Deutscher Bundestag **Drucksache 18/12132**

18. Wahlperiode 26.04.2017

Entschließungsantrag

der Fraktion BÜNDNIS 90/DIE GRÜNEN

zu der dritten Beratung des Gesetzentwurfs der Bundesregierung
– Drucksachen 18/11325, 18/11655, 18/11822 Nr. 10, 18/12084 –

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Mit der rasch fortschreitenden Digitalisierung nahezu aller Lebensbereiche und dem Internet der Dinge gewinnt der Umgang mit persönlichen Informationen und Daten wirtschaftlich und politisch weiter an Bedeutung. Das hat nicht zuletzt die kontroverse Debatte um die datenschutzrechtlichen Regelungen bei der Einführung des automatisierten Fahrens durch die entsprechenden Änderungen des Straßenverkehrsgesetzes gezeigt. Das im Umgang und mit der Verarbeitung von persönlichen Informationen und Daten erzielbare Wissen wird zunehmend kommerzialisiert. Der steigende Wert der Daten wurde kürzlich mit der Novellierung des Wettbewerbsrechtes unterstrichen (§ 50c Neuntes Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen).

Im Bereich der Verwaltung wird sie u. a. für Entscheidungsprozesse aller Art herangezogen. Diese Entwicklung birgt gleichermaßen Chancen und Risiken. Dem Vertrauen der Bürgerinnen und Bürger in den Schutz ihrer Privatheit wird im Prozess der Digitalisierung wesentlich durch ein modernes Datenschutzrecht Rechnung getragen.

Die dem vorliegenden Gesetzentwurf zugrundeliegende 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) gilt vom 25. Mai 2018 an mit all ihren Regelungen in allen Mitgliedstaaten unmittelbar und wird Teil ihrer Rechtsordnung. Ihr gingen jahrelange Verhandlungen voran. Daneben erließ der europäische Gesetzgeber die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich Justiz und Polizei. Sie erweitert den Anwendungsbereich des europäischen Datenschutzrechts zum Zweck der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit gegenüber dem bisherigen Rahmenbeschluss 2008/977/JI. Der

freie Verkehr personenbezogener Daten zwischen den zuständigen Behörden von Polizei und Justiz soll erleichtert und dabei zugleich ein hohes Schutzniveau gewährleistet werden.

Der Deutsche Bundestag begrüßt die vorliegenden europäischen Reformwerke als einen notwendigen und überfälligen Schritt in der Weiterentwicklung des Privatheitsschutzes, der Verbraucherrechte und des Datenschutzes in Europa.

Mit dieser umfänglichen Reform wird das Datenschutzrecht weiter vereinheitlicht, durch harmonisierte Vorgaben der Binnenmarkt gestärkt und in wichtigen Punkten der Datenschutz modernisiert. Davon profitieren Verbraucher als auch Unternehmen. Unter den innovativen Vorgaben insbesondere hervorzuheben sind das Marktortprinzip, mit der der räumliche Anwendungsbereich auf Anbieter erstreckt wird, die Waren oder Dienstleistungen in der Europäischen Union an hier aufhältige Personen anbieten oder deren Datenverarbeitung der Beobachtung des Verhaltens von hier aufhältigen Personen dient. Von großer Bedeutung für die Weiterentwicklung des Datenschutzes sind etwa auch die Anforderungen an den Datenschutz durch Technikgestaltung und Voreinstellungen (Privacy by Design und Privacy by Default) sowie die neu geschaffene Datenschutz-Folgenabschätzung. Das deutlich verschärfte Sanktionsregime trägt der Realität des Umganges mit global agierenden verantwortlichen Unternehmen besser Rechnung. Der Deutsche Bundestag begrüßt ferner, dass das als effektiv geltende System der betrieblichen Datenschutzbeauftragten aufrechterhalten und fortgesetzt werden kann.

Beide Regelwerke erfordern konkretisierende nationale Umsetzungsvorgaben und Anpassungen in bereits vorhandenen Datenschutzbestimmungen. Denn sie enthalten eine nicht unbeträchtliche Anzahl an unbestimmten Rechtsbegriffen und Öffnungsklauseln und sind Ergebnis eines zum Teil hart errungenen politischen Kompromisses. Ziel der Anpassungen sollte es sein, sowohl die Bestimmungen der Grundrechte-Charta der Europäischen Union als auch die einschlägigen Artikel des Grundgesetzes zu verwirklichen und zugleich ein hohes, einheitliches Datenschutzniveau in der EU zu gewährleisten. Einheitliche europäische Standards für die Datennutzung geben sowohl den Verbraucherinnen und Verbrauchern wie auch den Unternehmen Rechts- und Planungssicherheit. Die in der Datenschutz-Grundverordnung verankerten Öffnungsklauseln für die Mitgliedstaaten dürfen daher nicht genutzt werden, um die europäischen Standards mit nationalen Umsetzungsgesetzen zu unterbieten.

