darf die innerstaatliche Gewaltenteilung, die ein allen Verfassungen der EU-Mitgliedstaaten immanentes Prinzip ist, nicht aushebeln. Dies folgt aus Artikel 2 Abs. 2 lit. a DS-GVO, wonach Verarbeitungen personenbezogener Daten im Rahmen von Tätigkeiten aus dem Anwendungsbereich der DS-GVO und der nationalen Umsetzungsgesetze ausgenommen sind, die nicht in den Anwendungsbereich des Unionsrechts fallen. Alle Kontrollrechte und weiteren Befugnisse, welche die Exekutive in Gestalt der Datenschutzbeauftragten auf Bundes- und Landesebene aufgrund europarechtlicher Zuweisung erhält, darf sie nur im Rahmen des verfassungsrechtlich Zulässigen ausüben. Ausgenommen von der datenschutzrechtlichen Kontrolle nach der DS-GVO und dem BDSG-neu ist daher die legislative Arbeit der deutschen Parlamente. Dazu gehört insbesondere die Tätigkeit des Präsidiums und des Ältestenrates, der Ausschusssekretariate, der Fraktionen und Gruppen sowie der Abgeordnetenbüros – sowohl des Bundestages als auch der Landesparlamente.“[11]

Der Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung stellte jedenfalls eine **Ausnahme** von der **Kontrollzuständigkeit** der **Aufsichtsbehörde** für den parlamentarischen Bereich fest. Wie in der bisherigen Praxis würde es daher auch zukünftig im Rahmen einer verfassungskonformen Interpretation der datenschutzrechtlichen Vorgaben bei einem Kooperationsverhältnis zwischen Aufsichtsbehörde und Parlament bleiben, ohne dass Kontrollbefugnisse ausgeübt werden würden.

In der Literatur wird dennoch davon ausgegangen, dass diese Ausnahme von der Kontrolle die Geltung der materiellen **datenschutzrechtlichen Vorgaben** auch im parlamentarischen Bereich **unberührt** lässt.[12] Die Tätigkeit der Abgeordneten und der Fraktionen würde daher einem ähnlichen Regelungssystem unterliegen, wie es für die richterliche Tätigkeit gilt. Nach Art. 55 Abs. 3 DSGVO und § 9 Abs. 2 BDSG ist diese lediglich von der Aufsicht ausgenommen. Dennoch sind die datenschutzrechtlichen Regelungen bei Ausübung der richterlichen Tätigkeit anzuwenden und im Wege der **Selbstkontrolle** zu beachten.[13] Fraktionen und Abgeordnete wären bei Zugrundelegung dieser Sichtweise ebenfalls an die Vorgaben des Datenschutzrechts gebunden, würden aber keiner Kontrolle durch eine Aufsichtsbehörde unterliegen. Die Einhaltung der datenschutzrechtlichen Vorgaben müsste vielmehr im Rahmen der beschriebenen Selbstkontrolle erfolgen. An dieser Stelle sei jedoch darauf hingewiesen, dass eine abschließende gerichtliche Klärung dieser unklaren Rechtslage aufgrund der neu geschaffenen Rechtsbehelfsmöglichkeiten (vgl. hierzu die Ausführungen unter Ziff. 15) nicht unwahrscheinlich erscheint. Darüber hinaus könnte auch ohne eine aufsichtsbehördliche Kontrolle die Einhaltung der datenschutzrechtlichen Vorgaben über die Inanspruchnahme von Rechtsbehelfen durchgesetzt werden.

---

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

12 Zum Ganzen: Dammann, in: Simitis, 8. Aufl. 2014, § 2 BDSG Rn. 30.

13 Eichler, in: Wolff/Brink, Datenschutzrecht, 22. Edition, Stand: 01.11.2017, Art. 55 DSGVO Rn. 11; vgl. auch den 20. Erwägungsgrund zur DSGVO.

3. Datenschutzrechtliche Begriffe

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.[14] Es kommt vereinfacht ausgedrückt immer darauf an, ob eine Information einer bestimmten Person zugeordnet werden kann.

