Bundesrat **zu Drucksache 145/17 (Beschluss)**

25.10.17

Unterrichtung
durch die Europäische Kommission

Stellungnahme der Europäischen Kommission zu dem Beschluss des Bundesrates zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)

C(2017) 6935 final

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

EUROPÄISCHE KOMMISSION

Brüssel, 20. 10. 2017
C(2017) 6935 final

Sehr geehrte Frau Bundesratspräsidentin,

die Kommission dankt dem Bundesrat für seine Stellungnahme zum Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation {COM(2017) 10 final} („Verordnung über Privatsphäre und elektronische Kommunikation").

Die Kommission ist überzeugt, dass der Vorschlag den Schutz der Privatsphäre von Endnutzern verbessern, das Vertrauen in digitale Dienste stärken und die Unternehmen in die Lage versetzen wird, in vollem Umfang am digitalen Binnenmarkt teilzunehmen und von diesem zu profitieren.

Die Kommission ist erfreut, dass der Bundesrat die Zielsetzung des Verordnungsvorschlags begrüßt, die Privatsphäre der Endnutzer elektronischer Kommunikationsdienste zu schützen und für gleiche Dienste gleiche Wettbewerbsbedingungen zu gewährleisten. Die Kommission nimmt die Stellungnahme des Bundesrates ordnungsgemäß zur Kenntnis.

Die Kommission dankt dem Bundesrat für die übermittelten Fragen und Anmerkungen. Die Kommission begrüßt die Gelegenheit, einige Aspekte ihres Vorschlags klarzustellen, und hofft, die Bedenken des Bundesrats mit ihren Ausführungen ausräumen zu können.

Die Antworten auf die konkreten Fragen und Anmerkungen aus der Stellungnahme entnehmen Sie bitte dem beigefügten Anhang.

Die Erläuterungen in dieser Antwort stützen sich auf den ursprünglichen Vorschlag der Kommission, der derzeit im Rahmen des Gesetzgebungsverfahrens dem Europäischen Parlament und dem Rat zur Erörterung vorliegt.

Die Kommission hofft, dass die in der Stellungnahme des Bundesrats aufgeworfenen Fragen mit diesen Ausführungen geklärt werden konnten, und sieht der Fortsetzung des politischen Dialogs erwartungsvoll entgegen.

Mit freundlichen Grüßen

Frans Timmermans
Erster Vizepräsident

Andrus Ansip
Vizepräsident

Frau Malu DREYER
Präsidentin des Bundesrates
Leipziger Straße 3-4
10117 BERLIN
DEUTSCHLAND

ANHANG

Die Kommission hat die in der Stellungnahme des Bundesrates angesprochenen Punkte sorgfältig geprüft und möchte dazu, thematisch zusammengefasst, folgende Anmerkungen machen.

1. Verhältnis zwischen der vorgeschlagenen Verordnung über Privatsphäre und elektronische Kommunikation und der Datenschutz-Grundverordnung

Der Bundesrat fordert, dass das Verhältnis zwischen der vorgeschlagenen Verordnung und den Vorschriften der Datenschutz-Grundverordnung[1] genauer festgelegt werden muss. Eines der Hauptziele der Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation[2] besteht darin, im Einklang mit der Strategie für einen digitalen Binnenmarkt ein hohes Schutzniveau für die Verbraucher in der gesamten Union zu gewährleisten und einen kohärenten Rechtsrahmen für den Datenschutz zu erhalten. Wie in Artikel 1 Absatz 3 der vorgeschlagenen Verordnung dargelegt, stellt diese eine Lex specialis zur Datenschutz-Grundverordnung dar und wird diese im Hinblick auf elektronische Kommunikationsdaten, die als personenbezogene Daten einzustufen sind, präzisieren und ergänzen. Alle Fragen der Verarbeitung personenbezogener Daten, die in diesem Vorschlag nicht spezifisch geregelt sind, werden von der Datenschutz-Grundverordnung erfasst.

