



---

**Ausarbeitung**

---

**Datenschutzrecht der Europäischen Union, Deutschlands und der USA**



## **Datenschutzrecht der Europäischen Union, Deutschlands und der USA**

Verfasser/in:

[REDACTED]

Aktenzeichen:

WD 3 - 3000 - 064/15

Abschluss der Arbeit:

25.03.2015

Fachbereich:

WD 3: Verfassung und Verwaltung

Telefon:

[REDACTED]

---

## Inhaltsverzeichnis

<b>1.</b>	<b>Zusammenfassung</b>	<b>4</b>
<b>2.</b>	<b>Einleitung</b>	<b>5</b>
<b>3.</b>	<b>Primärrechtliche Grundlagen der EU, Verfassungsrecht der BRD und der USA</b>	<b>5</b>
3.1.	Primärrecht der Europäischen Union	5
3.2.	Verfassungsrechtlicher Rahmen im Grundgesetz	6
3.3.	Verfassungsrechtliche Grundlage in den USA	6
<b>4.</b>	<b>Konzeptionen des Datenschutzes</b>	<b>7</b>
4.1.	Konzeption des Datenschutzes: Europäische Union und Bundesrepublik	7
4.2.	Konzeption des Datenschutzes: USA	10
4.3.	Synopse der Grundkonzeptionen	14
<b>5.</b>	<b>Unabhängige Kontrollinstanzen und Rechtsschutz gegen Datenschutzverstöße</b>	<b>15</b>
5.1.	Europäische Union	15
5.2.	Bundesrepublik	17
5.3.	USA	17

## 1. Zusammenfassung

Aus einem Vergleich des Datenschutzrechtes der Europäischen Union, Deutschlands und der USA ergeben sich erhebliche Unterschiede. Während das Datenschutzrecht der Union und Deutschlands aufgrund der durch die Union mittels Richtlinien betriebenen Rechtsangleichung weitestgehend Parallelen aufzeigen, liegt dem US-amerikanischen Datenschutzrecht eine wesentlich andere Konzeption zugrunde. Mit einem **allgemeinen Regelungsmodell** auf der Seite der Union und Deutschlands und dem **bereichsspezifischen Konzept** auf US-amerikanischer Seite stehen sich bezüglich der Verarbeitung von personenbezogenen Daten der Grundsatz des **Verbots mit Erlaubnisvorbehalt** und die **Erlaubnis mit Verbotsvorbehalt** gegenüber. Gemeinsam ist den drei Rechtsordnungen die Möglichkeit der Unternehmen zu einer Regulierung der Verarbeitung von den das Unternehmen selbst betreffenden Daten im nicht-öffentlichen Bereich. Dabei zeigt sich jedoch eine **unterschiedliche Ausrichtung der Selbstregulierung**. Während dieses Instrument in den USA als Ersatz staatlicher Regelungen dient, ist das Regelungsmodell der Union und der Bundesrepublik auf den Vollzug des gesetzlichen Datenschutzes gerichtet.

Als unabhängige Kontrollinstanz zum Schutz gegen rechtswidrige Verarbeitung von personenbezogenen Daten sehen die Europäische Union sowie Deutschland **Datenschutzbeauftragte** vor. Eine solche Datenschutzaufsichtsbehörde ist in der US-amerikanischen Rechtsordnung nicht vorgesehen. Vielmehr können die Betroffenen in privatrechtlichen Streitigkeiten Beschwerde bei der „**Federal Trade Commission**“ einlegen. Im Übrigen sehen die Rechtsordnungen nach geltendem Recht keine speziellen Rechtsbehelfe vor, sodass die Betroffenen auf die allgemeinen Rechtsschutzmöglichkeiten beschränkt sind. Einzig die geplante EU-Datenschutzgrundverordnung enthält einige Besonderheiten, darunter die Möglichkeit einer näher ausgestalteten **Verbandsklage**.

## 2. Einleitung

Die vorliegende Ausarbeitung beschäftigt sich mit den Gemeinsamkeiten und Unterschieden des Datenschutzrechts der Europäischen Union, der Bundesrepublik Deutschland und der USA auf Bundesebene. Dabei beschränkt sich der Vergleich – mit Ausnahme einzelner Verweise auf bereichsspezifische Regelungen in den USA – auf die allgemeinen Regelungen des Datenschutzrechts. Zum Schluss wird ein Überblick über die jeweils in den Rechtsordnungen vorhandenen Rechtsschutzmöglichkeiten gegen datenschutzrechtliche Verstöße gegeben. In diesem Zusammenhang wird auch auf die wesentlichen Änderungen durch die geplante EU-Datenschutzgrundverordnung hingewiesen.

## 3. Primärrechtliche Grundlagen der EU, Verfassungsrecht der BRD und der USA

### 3.1. Primärrecht der Europäischen Union

Die Grundrechtecharta (GRC) gehört seit ihrer Inkorporierung über Art. 6 Abs. 1 UAbs. 1 EUV zum unionsrechtlichen Primärrecht und bildet damit einen geschriebenen rechtsverbindlichen Grundrechtskatalog.<sup>1</sup> Darin wird neben weiteren datenschutzrelevanten Freiheitsrechten<sup>2</sup> mit Art. 8 GRC ausdrücklich ein **Datenschutzgrundrecht** als Ausprägung des Rechts auf informationelle Selbstbestimmung gewährleistet.<sup>3</sup> Nach Absatz 1 dieser Vorschrift sowie dem im Wortlaut identischen Art. 16 Abs. 1 AEUV hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Über Art. 16 Abs. 1 AEUV und Art. 8 Abs. 1 GRC wird somit ein Schutz bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen oder sonstigen Stellen der Union sowie durch die Mitgliedsstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, gewährleistet.<sup>4</sup>