Eine **Verarbeitung** 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, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.[15] Jeder dieser aufgezeigten Vorgänge stellt einen selbstständigen Verarbeitungsvorgang dar. Daher ist auch für jeden einzelnen dieser Vorgänge zu prüfen, ob dieser den datenschutzrechtlichen Vorgaben entspricht. Werden etwa Daten zulässigerweise erhoben, schließt dies nicht zwingend mit ein, dass diese auch übermittelt werden dürfen.[16]

4. Allgemeine Anforderungen und Grundsätze

4.1. Rechtmäßigkeit der Datenverarbeitung

Die allgemeinen rechtlichen Vorgaben für die Rechtmäßigkeit einer Datenverarbeitung enthält Art. 6 DSGVO. Die Aufzählung ist jedenfalls für den Anwendungsbereich der Datenschutz-Grundverordnung weitgehend abschließend zu verstehen.[17] 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 nachfolgenden **Erlaubnistatbestände** greift. Die in Art. 6 Abs. 1 DSGVO genannten Erlaubnistatbestände umfassen:

---

14 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.

15 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.

16 Vgl. hierzu bereits zum bisherigen Recht: Gola/Klug/Körffer, in: Gola/Schomerus, 12. Auflage 2015, § 4 BDSG Rn. 5; zudem spricht der 39. Erwägungsgrund zur DSGVO davon, dass „jede Verarbeitung“ rechtmäßig zu erfolgen hat.

17 Albers, in: Wolff/Brink Datenschutzrecht, 22. Edition Stand: 01.11.2017, Art. 6 DSGVO Rn. 17.

- 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,

- 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,

- die Verarbeitung ist zur Wahrung der berechtigten **Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, **überwiegen**, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Außerhalb einer Einwilligung kommt es für die Zulässigkeit einer Datenverarbeitung zudem darauf an, dass neben einem der genannten Kriterien auch das Merkmal der **Erforderlichkeit** erfüllt wird. Hierzu reicht es nicht aus, dass die Datenverarbeitung einem der genannten Kriterien nutzt. Vielmehr muss ohne sie eine Erfüllung der jeweiligen Aufgabe nicht, nicht vollständig oder nicht rechtmäßig möglich sein.[18] Im Ergebnis wird es außerhalb einer Datenverarbeitung auf Grundlage einer Einwilligung daher darauf ankommen, dass eines der in Art. 6 DSGVO genannten Kriterien vorliegt und die Datenverarbeitung im Rahmen einer wertenden Abwägungsentscheidung hierfür auch erforderlich ist.

4.2. Grundsätze für die Datenverarbeitung

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

Zu diesen zählt etwa der Grundsatz der **Datenminimierung** 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.[19]

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

---

18 Albers, in: Wolff/Brink Datenschutzrecht, 22. Edition Stand: 01.11.2017, Art. 6 DSGVO Rn. 17.

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

festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Eine Weiterverarbeitung ist nur bei Vereinbarkeit mit dem Verwendungszweck möglich, solange keine entsprechende Ausnahmevorschrift greift.[20]

Art. 5 Abs. 1 lit. f und Art. 32 DSGVO 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.[21]

5. Vorgaben für eine wirksame Einwilligung

Die Verarbeitung personenbezogener Daten setzt regelmäßig eine wirksame Einwilligung der betroffenen Person voraus.[22] 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 ist“.[23] 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**.[24]

6. Informationspflichten und Auskunftsansprüche

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 Verarbeitungs-

---

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

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

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

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

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

zwecke, 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).[25] Eine Datenerhebung, die eine entsprechende Informationspflicht auslöst, kann dabei bereits in alltäglichen Vorgängen liegen, etwa dem Eingang einer Bewerbung oder eines Bürgerbriefes.

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.[26] Der Auskunftsanspruch besteht nach herrschender Meinung in der juristischen Literatur grundsätzlich auch dann, wenn ein Anspruchsteller ihn „ins Blaue hinein“ geltend macht.[27] Lediglich im Falle von offenkundigem Rechtsmissbrauch kann die Auskunft verweigert werden.[28]

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, wonach die DSGVO für die Datenverarbeitung öffentlicher Stellen auch außerhalb ihres Anwendungsbereiches gelten soll, wenn keine speziellen Regelungen existieren.[29] 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. 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 Abs. 3 i. V. m. § 19 Abs. 4 BDSG a. F. zu

---

25 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).