Kapitel II des Vorschlags sieht unter anderem Folgendes vor: Bestimmungen zur erlaubten Verarbeitung elektronischer Kommunikationsdaten (Artikel 6), Ausnahmen vom Verbot der Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und der Erhebung von Informationen aus Endeinrichtungen der Endnutzer (Artikel 8 Absatz 1) und Ausnahmen vom Verbot der Erhebung von Informationen, die von Endeinrichtungen ausgesendet werden (Artikel 8 Absatz 2). In der Praxis bedeutet dies, dass die Bestimmungen der Verordnung unter diesen besonderen Umständen gegenüber den allgemeinen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten nach der Datenschutz-Grundverordnung Vorrang hätten[3]. Was die personenbezogenen Daten betrifft, so bleiben hingegen die ursprünglichen Bestimmungen anwendbar, wie beispielsweise das Recht auf Vergessenwerden, das Recht auf Zugang, Löschung und Berichtigung von Daten sowie die Vorschriften in Bezug auf die Übermittlung von Daten an Drittländer. Im Rahmen des Gesetzgebungsverfahrens wird darauf geachtet werden, einen klaren Rechtsrahmen zu schaffen und Rechtsunsicherheit zu vermeiden.

---

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

2 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

3 In Erwägungsgrund 5 der vorgeschlagenen Verordnung heißt es: „Eine Verarbeitung elektronischer Kommunikationsdaten durch Betreiber elektronischer Kommunikationsdienste sollte nur im Einklang mit der vorliegenden Verordnung erlaubt sein." (*Hervorhebung hinzugefügt*).

2. Vertraulichkeit elektronischer Kommunikationsdaten: Anwendungsbereich

Der Bundesrat bittet um Klarstellung, inwieweit Internetanbieter, die Ortungsdienste anbieten (wie etwa Mapping-Dienste) und folglich ebenso Standortdaten verarbeiten, gleich behandelt werden wie elektronische Kommunikationsdienste, die Standortdaten verarbeiten.

Der Vorschlag sieht im Einklang mit der derzeitigen Datenschutzrichtlinie für elektronische Kommunikation vor, dass die Vertraulichkeit der Kommunikation natürlicher und juristischer Personen gewahrt werden muss. Dies deckt sich auch mit Artikel 7 der Charta der Grundrechte der Europäischen Union, wonach private und juristische Personen das Recht auf Achtung des Privatlebens und der Kommunikation haben. Der Vorschlag sieht vor, dass elektronische Kommunikationsdienste Metadaten, einschließlich Standortdaten, löschen müssen, außer wenn deren Verarbeitung nach Artikel 6 der vorgeschlagenen Verordnung erlaubt ist. Dies ist darauf zurückzuführen, dass Kommunikationsmetadaten Rückschlüsse auf die Lebensgewohnheiten einer Person zulassen, etwa ihr Bewegungsprofil, ihre Tätigkeiten und ihre sozialen Beziehungen.

Ein Mobiltelefon verbindet sich permanent mit dem nächsten Mobilfunkmast und übermittelt dem elektronischen Kommunikationsdienst Standortdaten. Der elektronische Kommunikationsdienst kann nicht abgeschaltet werden, da man sonst die Netzverbindung verlöre und somit weder selbst andere anrufen noch angerufen werden könnte. Bei bestimmten anderen Diensten, die Standortdaten verarbeiten, verhält sich dies anders. Einige Dienste stützen sich auf GPS-Standortdaten. Das GPS-Signal kann der Nutzer abschalten, sodass sein Standort dem betreffenden Dienst nicht übermittelt wird. Diese Daten werden durch die Datenschutz-Grundverordnung geschützt[4].

Unter verschiedenen Umständen ist es notwendig, Standortdaten auch außerhalb eines Kommunikationsvorgangs zu verarbeiten, und dies ist durch die Datenschutz-Grundverordnung gedeckt. Das ist beispielsweise bei einem Arbeitgeber der Fall, der wissen muss, welche Arbeitnehmer sich in einem bestimmten Gebäude befinden, und dafür ein Ausweissystem nutzt, oder bei einem Taxiunternehmen, das den Standort seiner Taxis ermitteln können muss. In bestimmten Fällen kann nach der Datenschutz-Grundverordnung die Einwilligung der Person erforderlich sein, dies muss aber nicht unbedingt der Fall sein. So kann sich beispielsweise im Rahmen eines Beschäftigungsverhältnisses der Arbeitgeber nicht auf die Einwilligung als Rechtsgrundlage für die Verarbeitung von Standortdaten stützen, da ein Arbeitnehmer die Einwilligung zwar theoretisch verweigern könnte, dadurch in der Praxis jedoch Gefahr liefe, die betreffende Arbeitsstelle nicht angeboten zu bekommen bzw. zu verlieren. Unter solchen Umständen gilt die Erteilung der Einwilligung als nicht freiwillig erfolgt und ist daher unwirksam[5].

