Sachstand

Grundlagen des Datenschutzrechts

Grundlagen des Datenschutzrechts

Aktenzeichen: WD 3 - 3000 - 327/18
Abschluss der Arbeit: 18.09.2018
Fachbereich: WD 3: Verfassung und Verwaltung

1. Vorbemerkung

Der vorliegende Sachstand soll einen Überblick über die Grundlagen des Datenschutzrechts geben und auf ausgewählte datenschutzrechtliche Fragen eingehen. Die Ausführungen stellen einen Überblick dar, ohne dabei den Anspruch auf Vollständigkeit zu erheben.

2. Verfassungs- und unionsrechtliche Grundlagen

Seinen Ursprung findet das Datenschutzrecht in Deutschland im Volkszählungsurteil aus dem Jahr 1983. Darin leitete das Bundesverfassungsgericht erstmals aus dem **Allgemeinen Persönlichkeitsrecht** des **Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG** auch ein **Recht auf informationelle Selbstbestimmung** ab. Ausdrücklich gewährleistet das Grundrecht „insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[1] Demnach stehen personenbezogene Daten grundsätzlich unter Grundrechtsschutz. Das Recht auf informationelle Selbstbestimmung als Ausprägung des Allgemeinen Persönlichkeitsrechts wurde in den zurückliegenden Jahrzehnten von den Gerichten weiter konkretisiert. Mit einer Entscheidung aus dem Jahr 2008 erweiterte das Bundesverfassungsgericht mit Rücksicht auf die zunehmende Digitalisierung seine Rechtsprechung und schuf als ergänzende Ausprägung ein **„Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität der informationstechnischen Systeme"**.[2]

Auch auf **europarechtlicher Ebene** ist der Datenschutz verankert. Nach **Art. 8 der EU-Grundrechte-Charta** hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Mit dem Vertrag von Lissabon wurde die EU-Grundrechte-Charta rechtsverbindlich und gilt nach Art. 6 Abs. 1 EUV gleichrangig neben den Verträgen und gehört damit zum primären Unionsrecht. Neben der Regelung in der EU-Grundrechte-Charta ist der Datenschutz auch in Art. 16 AEUV verankert. **Art. 16 Abs. 1 AEUV** wiederholt dabei zunächst das Recht auf den Schutz von personenbezogenen Daten. **Art. 16 Abs. 2 AEUV** schafft sodann eine umfassende Kompetenzgrundlage zur Schaffung datenschutzrechtlicher Regelungen. Entsprechende Regelungen können für den gesamten Anwendungsbereich des Unionsrechts erlassen werden. Dabei ist es unerheblich, ob personenbezogene Daten durch Unionsorgane oder Mitgliedstaaten verarbeitet werden. Mit der Kompetenzgrundlage des Art. 16 Abs. 2 AEUV ist es dem Unionsgesetzgeber möglich, den Datenschutz als Querschnittsmaterie zu regeln, die in sämtliche anderen Unionsrechtsgebiete hineinwirkt.

Bereits im Jahr **1995** trat die sog. **EU-Datenschutzrichtlinie** (Richtlinie 95/46/EG) in Kraft, die umfassende Vorgaben für die nationalen Gesetzgeber enthielt. Auf diesen beruhte wesentlich das bisherige Bundesdatenschutzgesetz (BDSG). Im Jahr **2016** erließ der Unionsgesetzgeber die nunmehr seit dem 25.05.2018 geltende **Datenschutz-Grundverordnung** (DSGVO). Diese löste die EU-Datenschutzrichtlinie ab und gilt anders als diese aufgrund ihres Verordnungscharakters als unmittelbar geltendes und anwendbares Recht in den Mitgliedstaaten. Da die Datenschutz-Grundverordnung zahlreiche Öffnungsklauseln und Regelungsspielräume beinhaltet, bedurfte es dennoch einer entsprechenden nationalen Begleitgesetzgebung. Ergänzende Regelungen befinden sich im ab dem 25.05.2018 geltenden Bundesdatenschutzgesetz. Anders als sein Vorgängergesetz ist das neue Bundesdatenschutzgesetz nur noch ein Rumpfgesetz, das an die Regelungen der

1 BVerfGE 65, 1, 1. LS.

2 BVerfGE 120, 274.

Datenschutz-Grundverordnung anknüpft, jedoch keine eigenständige datenschutzrechtliche Vollregelung mehr enthält. Ähnliche Regelungen bestehen wegen der föderalen Kompetenzlage auch auf der Landesebene. So haben die einzelnen Landesgesetzgeber für ihren Kompetenzbereich ebenfalls ergänzende Regelungen in den jeweiligen Landesdatenschutzgesetzen geschaffen.