Neben dem unmittelbar im Primärrecht der Europäischen Union niedergelegten Datenschutzrecht ist das Recht auf informationelle Selbstbestimmung auch in Art. 8 der Europäischen Menschenrechtskonvention (EMRK) niedergelegt. Hiernach hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. Vom Wortlaut des Art. 8 Abs. 1 EMRK wird damit zwar das Recht auf Schutz personenbezogener Daten nicht ausdrücklich in Bezug genommen. Es wird aber als Teil des Rechts auf Achtung des Privatlebens unbestritten durch Art. 8 EMRK garantiert.<sup>5</sup> Dies gilt es bei der Auslegung des Art. 8 GRC zu beachten. Denn die EMRK ist über Art. 52 Abs. 3 GRC als Mindestgehalt der Charta inkorporiert.<sup>6</sup> Hierbei ist darauf

---

1 Kingreen, in: Calliess/Ruffert (Hrsg.), EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta – Kommentar, 4. Auflage 2011, Art. 6 EUV Rn. 8.

2 Übersicht zu den datenschutzrelevanten Freiheitsrechten: Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 81 ff.

3 Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Auflage 2008, S. 45.

4 Herrmann, in: Streinz, EUV/AEUV, 2. Auflage 2012, Art. 16 EUV (ex Art. 286) Rn. 7.

5 Bernsdorff, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage 2014, Art. 8 Rn. 19.

6 Borowsky, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage 2014, Art. 8 Rn. 19.

hinzuweisen, dass Art. 8 EMRK maßgebend die Entstehung des Art. 8 GRC geprägt hat. Schließlich hat der Grundrechtskonvent mit dem Hinweis auf Art. 8 EMRK daran erinnert, dass das Recht auf informationelle Selbstbestimmung auch in der Rechtsprechung des Europarats seinen Niederschlag gefunden hat.<sup>7</sup>

### 3.2. Verfassungsrechtlicher Rahmen im Grundgesetz

Zwar benennt das Grundgesetz ein Datenschutzrecht nicht explizit. Der Schutz personenbezogener Daten wird aber neben Art. 10 Abs. 1 GG insbesondere durch zwei Grundrechte gewährleistet.<sup>8</sup> So hat das Bundesverfassungsgericht in seinem **Volkszählungsurteil**<sup>9</sup> mit Blick auf neuartige Gefahren der Datenverarbeitung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG das **Recht auf informationelle Selbstbestimmung** entwickelt.<sup>10</sup> Darunter ist das Recht des Einzelnen zu verstehen, über die eigenen personenbezogenen Informationen grundsätzlich selbst zu bestimmen.<sup>11</sup> Der Grundrechtsträger ist damit vor jeder Form der Erhebung, Kenntnisnahme, Speicherung, Verwendung, Weitergabe oder Veröffentlichung von persönlichen – also von individualisierten oder individualisierbaren – Informationen geschützt.<sup>12</sup> Seit dem Volkszählungsurteil hat das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung weiter konkretisiert. So entwickelte es mit dem **Grundeck auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** eine weitere Ausprägung des allgemeinen Persönlichkeitsrechts.<sup>13</sup> Dieses Recht schafft einen Schutz des persönlichen und privaten Lebensbereichs vor dem Zugriff auf informationstechnische Systeme und geht damit über das Recht auf informationelle Selbstbestimmung, das lediglich Informationen mit einem punktuellen Bezug zu einem bestimmten Lebensbereich des Betroffenen umfasst, hinaus.<sup>14</sup>

### 3.3. Verfassungsrechtliche Grundlage in den USA

Anknüpfungspunkt für das Datenschutzrecht in der „Constitution“ der USA ist der vierte Verfassungszusatz, das „Fourth Amendment“. Hierin heißt es:

---

7 Bernsdorff, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage 2014, Art. 8 Rn. 19.

8 Zur vertieften Darstellung verfassungsrechtlicher Grundlagen des Datenschutzrechts: Simitis, in: Simitis (Hrsg.)/Dammann, Bundesdatenschutzgesetz, 7. Auflage 2011, Einführung Rn. 192 ff.

9 BVerfGE 65, 1.

10 Di Fabio, in Maunz/Dürig (Hrsg.) Grundgesetz-Kommentar, 72. Ergänzungslieferung 2014, Art. 2 Rn. 176.

11 BVerfGE 65, 1 (43); Di Fabio, in Maunz/Dürig (Hrsg.) Grundgesetz-Kommentar, 72. Ergänzungslieferung 2014, Art. 2 Rn. 175; Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Auflage 2008, S. 75.

12 Di Fabio, in Maunz/Dürig (Hrsg.) Grundgesetz-Kommentar, 72. Ergänzungslieferung 2014, Art. 2 Rn. 176; Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Auflage 2008, S. 76.

13 BVerfGE 120, 274.

14 Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Auflage 2008, S. 89.

„The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated...”