Da die Datenschutz-Grundverordnung unter ganz unterschiedlichen Umständen Anwendung findet, ist ersichtlich, dass unterschiedliche Rechtsgrundlagen herangezogen werden müssen,

---

4 Wenn die GPS-Standortdaten aus der Endeinrichtung erlangt werden, müssen ferner die Verarbeitungsfunktionen der Endeinrichtung genutzt werden, sodass nach Artikel 8 Absatz 1 der vorgeschlagenen Verordnung die Einwilligung des Nutzers erforderlich ist.

5 Stellungnahme Nr. 13/2011 der Artikel-29-Datenschutzgruppe (WP 29) zu Geolokalisierungsdiensten bei intelligenten Mobilgeräten (WP 185).

wenn Standortdaten außerhalb eines Kommunikationsvorgangs verarbeitet werden sollen. In dem in Rede stehenden Fall weisen die elektronischen Kommunikationsdienste jedoch, wie oben dargelegt, besondere, bekannte Umstände auf, sodass eine besondere Regelung gerechtfertigt ist.

Darüber hinaus wirft der Bundesrat die Frage auf, ob der Anwendungsbereich der Verordnung auf die Übermittlung von Kommunikationsvorgängen zwischen Maschinen (M2M) ausgedehnt werden sollte oder ob dadurch die Innovation beeinträchtigt würde. Die vorgeschlagene Verordnung würde die Übermittlung von M2M-Kommunikationsdaten abdecken, sofern diese über einen elektronischen Kommunikationsdienst erfolgt – ebenso wie dies gegenwärtig bei der Datenschutzrichtlinie für elektronische Kommunikation der Fall ist. Dies hängt damit zusammen, dass M2M-Kommunikationsdaten sich ebenso wie Kommunikationsvorgänge von natürlichen oder juristischen Personen auf eine natürliche Person beziehen oder Geschäftsinformationen darstellen können. Wenn die Übermittlung von M2M-Daten nicht vertraulich sein müsste, könnte dies zu Eingriffen in das Recht auf Achtung des Privatlebens und der Kommunikation der betreffenden natürlichen bzw. juristischen Person führen.

3. Vertraulichkeit der Endeinrichtungen

Der Bundesrat sieht die vorgeschlagene Bestimmung zum Schutz der Vertraulichkeit von Endeinrichtungen (Artikel 8 Absatz 1 Buchstabe d des Vorschlags) als verfehlt an.

Artikel 8 Absatz 1 Buchstabe d sieht vor, dass die Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und die Erhebung von Informationen aus Endeinrichtungen der Endnutzer ohne Einwilligung des betreffenden Endnutzers zulässig ist, sofern dies für die Messung des Webpublikums nötig ist und der Betreiber des Dienstes der Informationsgesellschaft diese Messung durchführt. Bei Messungen des Webpublikums, die vom Betreiber des Dienstes der Informationsgesellschaft selbst durchgeführt werden, wird davon ausgegangen, dass diese keine oder nur geringfügige Auswirkungen auf die Privatsphäre haben. Diese Ausnahmegenehmigung wird vom Europäischen Datenschutzbeauftragten und der Artikel-29-Datenschutzgruppe unterstützt, sofern bestimmte Vorkehrungen getroffen werden[6]*.*

Was die in Artikel 9 Absatz 2 der vorgeschlagenen Verordnung vorgesehene Möglichkeit betrifft, die Einwilligung in den passenden technischen Einstellungen zu erteilen, so möchte die Kommission betonen, dass die Einwilligung gemäß den Voraussetzungen von Artikel 4 Absatz 11, Artikel 7 und Erwägungsgrund 42 der Datenschutz-Grundverordnung erfolgen muss. Somit muss es sich bei der Einwilligung um eine freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer eindeutigen bestätigenden Handlung handeln. Zu diesem Zweck sieht Erwägungsgrund 24

---

[6] Stellungnahme Nr. 6/2017 des EDSB zum Vorschlag für eine Verordnung über den Schutz der Privatsphäre in der elektronischen Kommunikation (Verordnung über Privatsphäre und elektronische Kommunikation); Stellungnahme Nr. 01/2017 der Artikel-29-Datenschutzgruppe (WP 29) zur vorgeschlagenen Verordnung in Bezug auf die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) (WP 247); Stellungnahme Nr. 04/2012 der Artikel-29-Datenschutzgruppe (WP 29) zur Ausnahme von Cookies von der Einwilligungspflicht (WP 194).