Der vorliegende Gesetzentwurf der Bundesregierungen erfüllt diese Anforderungen jedoch nicht. Die Bundesregierung schlägt stattdessen Regelungen vor, mit denen Deutschland vom europäischen Datenschutzniveau abweicht. Anstatt die Grundsätze des Datenschutzes – Einwilligungsvorbehalt, Zweckbindung und Datensparsamkeit – konsequent umzusetzen, schränkt die Bundesregierung ausgerechnet die Betroffenenrechte gegenüber der europäischen Datenschutzgrundverordnung ein und fällt damit hinter das europäische Schutzniveau zurück. Damit wären deutsche Verbraucherinnen und Verbraucher datenschutzrechtlich schlechter gestellt als Verbraucherinnen und Verbraucher in anderen EU-Mitgliedstaaten. So sind Einschränkungen der Informationspflichten vorgesehen, obwohl die EU-Datenschutzverordnung hier keine nationalen Öffnungsklauseln vorsieht. Ebenso soll das Recht auf Löschung in bestimmten Fällen wegen hohen Aufwands eingeschränkt werden, ohne dass die europäische Grundverordnung hierfür eine Ermächtigung vorsieht. Anders als bisher soll zudem die Möglichkeit automatisierter Entscheidungen ausgeweitet werden, so dass zukünftig private Krankenkassen bei Erstattungsanträgen automatische Ablehnungen verschicken können, ohne dass diese vorher durch einen Sachbearbeiter überprüft werden, wie es derzeit der Fall ist.

Der Bundesrat hat daher in seiner Stellungnahme zum vorliegenden Gesetzentwurf (mit Gegenäußerung der Bundesregierung, vgl. Bundestagsdrucksache 18/11655) umfängliche Änderungsvorschläge vorgelegt.

Der Deutsche Bundestag begrüßt die ausführlichen und konstruktiven Vorschläge des Bundesrates für verordnungskonforme Verbesserungen des vorgelegten Gesetzentwurfes, welche u. a. zahlreiche Vorschläge der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgreifen und konkretisieren. Er teilt das Bedauern des Bundesrates, der zu Recht darauf hinweist, dass ihm eine umfassende sachbezogene Bewertung der vorgeschlagenen Neuerungen schon deshalb nicht möglich erscheint, weil weitere umfängliche, in Arbeit befindliche Anpassungen des von den EU-Vorgaben mitbetroffenen Fachrechts bislang weder dem Bundesrat noch dem Bundestag vorliegen.

Der Innenausschuss des Deutschen Bundestages hat am 27. März 2017 in einer Sachverständigenanhörung zahlreiche weitere Vorschläge und Hinweise für Änderungen des vorliegenden Gesetzentwurfes erhalten. Der Deutsche Bundestag bedauert, dass ein gemeinsamer Änderungsantrag von CDU/CSU und SPD-Fraktion erst am Morgen der Anhörung vorlag (A-Drs. 18(4)842) und damit von den Sachverständigen nicht mehr angemessen berücksichtigt werden konnte.

Insgesamt vertritt der Deutsche Bundestag die Auffassung, dass hohe Datenschutzstandards und IT-Sicherheit einen internationalen Wettbewerbsvorteil für Deutschland im digitalen Zeitalter darstellen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. bei der Umsetzung und Anpassung an die EU-Vorgaben verbliebene Spielräume zurückhaltend und im Sinne des Datenschutzes zu nutzen, nationale Alleingänge weitestgehend zu vermeiden und der Datenschutzgrundverordnung als Vollharmonisierung mit Anwendungsvorrang angemessen Rechnung zu tragen;
2. bei den Rechten der Betroffenen, darunter den Informationspflichten der verantwortlichen Stellen, den Auskunfts- und Löschungsrechten der Betroffenen europarechtskonforme Umsetzungen vorzunehmen und schutzverkürzende Anpassungen unbedingt zu vermeiden;
3. bei den das Profiling und Scoring betreffenden, insgesamt die Zukunft eines datenschutz- und verbraucherrechtskonformen Big Data betreffenden maßgeblichen Bestimmungen weitere zivilrechtliche Vorgaben im materiellen Verbraucherschutzrecht vorzusehen, um Ausgrenzungen und Benachteiligungen ganzer Personengruppen zu vermeiden und zusätzliche verbraucherschützende Regeln für Bewertungen von Personen sicherzustellen;
4. Einschränkungen der Befugnisse der Aufsichtsbehörden gegenüber Berufsgeheimnisträgern und Amtsträgern präzise auf die den Geheimnisschutz unmittelbar betreffenden Bereiche zu begrenzen, damit effektive Prüfungen der Einhaltung des Datenschutzes in Krankenhäusern, bei privaten Krankenversicherungen, Apotheken, Anwalts- und Steuerberatern usw. weiterhin möglich bleiben;
5. Regelungen vorzulegen mit dem Ziel, dass die Datenschutzbehörden im Vorfeld von Zusammenschlussentscheidungen vom Bundeskartellamt konsultiert werden. Ihre Stellungnahme soll vom Kartellamt bei der Entscheidung berücksichtig werden;
6. die bereits mit dem sog. Videoüberwachungsverbesserungsgesetz (Bundestagsdrucksache 18/10941) eingebrachte Indienstnahme privater Videoüberwachungen für öffentliche Interessen zurückzunehmen bzw. lediglich die bisherige Regelung verordnungskonform anzupassen;
7. sich auf europäischer Ebene für harmonisierte Regelungen des Beschäftigtendatenschutzes einzusetzen und davon unabhängig bereits