3. Entstehung und Grundstruktur der DSGVO

Dem Erlass der Datenschutz-Grundverordnung ging auf europäischer Ebene ein **langjähriges Gesetzgebungsverfahren** voraus. Am **25.01.2012** stellte die Kommission den **Entwurf** einer Datenschutzreform vor, der auch einen Entwurf für eine Datenschutz-Grundverordnung enthielt. Der Verordnungscharakter sollte dabei insbesondere deshalb gewählt werden, weil trotz der bereits geltenden EU-Datenschutzrichtlinie 95/46/EG erhebliche Rechtsunterschiede in den Mitgliedstaaten bestanden, die durch den nun gewählten Verordnungscharakter überwunden werden sollten.[3] Der Kommissionsvorschlag wurde im sog. informellen Trilogverfahren zwischen Kommission, Rat und Europäischem Parlament umfassend und kontrovers diskutiert. Gerade die Debatte im Europäischen Parlament war dabei stark von den Enthüllungen von Edward Snowden geprägt. Das Trilogverfahren wurde am 15.12.2015 abgeschlossen. Im Anschluss daran durchlief die Datenschutz-Grundverordnung das weitere Gesetzgebungsverfahren, das mit der **Veröffentlichung im Amtsblatt am 04.05.2016** endete. Die Mitgliedstaaten und Rechtsanwender sollten dann ca. weitere zwei Jahre Zeit haben, sich mit den neuen Regelungen vertraut zu machen, bis diese dann am 25.05.2018 Geltung erlangen sollten.[4]

Die Datenschutz-Grundverordnung enthält umfangreiche unmittelbar anwendbare Vorgaben. Diese bestreffen sowohl den materiellen Datenschutz als auch dessen Durchsetzung und institutionelle Absicherung. Trotz des Anspruches als Vollregelung sind aber auch zahlreiche **Öffnungsklauseln** vorgesehen, die den Mitgliedstaaten umfangreiche eigene Regelungsspielräume belassen. Daneben sind zahlreiche Vorgaben der Datenschutz-Grundverordnung darauf angewiesen, durch **ergänzende nationale Rechtsvorschriften** umgesetzt bzw. ergänzt zu werden. Daher besteht auch nach Geltungserlangung der Datenschutz-Grundverordnung ein grundsätzliches Nebeneinander von Unionsrecht und mitgliedstaatlichen Regelungen, das zu Abgrenzungs- und Auslegungsschwierigkeiten führt. Es wird den Rechtsanwendern obliegen, in den nächsten Jahren eine handhabbare Auslegungspraxis zu etablieren.

4. Datenschutz und Informationsfreiheit

Der Schutz personenbezogener Daten kann mit den verschiedenen **Informationsansprüchen** in Konflikt stehen. Das Datenschutzrecht soll ein Zugänglichmachen von personenbezogenen Daten grundsätzlich begrenzen. Diesem Ansatz steht der Grundgedanke der Informationsfreiheit streng genommen entgegen. Aus diesem Grund finden sich in den Gesetzen, die den Informationszugang im Bund und in den Ländern regeln, auch entsprechende **Abwägungsklauseln**. Grundsätzlich hat jedermann Zugang zu amtlichen Informationen, die bei den Behörden vorhanden sind (vgl. § 1 Abs. 1 IFG). Ein Zugang auch zu personenbezogenen Daten wird jedoch nur dann gewährt, wenn das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss

3 Schantz, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 198.

4 Vgl. zum Ganzen: Schantz, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 197 ff.

des Informationszugangs überwiegt oder der Dritte eingewilligt hat (vgl. § 5 Abs. 1 IFG). Innerhalb dieser Abwägung im Einzelfall sind daher Belange der Informationsfreiheit und des Datenschutzes in Einklang zu bringen.

Ähnlich verhält es sich bei den spezialgesetzlich geregelten Informationsansprüchen des **Presse- und Rundfunkrechts** der Länder. Für beide Bereiche existieren spezielle Rechtsgrundlagen für etwaige Auskunftsansprüche. Die Datenschutz-Grundverordnung überlässt den Mitgliedstaaten nach Art. 85 DSGVO umfassende Regelungsspielräume zur Ausgestaltung der Datenverarbeitung für journalistische Zwecke. Die nationalen Regelungen können dabei auch von den Vorgaben der Datenschutz-Grundverordnung abweichen.[5] Richten sich entsprechende Informationsansprüche auf die Herausgabe personenbezogener Daten, muss auch hier eine entsprechende Interessenabwägung im Einzelfall erfolgen.

5. Datenschutz der Sicherheitsbehörden und Nachrichtendienste

Eine Ausnahme vom Anwendungsbereich der Datenschutz-Grundverordnung besteht nach Art. 2 Abs. 2 lit. d) DSGVO für die Verarbeitung von personenbezogenen Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Für diese Bereich gilt die sog. **JI-Richtlinie** (RL 2016/680 EU), die die Mitgliedstaaten parallel zur Datenschutz-Grundverordnung umzusetzen hatten.