der vorgeschlagenen Verordnung vor, dass Webbrowser dem Nutzer erlauben sollten, Ausnahmen für bestimmte Websites zu machen oder in Listen festzulegen oder anzugeben, von welchen Websites Cookies (auch von Drittanbietern) immer oder niemals angenommen werden sollen. Wenn es in den technischen Einstellungen nicht möglich ist, die Einwilligung in einer Weise zu erteilen, die den Anforderungen der Datenschutz-Grundverordnung genügt, können die technischen Einstellungen als für die Erteilung der Einwilligung ungeeignet erachtet werden.

4. Pflichten für Software, die elektronische Kommunikation ermöglicht

Der Bundesrat bittet um Erläuterung, auf welche Akteure sich Artikel 10 der vorgeschlagenen Verordnung bezieht. Die Anforderung, dass die Möglichkeit geboten werden muss zu verhindern, dass andere Parteien als die Endnutzer Informationen in der Endeinrichtung eines Endnutzers speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten, bezieht sich auf die Software, die eine elektronische Kommunikation ermöglicht. Dies gilt für Browser, aber auch für andere Arten von Software, so etwa für Anwendungen, die Anrufe und die Nachrichtenübermittlung ermöglichen oder Navigationshilfe bieten, wie in Erwägungsgrund 22 erläutert. Im Einklang mit dem Vorschlag des Bundesrates schließt dies auch Betriebssysteme ein, die elektronische Kommunikation ermöglichen. Hardware fällt hingegen nicht in den Anwendungsbereich der vorgeschlagenen Verordnung. Die Funkanlagenrichtlinie sieht jedoch vor, dass Anlagen so konstruiert sein müssen, dass sichergestellt ist, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden[7].

Nach Artikel 10 Absatz 1 der vorgeschlagenen Verordnung muss Software eine bestimmte Einstellung bieten, durch die verhindert wird, dass Dritte Informationen in der Endeinrichtung speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten. Dies schließt, wie in Erwägungsgrund 23 der vorgeschlagenen Verordnung dargelegt, nicht aus, dass Software auch andere Einstellungsmöglichkeiten bietet, wie etwa „Cookies immer annehmen" oder „Nur Cookies von Erstanbietern annehmen". Durch die Anforderung nach Artikel 10 Absatz 1 wird sichergestellt, dass eine technische Einstellung zur Verfügung steht, um das Verbot nach Artikel 8 Absatz 1 wirksam umzusetzen. Nach Artikel 8 Absatz 1 ist die Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und die Erhebung von Informationen aus Endeinrichtungen der Endnutzer verboten, außer wenn eine der unter den Buchstaben a bis d beschriebenen Situationen vorliegt. Dieses Verbot steht mit dem Ziel im Einklang, die Integrität der Endeinrichtungen zu schützen. Da die derzeitigen Verfolgungstechniken mit der Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen verbunden sind, soll Artikel 10 Absatz 1 dazu führen, dass mit der erforderlichen Einstellung dasselbe Ergebnis erzielt wird wie mit einer „Nicht verfolgen"-Einstellung, nämlich eine Verfolgung zu verhindern. Das Ziel des Artikels 10 Absatz 1 wird in den Erwägungsgründen 22 bis 24 der vorgeschlagenen Verordnung dargelegt.

---

[7] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG – Text von Bedeutung für den EWR (ABl. L 153 vom 22.5.2014, S. 62).

5. Erhebung von Daten, die vom Gerät ausgesendet werden (Offline-Verfolgung)

Die vorgeschlagene Verordnung enthält in Artikel 8 Absatz 2 Bestimmungen zur Erhebung von Daten, die vom Gerät ausgesendet werden. Der Bundesrat äußert Bedenken, dass durch die vorgeschlagene Verordnung das Schutzniveau sinken würde. Die Kommission möchte betonen, dass mit der vorgeschlagenen Verordnung nicht die Absicht verfolgt wird, das Schutzniveau zu senken.