Während in der Europäischen Union und der Bundesrepublik die vorgenannten Regelungen dem einzelnen Bürger ein abgesichertes Recht auf Schutz der Privatsphäre bei der Nutzung neuer Medien schaffen, besteht in den USA bei den Bundesgerichten und den Gerichten der Bundesstaaten diesbezüglich jedoch noch keine Einigkeit.<sup>15</sup>

#### 4. Konzeptionen des Datenschutzes

Das unionsrechtliche wie das hiesige Datenschutzrecht weisen zu dem Datenschutzrecht der USA erhebliche Unterschiede auf, sodass bereits von einem unterschiedlichen Grundkonzept ausgegangen werden kann.<sup>16</sup> Ursache hierfür dürften die verschiedenen Gesichtspunkte sein, unter denen das Datenschutzrecht jeweils betrachtet wird. So ist dieses in den USA im nicht-öffentlichen Bereich wettbewerbsorientierter ausgerichtet, da insbesondere die Befürchtung besteht, dass durch einen starken Datenschutz Innovationsanreize verloren gehen könnten.<sup>17</sup> Im Gegensatz dazu wird der Datenschutz in der Europäischen Union und in Deutschland aus der grundrechtlichen Perspektive betrachtet.<sup>18</sup>

##### 4.1. Konzeption des Datenschutzes: Europäische Union und Bundesrepublik

Das Datenschutzrecht der Mitgliedstaaten, mithin auch Deutschlands, wird bislang maßgebend durch Richtlinien<sup>19</sup> der Europäischen Union geprägt, was zu einem Rückgang der Regelungskompetenz nationaler Gesetzgeber und über Art. 288 Abs. 3 AUEV zu einer Rechtsangleichung geführt hat.<sup>20</sup> Folglich laufen das Datenschutzrecht der EU und der Bundesrepublik weitestgehend parallel. Ein jenseits der Richtlinien bestehendes, unmittelbar in den Mitgliedsstaaten geltendes EU-Datenschutzrecht besteht bislang nicht. Allerdings hat die Europäische Kommission mit Blick

---

15 Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 2011, 755 (755); Lejeune, Datenaustausch mit den Vereinigten Staaten von Amerika, CR 2013, 822 (826); ablehnend: Freedman v. America Online, Inc., 412 F. Supp. 2d 174 (D. Conn. 2005); United States v. Arnold, 533 F. 3d 1003 (9th Cir. 2008).

16 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (3).

17 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (5).

18 Simitis, in: Simitis (Hrsg.)/Dammann, Bundesdatenschutzgesetz, 7. Auflage 2011, Einführung Rn. 209 ff.; Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (5).

19 Allgemeine Datenschutzrichtlinie 95/46/EG (DSRL); Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (E-DSRL); Vorratsdatenspeicherungsrichtlinie 2006/24/EG (VDSRL), diese hat der EuGH allerdings in einem Urteil v. 08.04.2014 aufgrund eines Verstoßes gegen Art. 7 und 8 der Europäischen Grundrechtecharta für unzulässig erachtet, Az.: C-293/12 und C-594/12.

20 Simitis, in: Simitis (Hrsg.)/Dammann, Bundesdatenschutzgesetz, 7. Auflage 2011, Einführung Rn. 149; Kühling, Die Europäisierung des Datenschutzrechts, 1. Auflage 2014, S. 11 f., 15, geht sogar von einer richtlinienrechtlichen Vollharmonisierung aus.

auf die technologische Entwicklung im Jahre 2012 einen Vorschlag zu einer EU-Datenschutzgrundverordnung<sup>21</sup> vorgebracht.

In einer Grundfrage eines jeden datenschutzrechtlichen Regelungsmodells weist das deutsche Datenschutzrecht allerdings einen markanten Unterschied zum unionsrechtlichen Ansatz auf: Während das **Bundesdatenschutzgesetz** (BDSG) eine **traditionelle Zweiteilung** mit unterschiedlichen Datenschutzvorschriften für öffentliche und nicht-öffentliche Stellen vornimmt, hat man sich auf der Ebene der **Union** für einen **einheitlichen Regelungsansatz** entschieden.<sup>22</sup> Darum fehlt es in den europäischen Datenschutzrichtlinien – anders als im BDSG (§ 2) – an einer Definition zu den Begriffen „öffentliche“ und „nicht-öffentliche Stelle“.<sup>23</sup> Nicht zu verkennen ist allerdings die in der Entwicklung des BDSG festzustellende Tendenz, wonach der Umfang solcher Regelungen, welche für öffentliche wie nicht-öffentliche Stellen gleichermaßen gelten (vgl. §§ 1-11, 32, 43-46 BDSG), zunimmt.<sup>24</sup> Ebenso finden die zentralen datenschutzrechtlichen Prinzipien auf beide Bereiche Anwendung.<sup>25</sup>

Eine weitere Grundfrage eines jeden datenschutzrechtlichen Regelungsmodells geht dahin, ob der Gesetzgeber im Grundsatz einen punktuellen, also bereichsspezifischen bzw. sektoralen Regelungsansatz, oder einen umfassenden, also allgemeinen, Regelungsansatz wählt, welcher durch spezialgesetzliche Regelungen ergänzt wird.<sup>26</sup> In Deutschland wie der Europäischen Union wird seit jeher ein umfassender Regelungsansatz verfolgt. Danach ist im Ausgangspunkt jede Verarbeitung von personenbezogenen Informationen verboten, sodass von dem Grundsatz eines **Verbots mit Erlaubnisvorbehalt** auszugehen ist.<sup>27</sup> Dies ergibt sich für die Bundesrepublik aus Art. 4 Abs. 1 BDSG und für die Union aus Art. 7 der RL 95/46/EG (Allgemeine Datenschutzrichtlinie – DSRL). Nach diesen Bestimmungen darf die Verarbeitung personenbezogener Daten nur erfolgen, wenn die dort benannten Voraussetzungen erfüllt sind. Der Grundsatz eines Verbots zur Verarbeitung

- 
- 21 (2012) 11; abrufbar mit Änderungsvorschlägen des Europäischen Parlaments auf: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE>, zuletzt abgerufen am 18.03.2013; zur Chronologie der Verordnung vgl. <http://gesetzgebung.beck.de/node/1029754>.
- 22 Simitis, in: Simitis (Hrsg.)/Dammann, Bundesdatenschutzgesetz, 7. Auflage 2011, Einführung Rn. 206; Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 119 f.
- 23 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 220.
- 24 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 220.
- 25 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 220.
- 26 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 234.
- 27 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 235; Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (3, 6); Lejeune, Datenaustausch mit den Vereinigten Staaten von Amerika, CR 2013, 822 (826); Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Auflage 2008, S. 52.