26 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).

27 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.

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

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

erhalten.[30] Darüber hinaus beinhaltet insbesondere der Verweis auf § 32 Abs. 1 Nr.1 BDSG eine Einschränkung zugunsten kleinerer und mittlerer Einrichtungen, die Daten analog verarbeiten.[31]

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.[32]

7. Betroffenenrechte

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.[33]

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 Vergessenwerden“**.[34] 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“.[35] Inwieweit diese Regelung praktisch umsetzbar ist, wird in der Literatur durchaus unterschiedlich beurteilt.[36]

---

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

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

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

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

34 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).

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

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

8. Technische und organisatorische Maßnahmen

Ein Verantwortlicher muss nach Art. 24 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorgaben sicherstellen. 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.[37] 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.[38] Der Umfang der zu ergreifenden Maßnahmen ist im Rahmen einer Gesamtabwägung zu bestimmen, deren Abwägungsgegenstände Art. 25 Abs. 1 DSGVO näher benennt. Allgemein müssen desto umfassendere Maßnahmen ergriffen werden, je sensibler die Daten und je höher die Risiken für die betroffenen Personen sind.[39]

Datenschutzfreundliche Voreinstellungen nach Art. 25 Abs. 2 DSGVO 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, ihre Speicherfrist und ihre Zugänglichkeit. Damit soll erreicht werden, dass die gespeicherten Daten nicht einer unbestimmten Personenzahl zugänglich gemacht werden.[40]

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 Bayerische Landesbeauftragte für den Datenschutz geht hierfür derzeit von einem Zwei- bis Drei-Jahres-Rhythmus aus.[41]

---

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

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

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

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

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

9. Bestellung eines Datenschutzbeauftragten

Soweit man Fraktionen und Abgeordnete als öffentliche Stelle im Sinne des § 2 Abs. 1 BDSG einordnet, sind sie gemäß Art. 37 Abs. 1 lit. a DSGVO, § 5 Abs. 1 S. 1 BDSG **verpflichtet**, einen **Datenschutzbeauftragten** zu benennen.[42] Auf die Anzahl der Beschäftigten kommt es nicht an. Nach Art. 37 Abs. 1 lit. a DSGVO muss der Verantwortliche „auf jeden Fall" einen Datenschutzbeauftragten benennen, wenn die Verarbeitung von einer öffentlichen Stelle durchgeführt wird. In diesem Sinne bestimmt auch § 5 Abs. 1 S. 1 BDSG schlicht, dass öffentliche Stellen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benennen. Ausweislich der Gesetzesbegründung sollte die „Rechtsstellung der behördlichen Datenschutzbeauftragten in der Bundesverwaltung […] einheitlich ausgestaltet sein".[43] Gemeint ist damit der gesamte öffentliche Bereich.[44] Von dieser Pflicht sind allein **Gerichte** ausgenommen, die im Rahmen ihrer justiziellen Tätigkeit handeln (Art. 37 Abs. 1 lit. a 2. Halbsatz DSGVO).[45] Der Wortlaut enthält demnach auch insoweit **keine Bereichsausnahme** für Fraktionen und Abgeordnete. Obgleich die DSGVO zur Art und Weise, insbesondere zur Form der Benennung schweigt, empfiehlt sich, den Datenschutzbeauftragten **schriftlich** zu benennen.[46]

Für mehrere öffentliche Stellen kann ein **gemeinsamer Datenschutzbeauftragter** benannt werden (Art. 37 Abs. 3 DSGVO; § 5 Abs. 2 BDSG). Dabei sind Organisationsstruktur und Größe der öffentlichen Stellen zu berücksichtigen. Es wäre somit grundsätzlich zulässig, dass mehrere Abgeordnete einen gemeinsamen Datenschutzbeauftragten benennen. Voraussetzung ist aber, dass dieser auch tatsächlich in der Lage ist, seine Aufgaben (vgl. dazu Art. 39 DSGVO; § 7 BDSG) für sämtliche ihn benennende öffentliche Stellen effektiv wahrzunehmen.[47]