Sonderregelungen gelten auch für **Nachrichtendienste** und im Bereich der **Verteidigung**. Nach Art. 2 Abs. 2 lit. a) DSGVO gelten die europäischen Vorgaben nur im Anwendungsbereich des Unionsrechts. Gemäß des 16. Erwägungsgrundes sind Tätigkeiten, die die nationale Sicherheit betreffen, nicht vom Anwendungsbereich des Unionsrechts umfasst. Die Datenverarbeitung der Nachrichtendienste fällt daher nach überwiegender Auffassung in der Literatur nicht in den Anwendungsbereich der Datenschutz-Grundverordnung. Sie stützt sich überwiegend auf spezielle nationale Regelungen. Ergänzend verweist der Gesetzgeber über § 1 Abs. 8 BDSG auf eine entsprechende Anwendung der Datenschutz-Grundverordnung. Gleiches gilt für die Datenverarbeitung im Bereich der Verteidigung.[6]

6. Datensicherheit

Nach Art. 24 DSGVO ist ein Verantwortlicher grundsätzlich verpflichtet, **technische und organisatorische Maßnahmen** zu ergreifen, um eine Einhaltung der datenschutzrechtlichen Vorgaben sicherzustellen. Nach Art. 32 Abs. 1 DSGVO gehören hierzu auch Maßnahmen, die insbesondere unter Berücksichtigung des Stands der Technik ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten. Im Falle einer Verletzung des Schutzes personenbezogener Daten ist ein Verantwortlicher nach Art. 33 DSGVO verpflichtet, eine solche Verletzung der Aufsichtsbehörde zu melden. Nach Art. 34 DSGVO ist zudem der Betroffene entsprechend zu informieren.

---

5 Vgl. hierzu auch: Ausarbeitung der Wissenschaftlichen Dienste zum Thema: Die Öffnungsklausel des Art. 85 der Datenschutz-Grundverordnung, WD 3 - 3000 - 123/18.

6 Wolff, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 254.

7. Datenschutzaufsicht

Zur institutionellen Durchsetzung des Datenschutzrechts verpflichtet Art. 51 DSGVO die Mitgliedstaaten, eine oder mehrere unabhängige **Aufsichtsbehörden** einzurichten. In Deutschland nehmen die Bundesbeauftragte für den Datenschutz und die jeweiligen Landesbeauftragten diese Aufgabe war. Besondere Aufsichtsbehörden bestehen zudem für den Rundfunk und bei den Kirchen.

Die Aufsichtsbehörden überwachen den Datenschutz in den Behörden des Bundes und der Länder sowie im privatrechtlichen Bereich. Ihnen werden hierfür umfassende **aufsichtsbehördliche Aufgaben** und **Befugnisse** eingeräumt (vgl. Art. 57 u. 58 DSGVO). Nach Art. 83 f. DSGVO können die Aufsichtsbehörden zudem **Bußgelder** verhängen.

Hervorzuheben ist auch das **Beschwerderecht** nach Art. 77 DSGVO. Danach kann sich jede betroffene Person mit einer Beschwerde an die Aufsichtsbehörde wenden, wenn sie der Auffassung ist, dass sie betreffende personenbezogene Daten unzulässig verarbeitet wurden.

8. Durchsetzung des Datenschutzrechts

Die Datenschutz-Grundverordnung enthält einen umfassenden Katalog an Betroffenenrechten, die die Durchsetzung des Datenschutzes sicherstellen sollen. Grundsätzlich muss jede Verarbeitung personenbezogener Daten entweder auf einer **Einwilligung** des Betroffenen oder auf einer **rechtlichen Grundlage** beruhen. Die zentrale Regelung hierzu findet sich in Art. 6 DSGVO. Daneben stehen einem Betroffenen unter anderem Auskunftsrechte, Berichtigungs- und Löschungsansprüche zu. Über die Informationspflichten, insbesondere des Art. 13 DSGVO, soll zudem sichergestellt werden, dass jeder Betroffene über eine ihn betreffende Datenverarbeitung in Kenntnis gesetzt wird und aus dieser Kenntnis heraus seine Rechte geltend machen kann.

Zur Durchsetzung der datenschutzrechtlichen Vorgaben kann ein Betroffener neben der oben genannten Beschwerde auch speziell geregelte **Klagerechte** ausüben, die in den Art. 78 bis 81 DSGVO geregelt sind. Nach Art. 82 DSGVO besteht zudem ein spezieller **Schadensersatzanspruch**.

Darüber hinaus kann die Aufsichtsbehörde wie bereits erwähnt auch **Bußgelder** verhängen. Diese können je nach Schwere des Verstoßes bis zu 20.000.000 € oder bei Unternehmen bis zu 4% des weltweit erzielten Jahresumsatzes betragen.

***