personenbezogener Daten bleibt auch in dem von der Europäischen Kommission vorgebrachten Entwurf einer allgemeinen **EU-Datenschutzgrundverordnung**<sup>28</sup> in Art. 6 und 7 aufrechterhalten.<sup>29</sup>

Neben diesen Grundsatz treten weitere Prinzipien, welche auf unionsrechtlicher Ebene wie der hiesigen Bundesebene gleichermaßen Geltung entfalten. Hierzu zählt der Grundsatz der **Zweckbindung**, welcher sich für die Union aus Art. 8 Abs. 2 GRC sowie Art. 6 Abs. 1 lit. b DSLR und für die Bundesrepublik aus Art. 4 Abs. 3 Nr. 2 BDSG ergibt. Daneben sehen die DSLR sowie das BDSG das **Transparenzgebot**<sup>30</sup> vor, wonach eine Pflicht der verantwortlichen Stelle zur **Benachrichtigung** gegenüber den Betroffenen über die Datenverarbeitung besteht (Art. 10, 11 DSLR, § 4 Abs. 3 BDSG). Im BDSG ist zudem der Grundsatz der **Datenvermeidung und Datensparsamkeit** (§ 3a BDSG) sowie der Grundsatz der **Direkterhebung** (Art. 4 Abs. 2 S. 1 BDSG) niedergelegt.

Zu der staatlichen Normierung des Datenschutzrechts kommt im nicht-öffentlichen Bereich die Möglichkeit einer **Selbstregulierung** der Datenverarbeitung durch die verantwortlichen Stellen hinzu. Im Grundsatz handelt es sich hierbei um Selbstverpflichtungen der Unternehmen, durch welche der Umgang mit den in ihrem Unternehmen aufkommenden personenbezogenen Daten geregelt wird. Solche Selbstverpflichtungen werden durch die Unternehmen selbst und freiwillig ausgearbeitet.<sup>31</sup> Welcher Zweck durch eine Selbstregulierung verfolgt wird und welches Mindestniveau einzuhalten ist, hängt vom Konzept der jeweiligen Rechtsordnung ab. So fördern die Mitgliedsstaaten und die Europäische Kommission nach Art. 27 Abs. 1 DSRL die Ausarbeitung von Verhaltensregelungen, welche nach Maßgabe der Besonderheiten einzelner Bereiche zur **ordnungsgemäßen Durchführung einzelstaatlicher Vorschriften** beitragen sollen. Hieraus wird zweierlei deutlich: Nach unionsrechtlichen Maßstäben ist eine Selbstregulierung möglich und sogar erwünscht, wenngleich eine datenschutzrechtliche Selbstregulierung gleichzeitig auf den **Vollzug gesetzlicher Vorschriften** beschränkt wird.<sup>32</sup> Auch nach Art. 38 Abs. 1 der geplanten EU-Datenschutzgrundverordnung<sup>33</sup> soll die Selbstregulierung weiterhin auf den Vollzug der unionsrechtlichen Vorgaben begrenzt bleiben.<sup>34</sup> In entsprechender Weise wird in § 38a BDSG eine datenschutzrechtliche Selbstregulierung auf die **Durchführung datenschutzrechtlicher Regelungen** beschränkt. Das bestehende gesetzliche Datenschutzrecht bildet somit das datenschutzrechtliche

---

28 KOM (2012) 11; abrufbar mit Änderungsvorschlägen des Europäischen Parlaments auf: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE>, zuletzt abgerufen am 18.03.2015.

29 Körner, Die Reform des EU-Datenschutzes: Der Entwurf einer EU-Datenschutzgrundverordnung (DS-GVO) – Teil I, ZESAR 2013, 99 (102).

30 Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Auflage 2008, S. 52.

31 Zu Einzelheiten der Selbstregulierung eingehend: Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3.

32 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3.

33 5853/12, KOM(2012)11.

34 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (7).

Mindestniveau. Dieses darf durch die Selbstregulierung nicht unterschritten werden.<sup>35</sup> Um dies zu gewährleisten, können Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, entsprechende Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der Aufsichtsbehörde unterbreiten (§ 38a Abs. 1 BDSG). Diese überprüft die Vereinbarkeit des Entwurfs mit dem geltenden Datenschutzrecht. Wird festgestellt, dass die Verhaltensregeln dem geltenden Datenschutzrecht entsprechen, ist ein feststellender begünstigender Verwaltungsakt zu erlassen.<sup>36</sup> Die Selbstregulierung unterliegt also einer präventiven Kontrolle. Dieses Verfahren wird dementsprechend als „**kontrollierte Selbstregulierung**“ bezeichnet.<sup>37</sup> Dieses nach deutschem Recht vorgesehene Verfahren könnte in Zukunft durch die **EU-Datenschutzgrundverordnung**<sup>38</sup> eine wesentliche Änderung erfahren. Nach Art. 38 DSGVO sollen die Aufsichtsbehörden nämlich lediglich ein Frage- und Antwortrecht erhalten. Damit würden deutsche Aufsichtsbehörden ihre Entscheidungskompetenz zur verbindlichen Feststellung der Vereinbarkeit von unternehmerischen Verhaltenskodizes verlieren.<sup>39</sup> Soweit für mehrere Mitgliedsstaaten Verhaltensregelungen aufgestellt werden, soll die Europäische Kommission den Verhaltensregelungen ihre Gültigkeit verschaffen (Art. 38 Abs. 4 DSGVO).