Weiterhin ist der Datenschutzbeauftragte auf der Grundlage seiner **beruflichen Qualifikation** und insbesondere seines **Fachwissens**, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, zu benennen (Art. 37 Abs. 5 DSGVO; § 5 Abs. 3 BDSG). Nach dem 97. Erwägungsgrund der DSGVO sollte sich das „Niveau des Fachwissens" sowohl an den Datenverarbeitungsvorgängen als auch an dem erforderlichen Schutz der personenbezogenen Daten orientieren. Der Datenschutzbeauftragte muss letztlich fähig sein, die in Art. 39 DSGVO genannten Aufgaben zu erfüllen (s. Art. 37 Abs. 5 DSGVO).

---

42 Für nicht-öffentliche Stellen gelten hingegen Art. 37 Abs. 1 lit. b und c DSGVO sowie ergänzend § 38 BDSG.

43 BT-Drs. 18/11325, S. 81.

44 Bergt, in: Kühling/Buchner, DSGVO, 2017, Art. 37 Rn. 16.

45 Vgl. zu dieser Ausnahme Helfrich, in: Sydow, DSGVO, 2017, Art. 37 Rn. 56 ff.

46 So auch Paal, in: Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 37 Rn. 16 m.w.N.

47 Vgl. Paal, in: Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 37 Rn. 11 m.w.N.; vgl. auch das Kurzpapier Nr. 12 zum Thema „Datenschutzbeauftrage bei Verantwortlichen und Auftragsverarbeitern", abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_Datenschutzbeauftragte.pdf?__blob=publicationFile&v=3 (Stand: 13.03.2018).

Der Datenschutzbeauftragte kann sowohl **Beschäftigter** des Verantwortlichen sein, als auch seine Aufgaben auf der Grundlage eines **Dienstleistungsvertrags**, mithin extern, erfüllen (Art. 37 Abs. 6 DSGVO).[48] Das soll, da der Wortlaut insoweit nicht differenziert, gleichermaßen für öffentliche wie für nicht-öffentliche Stellen gelten.[49] Jedenfalls ist sicherzustellen, dass der Datenschutzbeauftragte seine Pflichten und Aufgaben „in vollständiger Unabhängigkeit" (Erwägungsgrund 97 S. 4) ausüben kann. Daher unterliegt der Datenschutzbeauftragte nach Art. 38 DSGVO insbesondere bei der Erfüllung seiner Aufgaben **keinen Weisungen** des Verantwortlichen (Abs. 3 S. 1; § 6 Abs. 3 S. 1 BDSG) und darf von diesem deswegen auch **nicht abberufen oder benachteiligt** werden (Abs. 3 S. 2; § 6 Abs. 3 S. 3 BDSG). Die **Unabhängigkeit** des Datenschutzbeauftragten ist insoweit in besonderer Weise geschützt.

Für den parlamentarischen Bereich wären zur Umsetzung dieser Pflicht verschiedene Varianten denkbar. Bei den Fraktionen müssten zunächst wie bisher auch Datenschutzbeauftragte bestellt werden. In den Abgeordnetenbüros sind mehrere Ausgestaltungen möglich. So könnte, auch wenn dies wahrscheinlich nicht praktikabel erscheint, jedes Abgeordnetenbüro zunächst einen eigenen Datenschutzbeauftragten bestellen. Zulässig wäre zudem die Bestellung eines gemeinsamen Datenschutzbeauftragten über das sog. Pooling. Wie bereits oben erwähnt wurde, ist ferner die Bestellung eines externen Dienstleisters möglich, der die Aufgaben des Datenschutzbeauftragten übernimmt.