Mit dem Vorschlag soll einer besonderen Situation Rechnung getragen werden: der Zählung von Personen ohne die Erhebung jeglicher anderer Informationen, wie in Erwägungsgrund 25 dargelegt. Für stärker in die Privatsphäre eingreifende Zwecke, beispielsweise die Zusammenführung von erhobenen Daten mit personenbezogenen Daten, reicht die Bereitstellung von Informationen möglicherweise nicht aus, sodass eine zusätzliche Rechtsgrundlage aus der Datenschutz-Grundverordnung erforderlich sein kann.

6. Beschränkung der Rechte und Pflichten durch die vorgeschlagene Verordnung über Privatsphäre und elektronische Kommunikation

Der Bundesrat äußert Bedenken hinsichtlich des Ausgleichs zwischen den erforderlichen Maßnahmen zur Gewährleistung des Schutzes der Kommunikationsdaten auf der einen Seite und den Erfordernissen der effektiven Bekämpfung von Terrorismus und Kriminalität auf der anderen Seite. Zu diesem Zweck bittet der Bundesrat um eine Erläuterung des Verhältnisses zwischen Artikel 2 Absatz 2 Buchstabe d, der besagt, dass die Verordnung nicht gilt für „Tätigkeiten zuständiger Behörden zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit", und Artikel 11, der Beschränkungen vorsieht.

Aus Artikel 2 Absatz 2 Buchstabe d der vorgeschlagenen Verordnung geht hervor, dass die Verordnung auf die Tätigkeiten der zuständigen Behörden zu den genannten Zwecken nicht anwendbar ist[8]. Artikel 11 bezieht sich hingegen auf andere Akteure wie die Anbieter elektronischer Kommunikationsdienste und besagt, dass die Mitgliedstaaten oder die Union im Wege von Gesetzgebungsmaßnahmen den Umfang von deren Rechten und Pflichten nach dieser Verordnung beschränken können.

Der Bundesrat vertritt die Ansicht, dass die Mitgliedstaaten aufgefordert werden sollten, bei der Bekämpfung von Cyberbedrohungen zusammenzuarbeiten. Die Kommission ist ebenfalls der Auffassung, dass die Mitgliedstaaten im Bereich der Cybersicherheit zusammenarbeiten sollten, und weist diesbezüglich darauf hin, dass die gesetzgebenden Organe der Union diesem Anliegen mit der Richtlinie (EU) 2016/1148 über die Sicherheit von Netz- und Informationssystemen (im Folgenden die „NIS-Richtlinie") Rechnung getragen haben. Die Richtlinie sieht vor, dass Mechanismen zur Verbesserung der strategischen und technischen

[8] Diese Tätigkeiten fallen möglicherweise in den Anwendungsbereich der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

Zusammenarbeit zwischen den Mitgliedstaaten eingerichtet werden, um ein hohes gemeinsames Cybersicherheitsniveau in der Europäischen Union zu erreichen. Im Hinblick auf die Vertiefung der strategischen Zusammenarbeit wurde in der Richtlinie festgelegt, dass eine Kooperationsgruppe eingerichtet wird, die den Austausch von Informationen zwischen den zuständigen nationalen Behörden fördern und Vertrauen zwischen ihnen aufzubauen soll. Die Richtlinie sah ferner die Schaffung eines Netzwerks von Computer-Notfallteams (Computer Security Incident Response Teams Network – CSIRTs-Netzwerk) vor, um eine rasche und wirksame operative Zusammenarbeit zu erreichen. Über das CSIRTs-Netzwerk können die nationalen Experten Informationen über mögliche Gefahren für die Cybersicherheit austauschen und im Falle eines Cybervorfalls effizienter zusammenarbeiten.

Der Bundesrat vertritt ferner die Auffassung, dass die Sicherheitsbehörden zusammenarbeiten und auf effektive Weise Daten austauschen sollten. Da die nationale Sicherheit jedoch gemäß Artikel 4 Absatz 2 des Vertrags über die Europäische Union in der alleinigen Zuständigkeit der einzelnen Mitgliedstaaten liegt, beabsichtigt die Kommission nicht, eine Initiative zum Datenaustausch und zur Zusammenarbeit zwischen den Sicherheitsbehörden einzuleiten.

Der Bundesrat hält es zudem für unzureichend, dass die in Artikel 11 der vorgeschlagenen Verordnung vorgesehenen Beschränkungen lediglich durch „Ausführungen im Vorblatt" erläutert werden, und schlägt vor, Artikel 15 Absatz 1 Satz 2 der Datenschutzrichtlinie für elektronische Kommunikation in diese Bestimmung aufzunehmen.