#### 4.2. Konzeption des Datenschutzes: USA

Ein zentrales Datenschutzrecht, das heißt ein mit den Regelungen der EU und Deutschlands vergleichbares umfassendes Datenschutzrecht, ist in den USA auf Bundesebene bislang nicht gegeben.<sup>40</sup> Datenschutzrechtliche Regelungen sind in den USA vielmehr stark **anlassbezogen**.<sup>41</sup> So beschränkt sich der Datenschutz auf spezielle Vorschriften als **Reaktion auf konkrete datenschutzrechtliche Probleme in einem bestimmten Bereich**.<sup>42</sup> Gleichzeitig sind spezifische datenschutzrechtliche Regelungen in Gesetze integriert, welche andere als datenschutzrechtliche Zwecke verfolgen, gleichzeitig

---

35 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (4).

36 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (4).

37 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (4).

38 KOM (2012) 11; abrufbar mit Änderungsvorschlägen des Europäischen Parlaments auf: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE>, zuletzt abgerufen am 18.03.2015; zur Chronologie der Verordnung vgl. <http://gesetzgebung.beck.de/node/1029754>.

39 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (7).

40 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (5, 9); Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 2011, 755 (755); Lejeune, Datenaustausch mit den Vereinigten Staaten von Amerika, CR 2013, 822 (826).

41 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (5).

42 Tinnfeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 234.

---

aber auch personenbezogene Informationen tangieren.<sup>43</sup> Anders als das unionsrechtliche sowie deutsche Datenschutzrecht ist das Datenschutzrecht in den USA also stark **bereichsspezifisch** ausgestaltet.<sup>44</sup> Neben einigen Sicherheitsgesetzen<sup>45</sup> lassen sich hier z.B. folgende sektorale Datenschutzgesetze nennen: Der „Video Privacy Protection Act“ von 1998, der „Fair Credit Reporting Act“ von 1971 oder der „Children Online Privacy Protection Act“ (COPPA) von 1998.<sup>46</sup> Die bereichsspezifische Ausprägung des US-amerikanischen Datenschutzrechts führt dazu, dass im Grundsatz ein freier Umgang mit personenbezogenen Daten gewährt wird, welcher im Einzelfall verboten ist. Damit liegt diesem System eine **Erlaubnis mit Verbotsvorbehalt** zugrunde.<sup>47</sup>

Eine Zweiteilung des Datenschutzrechtes in einen „öffentlichen“ und „nicht öffentlichen“ Bereich lässt sich dem US-amerikanischen Datenschutzrecht ebenso wenig entnehmen wie ein einheitlicher Regelungssatz.

Eine Folge der bereichsspezifischen Ausprägung ist, dass das US-amerikanische System – anders als in den Rechtsordnungen der Union und der Bundesrepublik – **keine übergreifenden datenschutzrechtlichen Prinzipien** bereithält. So findet sich etwa kein übergreifendes Transparenzgebot.<sup>48</sup> Bislang sieht lediglich der „Health Insurance Portability Accountability Act“, kurz HIPAA, eine Benachrichtigungspflicht vor. Gegenstand dieses Gesetzes ist der Schutz der Vertraulichkeit von personenbezogenen Patientendaten wie Name, Anschrift, oder Angaben zum Gesundheitszustand oder Details zur Krankenversicherung.<sup>49</sup> Hiernach sind die Betroffenen jedoch nur bei einer Verwendung der Patientendaten entgegen den Vorschriften und auch nur in dem Fall zu informieren, wenn ernsthaft zu befürchten ist, dass dem Betroffenen daraus ein finanzieller Schaden oder persönlicher Nachteil entstehen könnte.<sup>50</sup> Eine einheitliche rechtliche Grundlage zur Benachrichtigungspflicht sieht jedoch der in den Senat eingebrachte Gesetzentwurf „Data Security and Breach Notification

---

43 Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 2011, 755 (755).

44 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 234; Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 2011, 755 (755); Lejeune, Datenaustausch mit den Vereinigten Staaten von Amerika, CR 2013, 822 (826); Blaxell/Grant, Gegenüberstellung der europäischen und US-amerikanischen Haltung zum Datenschutz, RDV 2014 S, 142 (143).

45 Etwa: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, H.R. 3162 (PATRIOT Act); Electronic Communications Privacy Act (ECPA).

46 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (5);

47 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (9); Lejeune, Datenaustausch mit den Vereinigten Staaten von Amerika, CR 2013, 822 (826).

48 Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 2011, 755 (758); ; Lejeune, Datenaustausch mit den Vereinigten Staaten von Amerika, CR 2013, 822 (826).

49 Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 2011, 755 (757).

50 Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 2011, 755 (757).

Act 2013“ vor.<sup>51</sup> Allerdings ist dieses Gesetz bislang nicht verabschiedet worden, sondern wurde nach der zweiten Lesung an den „Committee on Commerce, Science, and Transportation“ zurücküberwiesen.<sup>52</sup>

Eine weitere, das stark sektoral ausgeprägte Datenschutzsystem der USA kennzeichnende Folge ist das unterschiedliche Verständnis, was unter „personenbezogenen Daten“ zu verstehen ist.<sup>53</sup> So kann sich je nach Regelungsgegenstand eines bereichsspezifischen Gesetzes eine andere Definition „personenbezogener Daten“ ergeben.