10. Verzeichnisführung

Nach Art. 30 Abs. 1 DSGVO führt jeder Verantwortliche 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.[50]

11. Meldepflichten

Im Falle einer **Verletzung des Schutzes personenbezogener Daten** muss diese nach Art. 33 Abs. 1 DSGVO unverzüglich und nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls der zuständigen **Aufsichtsbehörde** gemeldet werden. Nach Art. 34 DSGVO muss zudem

---

48 Vgl. dazu insbesondere Heberlein, in: Ehmann/Selmayr, DSGVO, 2017, Art. 37 Rn. 41 ff.

49 H.M. Vgl. Bergt, in: Kühling/Buchner, DSGVO, 2017, Art. 37 Rn. 36; Paal, in: Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 37 Rn. 14; Helfrich, in: Sydow, DSGVO, 2017, Art. 37 Rn. 115.

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

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.[51]

12. Datenverarbeitung zu anderen Zwecken

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.[52] In folgenden Fällen ist eine solche Weiterverarbeitung zulässig:

1. Es ist offensichtlich, dass sie im **Interesse der betroffenen** Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,

2. **Angaben** der betroffenen Person müssen **überprüft** werden, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

3. weil sie zur Abwehr **erheblicher Nachteile für das Gemeinwohl** oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,

4. weil sie zur Verfolgung von **Straftaten** oder **Ordnungswidrigkeiten**, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,

5. weil sie zur Abwehr einer **schwerwiegenden Beeinträchtigung** der **Rechte** einer anderen Person erforderlich ist oder

6. weil sie der Wahrnehmung von **Aufsichts-** und **Kontrollbefugnissen**, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies

---

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

52 BT-Drs. 18/11325, S. 95; vgl. hierzu auch: Frenzel, in: Paal/Pauly, DSGVO BDSG, 2. Auflage 2018 § 23 BDSG Rn. 1 ff.

gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

13. Datenübermittlung

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.[53] Dabei unterscheidet die gesetzliche Regelung zwischen einer Übermittlung von Daten **zwischen öffentlichen Stellen** (§ 25 Abs. 1 BDSG) und einer Übermittlung von Daten **einer öffentlichen Stelle an eine nichtöffentliche Stelle** (§ 25 Abs. 2 BDSG). Ordnet man entsprechend der oben dargestellten vereinzelten Literaturstimmen Abgeordnete als nichtöffentliche Stelle ein, so würde sich die Datenübermittlung an diese von der jeweiligen Fraktion oder auch von der Bundestagsverwaltung nach § 25 Abs. 2 BDSG richten. Bei einer Einordnung als öffentliche Stelle richtet sie sich nach § 25 Abs. 1 BDSG.

14. Datenerhebung im Internet

Werden Daten im Internet erhoben, so besteht bisher eine Informationspflicht nach § 13 Abs. 1 Telemediengesetz (TMG). Danach muss ein Webseitenbetreiber Nutzer der Seite informieren, wenn er Daten von ihnen erhebt. Dies erfolgt zumeist im Rahmen üblicher Datenschutzerklärungen. Die bisherige Regelung in § 13 Abs. 1 TMG wird nunmehr nach Ansicht des Gesetzgebers und der Literatur weitgehend durch Art. 13 DSGVO verdrängt.[54] Die bisherigen Datenschutzerklärungen werden daher weitere Informationen beinhalten müssen. Der Verantwortliche muss dem Betroffenen zum Zeitpunkt der Erhebung daher Folgendes mitteilen:

- den Namen und die **Kontaktdaten des Verantwortlichen**,
- gegebenenfalls die Kontaktdaten des **Datenschutzbeauftragten**,
- die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung,
- wenn die Verarbeitung auf Art. 6 Abs. 1 Buchstabe f DSGVO beruht, die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden,
- gegebenenfalls die **Empfänger oder Kategorien** von Empfängern der personenbezogenen Daten und
- gegebenenfalls die **Absicht des Verantwortlichen**, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der (EU-)Kommission oder im Falle

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

54 Vgl. BT-Drs. 18/12356, S. 28; v. Schenk/Mueller-Stöfen, Die Datenschutz-Grundverordnung: Auswirkungen in der Praxis, GWR 2017, 171 (177); Sydow, in: Sydow, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Einleitung Rn. 43 m.w.N.