Die im Vorschlag enthaltene Bestimmung nimmt den wesentlichen Inhalt des Artikels 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation auf und passt ihn unter Verweis auf Artikel 23 Absatz 1 Buchstaben a bis e der Datenschutz-Grundverordnung an den betreffenden Wortlaut der Datenschutz-Grundverordnung an. Konkret sieht die Bestimmung vor, dass die Mitgliedstaaten den Umfang der in bestimmten Artikeln der Datenschutzrichtlinie für elektronische Kommunikation vorgesehenen Rechte und Pflichten beschränken können. Somit bleibt es den Mitgliedstaaten unbenommen, nationale Vorschriften zur Vorratsdatenspeicherung zu erlassen. Diese Vorschriften müssen allerdings mit dem Unionsrecht, der Rechtsprechung des Gerichtshofs zur Auslegung der Datenschutzrichtlinie für elektronische Kommunikation und der Charta der Grundrechte der Europäischen Union im Einklang stehen. Folglich müssen die Vorschriften unter anderem gewährleisten, dass die Vorratsdatenspeicherung gezielt erfolgt[9]*. Vor diesem Hintergrund sieht die Kommission keinen rechtlichen Grund, Artikel 11 in dieser Hinsicht zu ändern.*

7. <u>Durchsetzung der vorgeschlagenen Verordnung und Rechtsbehelfe</u>

Die vorgeschlagene Verordnung sieht vor, dass die für die Überwachung der Anwendung der Datenschutz-Grundverordnung zuständigen unabhängigen Aufsichtsbehörden auch für die Überwachung der Anwendung dieser Verordnung zuständig sind. Der Bundesrat befürchtet,

---

[9] Siehe Urteil des Gerichtshofs vom 8. April 2014, Digital Rights Ireland und Seitlinger u. a., verbundene Rechtssachen C-293/12 und C-594/12, ECLI:EU:C:2014:238; Urteil des Gerichtshofs vom 21. Dezember 2016, Tele2 Sverige AB und Secretary of State for the Home Department, verbundene Rechtssachen C-203/15 und C-698/15, ECLI:EU:C:2016:970.

dass dies zu einer Mehrbelastung der Datenschutzaufsichtsbehörden führt und schlägt vor, den Mitgliedstaaten diesbezüglich mehr Flexibilität einzuräumen.

In der vorgeschlagenen Verordnung werden die Überwachungsbestimmungen mit den betreffenden Vorschriften der Datenschutz-Grundverordnung in Einklang gebracht, um einen einheitlichen Rechtsrahmen zu gewährleisten.

In den meisten Fällen geht es bei der Durchsetzung privatsphärebezogener Bestimmungen im Zusammenhang mit elektronischer Kommunikation nicht nur um die Privatsphäre, sondern auch um den Datenschutz. Deshalb zählt Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) zu den Rechtsgrundlagen der vorgeschlagenen Verordnung. Artikel 16 AEUV bildet eine besondere Rechtsgrundlage für den Erlass von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Da elektronische Kommunikationsvorgänge, an denen natürliche Personen beteiligt sind, in der Regel als personenbezogene Daten einzustufen sind, sollte der Schutz natürlicher Personen im Hinblick auf ihre Privatsphäre in der Kommunikation und die Verarbeitung solcher Daten auf Artikel 16 AEUV gestützt werden. Artikel 16 AEUV sieht vor, dass die Einhaltung dieser Vorschriften von unabhängigen Behörden überwacht wird. Das bedeutet, dass die Aufsichtsbehörden, die die Anwendung der Datenschutz-Grundverordnung und der vorgeschlagenen Verordnung überwachen, unabhängig sein müssen. Artikel 52 der Datenschutz-Grundverordnung enthält Anforderungen in Bezug auf die Unabhängigkeit der Behörden, die die Anwendung der Datenschutz-Grundverordnung überwachen. Dass die Aufsichtsbehörden, die die Anwendung der Datenschutz-Grundverordnung überwachen, unabhängig sein müssen, wurde bereits dargelegt; wenn diese Behörden auch mit der Durchsetzung der vorgeschlagenen Verordnung betraut werden, ist folglich gewährleistet, dass diese Durchsetzungsbehörden ebenfalls unabhängig sind.