Besonders deutlich wird der in den USA sektoral ausgeprägte Datenschutz durch die Möglichkeit nicht-öffentlicher Stellen zur freiwilligen **Selbstregulierung**. Im Gegensatz zu den Rechtsordnungen der Europäischen Union und der Bundesrepublik ist das Instrument der Selbstregulierung in den USA im nicht-öffentlichen Bereich weit verbreitet. Soweit nämlich keine der wenigen bereichsspezifischen Regelungen anwendbar sind, sind die verantwortlichen Stellen in der Regulierung der eigenen Datenverarbeitung frei.<sup>54</sup> Dies wird zudem dadurch bedingt, dass es bislang in den USA grundsätzlich<sup>55</sup> kein Verfahren gibt, welches die Selbstregulierung vorab einer hoheitlichen Kontrolle unterzieht.<sup>56</sup> Die Selbstregulierung tritt insgesamt vor allem als **Ersatz für staatliche oder föderale Regelungen** ein und dient sogar als Mittel zur Verhinderung staatlicher Rechtsetzung.<sup>57</sup> Hierdurch zeigt sich der wirtschaftliche Gesichtspunkt, unter dem der Datenschutz in den USA betrachtet wird: In den USA wird die Selbstregulierung als Schlüssel zur Schaffung flexibler Regelungen gesehen, um staatliche Eingriffe in die Wirtschaft zu vermeiden. So soll der Befürchtung begegnet werden, durch einen staatlich vorgegebenen Datenschutz könnten Innovationsrechte verloren gehen.<sup>58</sup>

---

51 Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 2011, 755 (758).

52 Stand am 17.03.2015, abrufbar auf: <https://www.congress.gov/bill/113th-congress/senate-bill/1193>, zuletzt abgerufen am 17.03.2015.

53 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (9); Lejeune, Datenaustausch mit den Vereinigten Staaten von Amerika, CR 2013, 822 (826).

54 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 234.

55 Eine Ausnahme findet sich hier lediglich i.R.d. COPPA, welche vorsieht, dass die Federal Trade Commission (FTC) das Selbstregulierungskonzept von „Industriegruppen oder anderer Personen“ vor ihrer Geltung prüft.

56 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (5).

57 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (3, 5, 6); soweit ersichtlich ist ein solches Verfahren lediglich i. R. d. COPPA in der Art vorgesehen, dass die FTC das Selbstregulierungskonzept von „Industriegruppen und anderen Personen“ prüft und gegebenenfalls akzeptiert.

58 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (3, 6).

Abzuwarten bleibt, wie sich das Datenschutzrecht der USA in der Zukunft entwickeln wird. Dort hat die Auseinandersetzung mit den Folgen der Verarbeitung personenbezogener Daten erst begonnen.<sup>59</sup> So hat das Weiße Haus im Jahr 2012 eine Reihe von datenschutzrechtlichen Grundprinzipien ausgearbeitet und dabei an erster Stelle die Selbstbestimmung der Konsumenten über ihre personenbezogenen Daten hervorgehoben, allerdings ohne auf die primäre unternehmerische Selbstregulierung zu verzichten.<sup>60</sup> Auf dieses Konzeptpapier geht ein Anfang des Jahres 2015 durch das Weiße Haus vorgelegter Gesetzesvorschlag zur Verbesserung der Privatsphäre von US-Amerikanern gegenüber privaten Datenverarbeitern zurück.<sup>61</sup>

---

59 Simitis, in: Simitis (Hrsg.)/Dammann, Bundesdatenschutzgesetz, 7. Auflage 2011, Einführung Rn. 110.

60 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 235; "Consumer Privacy in a Network World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", abzurufen auf: <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>, zuletzt abgerufen am 13.03.2015.

61 Consumer Privacy Bill of Rights Act: <https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf>, abgerufen am 12.03.2015.

## 4.3. Synopse der Grundkonzeptionen

	USA	EU	Deutschland
<b>Perspektive auf den Datenschutz</b>	– Wirtschaftliche Perspektive	– Grundrechtliche Perspektive	
<b>Regelungsansatz und Geltungsbereich</b>	– Keine umfassende gesetzliche Regelung für den Datenschutz	– Bislang DSRL als zentrale Regelung – Geplant: EU Datenschutzgrundverordnung	– BDSG als zentrales Datenschutzrecht
	– Bereichsspezifischer Regulationsansatz hat zur Folge, dass dem Datenschutzrecht eine <b>Erlaubnis mit Verbotsvorbehalt</b> zugrunde liegt	– Aus dem allgemeiner Regulationsansatz mit bereichsspezifischen Zusätzen folgt ein <b>Verbot mit Erlaubnisvorbehalt</b>	
	– eine Zweiteilung in einen öffentlichen und nicht-öffentlichen Bereichen ist ebenso wie ein einheitlicher Regelungssatz nicht zu erkennen	– Einheitliche Behandlung von öffentlichen und nicht-öffentlichen Stellen	– Zweiteilung
<b>Rahmenbedingungen der Selbstregulierung</b>	– Kein präventives Verfahren – Ersatz für gesetzliche Regelungen i.S.v. „quasi-gesetzlichen“ Normen – Soweit kein bereichsspezifisches Gesetz anwendbar ist: weitgehende Freiheit in Art und Weise der Datenverarbeitung	– „kontrollierende“ Selbstregulierung – Umfasst lediglich Vollzugsfragen – Bindung an festgelegtes datenschutzrechtliches Mindestschutzniveau	