von Übermittlungen gemäß Art. 46 oder Art. 47 oder Art. 49 Absatz 1 Unterabs. 2 DSGVO einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

Daneben bestehen nach Art. 13 Abs. 2 DSGVO möglicherweise weitere Informationspflichten, wenn diese notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Die formellen Anforderungen für die Erfüllung der Informationspflichten finden sich in Art. 12 Abs. 1 DSGVO. Diese haben in präziser, transparenter, verständlicher und leicht zugänglicher Form zu erfolgen. Diese Anforderungen stellen eine Neuerung gegenüber den bisherigen Regelungen dar. Insbesondere Online-Angebote, die sich an Kinder richten, müssen in besonderer Weise auch eine kindgerechte Sprache verwenden. Zudem ist auf die besonderen Einwilligungsanforderungen für Kinder gem. Art. 8 DSGVO zu achten.

15. Rechtsbehelfe Betroffener, Haftung und Sanktion

Die Regelungen der DSGVO bringen auch zahlreiche Neuerungen im Bereich der Rechtsbehelfsmöglichkeiten Betroffener und der Haftung von Verantwortlichen mit sich.

15.1. Beschwerderecht, Recht auf wirksamen Rechtsbehelf bei Untätigkeit

Nach Art. 77 Abs. 1 DSGVO hat jede betroffene Person das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Ansicht ist, dass sie betreffende personenbezogene Daten rechtswidrig verarbeitet wurden. Gemäß Art. 77 Abs. 2 DSGVO hat die Aufsichtsbehörde den Beschwerdeführer über den Stand der Ergebnisse zu informieren. Nach Ansicht in der Literatur folgt aus dem Beschwerderecht kein Anspruch auf das Ergreifen bestimmter Maßnahmen.[55] Die Aufsichtsbehörde trifft jedoch eine Befassungspflicht.

Bleibt die Aufsichtsbehörde untätig, kann nach Art. 78 Abs. 2 DSGVO durch den Betroffenen Klage erhoben werden. Ziel eines solchen Verfahrens ist dann das Tätigwerden der Aufsichtsbehörde.[56] Im Rahmen einer solchen Klage ist es denkbar, dass die oben beschriebene Anwendbarkeit der Datenschutz-Grundverordnung auf den parlamentarischen Bereich einer gerichtlichen Klärung zugeführt werden könnte. Bliebe etwa die Beschwerde eines Betroffenen mit der Begründung unbearbeitet, die Aufsichtsbehörde könne den genannten Bereich nicht kontrollieren, könnte möglicherweise eine entsprechende Klage gegen diese erhoben werden. Die Frage nach der Aufsicht würde dann von den Gerichten geklärt werden.

15.2. Recht auf einen wirksamen Rechtsbehelf gegen Verantwortliche

Nach Art. 79 DSGVO kann ein Betroffener auch unmittelbar gegen Verantwortliche klagen, wenn er der Ansicht ist, in seinen Rechten infolge einer nicht im Einklang mit der Datenschutz-Grundverordnung stehenden Verarbeitung seiner personenbezogenen Daten verletzt zu sein. Die Vorschrift

---

55 Vgl. Körffer, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 78 DSGVO Rn. 5; Mundil, in: Wolff/Brink, Datenschutzrecht, 22. Edition, Stand: 01.02.2017, Art. 77 DSGVO Rn. 14 f.

56 Vgl. Körffer, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 78 DSGVO Rn. 8 ff.; Mundil, in: Wolff/Brink, Datenschutzrecht, 22. Edition, Stand: 01.02.2017, Art. 78 DSGVO Rn. 20.

soll dazu dienen, die materiellen Vorgaben des Datenschutzrechts prozessual durchsetzbar zu machen.[57] Gestützt auf dieses Rechtsmittel können folglich auch Datenverarbeitungsvorgänge von Abgeordneten und Fraktionen ggf. gerichtlich überprüft werden.