Abgesehen von der Unabhängigkeit muss sichergestellt werden, dass für die Durchsetzung der vorgeschlagenen Verordnung dieselben Behörden zuständig sind wie für die Durchsetzung der Datenschutz-Grundverordnung; dadurch soll vermieden werden, dass es in Bezug auf datenschutzrechtliche Aspekte zu Meinungsverschiedenheiten zwischen den Behörden kommt, die für die Durchsetzung der Datenschutz-Grundverordnung und der vorgeschlagenen Verordnung zuständig sind. Das könnte zudem dazu führen, dass die Durchsetzung der vorgeschlagenen Verordnung durch die Kohärenz und die im Rahmen der Datenschutz-Grundverordnung eingerichteten Mechanismen der einzigen Anlaufstelle begünstigt wird. Dies ist insbesondere in Anbetracht der Ausdehnung des Anwendungsbereichs der vorgeschlagenen Verordnung auf Over-the-Top-Dienste von Belang. Da diese Dienste naturgemäß grenzüberschreitend angeboten werden, würden die Mechanismen der Datenschutz-Grundverordnung sowohl den Durchsetzungsbehörden als auch den Unternehmen zugutekommen.

Wenn die Durchsetzung der vorgeschlagenen Verordnung zu einer Mehrbelastung der zuständigen Behörde führen sollte, müssen deren Ressourcen entsprechend aufgestockt werden. Diesbezüglich heißt es in Erwägungsgrund 38: „Jede Aufsichtsbehörde sollte

zusätzlich mit Finanzmitteln, Personal, Räumlichkeiten und Infrastruktur ausgestattet werden, die für die wirksame Wahrnehmung ihrer Aufgaben nach dieser Verordnung notwendig sind." Dieser Erwägungsgrund besagt ferner, dass die Mitgliedstaaten mehr als eine Aufsichtsbehörde haben können sollten, „wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht."

Ferner schlägt der Bundesrat die Einführung eines Verbandsklagerechts vor. Dieser Vorschlag bezieht sich auf Artikel 80 der Datenschutz-Grundverordnung. Nach Ansicht der Kommission sind nach der vorgeschlagenen Verordnung Verbandsklagen möglich. Gemäß Artikel 21 der vorgeschlagenen Verordnung stehen Endnutzern die in den Artikeln 77 bis 79 der Datenschutz-Grundverordnung vorgesehenen Rechtsbehelfe zur Verfügung. Auf Artikel 80 der Datenschutz-Grundverordnung wird an dieser Stelle zwar nicht verwiesen, da die vorgeschlagene Verordnung jedoch die Datenschutz-Grundverordnung präzisiert und ergänzt, ist das in Artikel 80 der Datenschutz-Grundverordnung genannte Recht auf Endnutzer anwendbar, bei denen es sich um natürliche Personen handelt. Gemäß Erwägungsgrund 5 der vorgeschlagenen Verordnung führt diese zu keiner Absenkung des Schutzniveaus, das natürliche Personen nach der Datenschutz-Grundverordnung genießen. Dies könnte erforderlichenfalls in dem Rechtsakt klargestellt werden. Die Kommission wird sich weiterhin sorgfältig um die Kohärenz der genannten Instrumente bemühen.

Unter Verweis auf Artikel 21 Absatz 2 der vorgeschlagenen Verordnung bittet der Bundesrat die Kommission außerdem zu klären, inwieweit es erforderlich ist, natürlichen und juristischen Personen das Recht einzuräumen, rechtliche Schritte einzuleiten. Nach Artikel 13 Absatz 6 der Datenschutzrichtlinie für elektronische Kommunikation besteht dieses Recht bereits bei Verstößen gegen die nationalen Vorschriften in Bezug auf unerbetene Nachrichten. In der Praxis würde dies es Dienstleistern beispielsweise ermöglichen, rechtliche Schritte gegen die Absender von Direktwerbung einzuleiten, um die Interessen ihrer Kunden zu schützen[10]. Diese Regel wird durch Artikel 21 Absatz 2 der vorgeschlagenen Verordnung übernommen und auf die übrigen Bestimmungen der Verordnung ausgedehnt.

[10] Erwägungsgrund 68 der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (Text von Bedeutung für den EWR) (ABl. L 337 vom 18.12.2009, S. 11).