## 5. Unabhängige Kontrollinstanzen und Rechtsschutz gegen Datenschutzverstöße

### 5.1. Europäische Union

Die Rechtsordnung der Europäischen Union verdeutlicht die Bedeutung des Datenschutzes, indem durch verschiedene Vorschriften die Möglichkeit gewährt wird, außergerichtliche Institutionen oder die Gerichte selbst zum Schutz gegen datenschutzrechtlichen Verstöße anzurufen. So sieht Art. 8 Abs. 3 GRCh die Bestellung einer **unabhängigen Kontrollinstanz** vor, welche die Einhaltung des Schutzes personenbezogener Daten überwacht. Eine vergleichbare Verpflichtung findet sich in Art. 16 Abs. 2 S. 2 AEUV, in Art. 39 S. 2 EUV und in Art. 28 DSRL. Die unabhängige Stelle ist der **Europäische Datenschutzbeauftragte**.<sup>62</sup> Dieser ist primär ein Instrument der Eigenkontrolle der EU-Institutionen.<sup>63</sup> Für den Bereich der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Union werden die Einzelheiten in einer Verordnung über den Datenschutz der EU-Institutionen (VO-DSI) festgelegt.<sup>64</sup> Aufgabe des Europäischen Datenschutzbeauftragten ist es nach Art. 41 Abs. 2 VO-DSI im Hinblick auf die Verarbeitung personenbezogener Daten sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden. In Art. 32 Abs. 2 VO-DSI wird jeder betroffenen Person das Recht zugesprochen, beim Europäischen Datenschutzbeauftragten eine Beschwerde einzureichen, wenn sie der Ansicht ist, dass die ihr in Art. 286 EG Vertrag (nunmehr Art. 16 AEUV) eingeräumten Rechte infolge der Verarbeitung von sie selbst betreffenden personenbezogenen Daten durch ein Organ oder eine Einrichtung der Gemeinschaft verletzt wurden.

Der **individuelle gerichtliche Rechtsschutz gegen datenschutzrechtliche Verstöße durch Institution der Europäischen Union** ist beschränkt. Besondere Gerichte, welche sich mit Verstößen gegen unionsrechtliches Datenschutzrecht befassen, existieren auf Unionsebene ebenso wenig wie eine besondere Individualbeschwerde vor dem Gerichtshof der Europäischen Union (EuGH) wegen der Verletzung von Chartagrundrechten.<sup>65</sup> Somit greifen weder die Grundrechtecharta noch die Verträge den im Verfassungskonvent vorgebrachten Vorschlag auf, eine „Chartabeschwerde“ zum EuGH einzuführen.<sup>66</sup> Vielmehr beschränkte man sich auf kleine Änderungen der Voraussetzungen einer Individualklage zum EuGH im Rahmen von Art. 263 Abs. 4 AEUV.<sup>67</sup> Danach kann nun jede natürliche oder juristische Person unter den Bedingungen des Art. 263 Abs. 1 und 2 AEUV gegen an sie gerichtete oder sie unmittelbar und individuell betreffenden Handlungen sowie gegen Rechtsakte mit Verordnungscharakter, die sie unmittelbar betreffen und keine Durchführungsmaßnahmen

---

62 Gersdorf, in Gersdorf/Paal, BeckOK EU-GRCharta, Edition 7 Stand 01.11.2014, Art. 8 Rn. 41.

63 Eckhardt/Kramer/Mester, Auswirkungen der geplanten EU-DS-GVO auf den deutschen Datenschutz, DuD 2013, 623 (628).

64 Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft zum freien Datenverkehr, ABl. L8 v. 12.01.2001.

65 Streinz/Ohler/Herrmann, Der Vertrag von Lissabon zur Reform der EU, 3. Auflage 2010, § 14 Abschnitt V. Nummer 4.

66 Streinz/Ohler/Herrmann, Der Vertrag von Lissabon zur Reform der EU, 3. Auflage 2010, § 14 Abschnitt V. Nummer 4.

67 Streinz/Ohler/Herrmann, Der Vertrag von Lissabon zur Reform der EU, 3. Auflage 2010, § 14 Abschnitt V. Nummer 4.

sind, **Nichtigkeitsklage** erheben. Beschwerdegegenstand sind nach Art. 263 Abs. 1 S. 2 AEUV Handlungen der Einrichtungen oder sonstiger Stellen der Union mit Rechtswirkung gegenüber Dritten. Erfüllt eine Handlung der durch Art. 263 Abs. 1 AEUV bezeichneten unionsrechtlichen Institutionen diese engen Voraussetzungen, kann also ein datenschutzrechtlicher Verstoß vor dem EuGH durch eine Individualbeschwerde gerügt werden. Zusätzlich kann gegen beschwerende Entscheidungen des Europäischen Datenschutzbeauftragten gemäß Art. 32 Abs. 3 VO-DSI Klage beim EuGH eingereicht werden.<sup>68</sup>

Dem Europäischen Datenschutzbeauftragten selbst steht eine eigene Rechtsschutzmöglichkeit zu. So kann dieser gemäß Art. 47 lit. h der VO-DSI unter den im Vertrag vorgesehenen Voraussetzungen Klage vor dem EuGH erheben.<sup>69</sup> Allerdings beschränkt sich dieses Klagerecht auf Rechtsakte, welche ihn selbst in seinem Status betreffen.<sup>70</sup> Eine Möglichkeit des Datenschutzbeauftragten, im Namen des Betroffenen zu klagen (i.S.e. Prozessstandschaft), ist damit nicht vorgesehen. In dem Vorschlag zur **EU-Datenschutzgrundverordnung** hingegen sollen Einrichtungen, Organisationen oder Verbände, die sich den Schutz der Rechte und Interessen der betroffenen Personen im Bereich des Datenschutzes zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, das Recht haben, im Namen der betroffenen Person Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen oder unabhängig von der Beschwerde einer betroffenen Person eine eigene Beschwerde zu erheben, wenn ihrer Ansicht nach der Schutz personenbezogener Daten verletzt wurde (Art. 76 DSGVO). Hierdurch wird die Möglichkeit einer **Verbandsklage** eröffnet.<sup>71</sup> Zusätzlich soll der betroffenen Person, die sich in ihrem durch die Verordnung gewährten Recht verletzt sieht, das Recht zustehen, bei einer Aufsichtsbehörde in einem Mitgliedsstaat Beschwerde zu erheben, und wenn die Aufsichtsbehörde auf die Beschwerde nicht reagiert oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist, ein Recht auf gerichtlichen Rechtsschutz zustehen (Art. 75 DSGVO).