15.3. Vertretung Betroffener, Verbandsklage

Nach Art. 80 Abs. 1 DSGVO kann sich eine betroffene Person durch eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht vertreten lassen, um ihre Rechte durchzusetzen. Durch die Regelung wird eine Prozessstandschaft begründet. Die beauftragten Organisationen können die Rechte der Betroffenen gegenüber den Verantwortlichen, der Aufsichtsbehörde und vor den Gerichten geltend machen.[58]

Zudem sieht Art. 80 Abs. 2 DSGVO für die Mitgliedstaaten die Möglichkeit zur Schaffung einer Verbandsklage vor. Entsprechende Regelungen bestehen bisher lediglich vereinzelt für den Bereich des Verbraucherschutzes (vgl. § 1 und § 2 UKlaG, § 3 a Abs. 1 UWG).[59]

15.4. Haftung und Recht auf Schadensersatz

Art. 82 DSGVO enthält eine Anspruchsgrundlage zur Geltendmachung von Schadensersatzansprüchen. Danach kann jede Person, der wegen eines Verstoßes gegen die Datenschutz-Grundverordnung ein materieller oder immaterieller Schaden entstanden ist, Schadensersatz vom Verantwortlichen verlangen. Eine Entlastungsmöglichkeit sieht Art. 82 Abs. 3 DSGVO vor, wenn der Verantwortliche die erforderliche Sorgfalt beachtet hat.[60] Der Anspruch richtet sich grundsätzlich auch gegen öffentliche Stellen.[61]

15.5. Sanktionen

Sanktionsmöglichkeiten sieht zudem Art. 83 f. DSGVO bei Verstößen gegen die datenschutzrechtlichen Vorgaben vor. Nach Art. 83 Abs. 7 DSGVO kann jeder Mitgliedstaat festlegen, ob und in welchem Umfang öffentliche Stellen sanktioniert werden können. Nach den Regelungen des Bundesdatenschutzgesetzes ist eine Sanktionierung von öffentlichen Stellen nicht vorgesehen.[62] In § 43 Abs. 3 BDSG ist ausdrücklich geregelt, dass gegen Behörden und sonstige öffentliche Stellen keine Geldbußen verhängt werden.

---

57 Martini, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 79 DSGVO Rn. 4.

58 Karg, in: Wolff/Brink, Datenschutzrecht, 22. Edition, Stand: 01.05.2017, Art. 80 DSGVO Rn. 8 f.

59 Frenzel, Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 80 DSGVO Rn. 13.

60 v. Schenk/Mueller-Stöfen, Die Datenschutz-Grundverordnung: Auswirkungen in der Praxis, GWR 2017, 171 (178).

61 Frenzel, Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 82 DSGVO Rn. 12.

62 BT-Drs. 18/11325, S. 109.

16. Literaturverzeichnis

- Ehmann, Eugen/Selmayr, Martin (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2017.
- Epping, Volker/Hillgruber, Christian (Hrsg.), Beck´scher Online-Kommentar Grundgesetz, 35. Edition (Stand: 01.10.2017).
- Eßer, Martin/Kramer, Philipp/von Lewinski, Kai (Hrsg.), Auernhammer, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze, Kommentar, 5. Aufl. 2017.
- Gola, Peter/Schomerus, Rudolf, Bundesdatenschutzgesetz, Kommentar, 12. Aufl. 2015.
- Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2017.
- Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, Kommentar, 2. Aufl. 2018.
- Plath, Kai-Uwe (Hrsg.), BDSG/DSGVO. Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. Aufl. 2016.
- Sachs, Michael (Hrsg.), Grundgesetz, Kommentar, 8. Aufl. 2018.
- Schantz, Peter/Wolff, Heinrich Amadeus, Das neue Datenschutzrecht: Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, 2017.
- von Schenk, Sophie/Mueller-Stöfen, Tilman, Die Datenschutz-Grundverordnung: Auswirkungen in der Praxis, Gesellschafts- und Wirtschaftsrecht (GWR) 2017, 171.
- Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 8. Aufl. 2014.
- Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung, Kommentar, 2017.
- Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Beck´scher Online-Kommentar Datenschutzrecht, 22. Edition (Stand: 01.11.2017).

***