Eine Individualbeschwerde wegen der **Verletzung von Chartagrundrechten durch die Mitgliedsstaaten** sieht das Unionsrecht hingegen nicht vor. Schließlich zählt die Nichtigkeitsklage nach Art. 263 AEUV Akte der Mitgliedsstaaten nicht als zulässigen Beschwerdegegenstand auf. Damit ist der Betroffene auf den innerstaatlichen Rechtsweg und bei Ausschöpfung desselben auf eine Individualbeschwerde vor dem Europäischen Gerichtshof für Menschenrechte gem. Art. 34 EMRK beschränkt, soweit Rechte aus der EMRK betroffen sind. In dieser Konsequenz verlangt Art. 22 DSLR von den Mitgliedsstaaten die Einrichtung eines Rechtsbehelfs, der es jeder Person

---

68 Sobotta, in Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 54. Ergänzungslieferung 2014, Art. 16 Rn. 58, (dieser geht von einer Klage gegen beschwerte Entscheidungen der Datenschutzkontrollstelle aus).

69 Sobotta, in Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 54. Ergänzungslieferung 2014, Art. 16 Rn. 60.

70 Sobotta, in Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 54. Ergänzungslieferung 2014, Art. 16 Rn. 60.

71 Fraktionen CDU/CSU und FDP ablehnend zur Verbandsklage: BT-Drs. 17/11810 S.2, 6; das Europäische Parlament hat in seiner Entschließung zum Vorschlag der Europäischen Kommission gegen eine Verbandsklage ohne Einwilligung und Beauftragung durch den Betroffenen ausgesprochen, vgl. hierzu geänderter Text zu Art. 76, abrufbar auf: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE>, zuletzt abgerufen am 18.03.2015.



ermöglicht, die Verletzung ihrer Rechte zu rügen, welche ihr durch die geltenden einzelstaatlichen Rechtsvorschriften betreffend die Verarbeitung von Daten garantiert sind.

## 5.2. Bundesrepublik

Nach § 4f Abs. 1 S. 1 BDSG haben öffentliche und nicht-öffentliche Stellen, welche personenbezogene Daten automatisiert verarbeiten, einen **Datenschutzbeauftragten** zu bestellen. Dieser wirkt auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hin (§ 4g Abs. 1 BDSG). Zur präventiven Kontrolle im Rahmen der Selbstregulierung kann überdies die Aufsichtsbehörde die Entwürfe der Unternehmen auf Einhaltung des geltenden Datenschutzrechts überprüfen. Hierzu ist die Aufsichtsbehörde jedoch auf die freiwillige Vorlage durch die Unternehmen angewiesen (hierzu bereits 4.1.). Abgesehen von der Bestellung eines Datenschutzbeauftragten sieht die deutsche Rechtsordnung **keine weiteren speziell zum Datenschutz einzurichtenden Institutionen** vor. **Ebenso wenig sind spezielle gerichtliche Rechtsbehelfe vorgesehen.** §§ 7 und 8 BDSG stellen lediglich besondere Anspruchsgrundlagen zur Geltendmachung von Schadensersatz bei Verstößen dar. Es bleibt daher bei öffentlich-rechtlichen Streitigkeiten beim verwaltungsgerichtlichen (§ 40 Abs. 1 S. 1 VwGO) und im Rahmen von bürgerlichen Rechtsstreitigkeiten beim ordentlichen Rechtsweg (§ 13 GVG).

## 5.3. USA

Anders als dem Unionsrecht und dem deutschen Recht ist der US-amerikanischen Rechtsordnung **keine genuine Datenschutzaufsichtsbehörde** zu entnehmen.<sup>72</sup> Im Rahmen privatrechtlicher Streitigkeiten wegen etwaiger Verstöße gegen die unternehmenseigenen Selbstregulierungen bleibt damit – soweit die Selbstregulierung keine eigene Regressmöglichkeit vorsieht – in der Regel nur die Möglichkeit zur Beschwerde bei der **Federal Trade Commission** (Bundeshandelskommission), kurz FTC.<sup>73</sup> Diese kann Verstöße als „Unfair Competition“ ahnden.<sup>74</sup> So hat die FTC in den letzten Jahren in Einzelfällen erhebliche Sanktionen verhängt.<sup>75</sup> Einen besonderen Rechtsschutz sieht hingegen der HIPAA vor. Der HIPAA verpflichtet die betroffenen Unternehmen, personenbezogene Patientendaten zu schützen, und gibt dem „Department of Health and Human Services“ bei Verletzung dieser Pflicht das Recht und die entsprechenden Befugnisse, direkt gegen den Verantwortlichen vorzugehen.<sup>76</sup>

Ein Verfahren zur Vorabprüfung der unternehmerischen Verhaltensregeln durch einen Hoheitsträger sieht die US-amerikanische Rechtsordnung – anders als das Verfahren zur kontrollierenden

---

72 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (6).

73 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (6).

74 Kranig/Peintinger, Selbstregulierung im Datenschutzrecht – Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, 3 (6).

75 Vgl. hierzu Fn. 41 bei: Lejeune, Datenaustausch mit den Vereinigten Staaten von Amerika, CR 2013, 822 (828).

76 Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 2011, 755 (757).