8. ein eigenständiges Beschäftigtendatenschutzgesetz vorzulegen, in welchem der Umgang mit Beschäftigtendaten umfassend geregelt wird, der Ausgestaltungsspielraum beim Beschäftigtendatenschutz besser genutzt wird und dabei insbesondere
   a) die Anforderungen an die Datenverarbeitungsgrundsätze im Beschäftigtenkontext zu konkretisieren, indem technische und organisatorische Maßnahmen zur Vermeidung von Beschäftigten-Profilings getroffen werden,
   b) klargestellt wird, dass es ein umfassendes Mitbestimmungsrecht für betriebliche Interessenvertretungen beim Datenschutz gibt,
   c) klarstellt, dass auch bestimmte nichtautomatisierte Informationsverarbeitungen wie etwa Regelungen zum Fragerecht der Arbeitgeber ebenfalls vom Anwendungsbereich des Datenschutzrechts umfasst sind,
   d) beim Beschäftigungsbegriff auch Werkvertragsbeschäftigte miteinbezogen werden und
   e) der Videoüberwachung von Beschäftigten in öffentlich zugänglichen Räumen klare Grenzen gesetzt werden. Es wird dafür gesorgt, dass Beschäftigte bei der Videoüberwachung möglichst nicht erfasst werden (§26 Abs.8);
9. die Befugnisse der BfDI im Bereich der JI-Richtlinie europarechtskonform so anzupassen, dass diese über bloße Beanstandungen hinausgehend verbindliche Anordnungen gegen rechtswidrig handelnde Behörden aussprechen kann,
10. die Befugnisse der BfDI dahingehend anzupassen, dass diese gegenüber einer Behörde oder deren Rechtsträger, etwa zur Beseitigung von Sicherheitslücken, die sofortige Vollziehung anordnen kann;
11. auf verkürzende Regelungen zur Zweckbindung wie in § 49 BDSG-neu zu verzichten und die Anforderungen an die Zulässigkeit von Zweckänderungen hinreichend differenziert in den Fachgesetzen vorzunehmen;
12. bei den Anforderungen an die Sicherheit der Datenverarbeitung von fachlich veralteten, die IT-Sicherheit schwächenden Vorgaben abzusehen und stattdessen zeitgemäße, den technischen Möglichkeiten Rechnung tragende Begrifflichkeiten und Konzepte aufzugreifen;
13. die Regelung zur allgemeinen Verwendbarkeit von Protokolldaten in Strafverfahren zu streichen;
14. die Zutrittsberechtigung der BfDI im Rahmen von Kontrollen nicht hinsichtlich der Räumlichkeiten und Räume zu beschränken, die gemeinsam mit oder ausschließlich durch einen Nachrichtendienst eines Drittstaates auf deutschem Boden genutzt werden;
15. die Möglichkeit der BfDI, sämtlichen Ausschüssen des Deutschen Bundestages über ihre Prüfungstätigkeit berichten zu dürfen, nicht zu beschränken.

Berlin, den 25 .April 2017

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

Begründung

Zu. 1:
Zwar enthält auch die jetzt vorliegende Datenschutzgrundverordnung noch eine Vielzahl von unbestimmten Rechtsbegriffen und auch Öffnungsklauseln. Diese sollten jedoch nicht dazu genutzt werden, um die zentrale Funktion der Verordnung als Vollharmonisierung zu hintertreiben. Rechtsprechung und Aufsichtspraxis werden hinsichtlich bestehender Unsicherheiten der Auslegung Lücken schließen. Anstatt hinter den europäischen Vorgaben zu bleiben, sollte die Bundesregierung sich auf europäischer und internationaler Ebene dafür einsetzen, datenschutzrechtliche Standards in internationalen Handelsabkommen fest zu verankern.

Zu 2.
Entgegen den europäischen Vorgaben, die allenfalls geringfügige nationale Spielräume beließen, hat die Bundesregierung in den Vorentwürfen und auch im jetzt vorliegenden Gesetzentwurf ausgerechnet bei den Betroffenenrechten schutzverkürzend eingegriffen, beispielsweise durch die Einschränkung der Informationsrechte sowie des Rechts auf Löschen. Das ist mit Blick auf deren Funktion aus Bedingungen der Grundrechtsausübung und Mindestvoraussetzungen der Transparenz für immer komplexer werdende Datenverarbeitungsvorgänge nicht sachgerecht und zudem in der EU-Datenschutzgrundverordnung nicht durch entsprechende Öffnungsklauseln abgedeckt. Durch diese Einschränkungen werden deutsche Verbraucherinnen und Verbraucher gegenüber anderen europäischen Verbrauchern benachteiligt. Ein einheitliches europäisches Schutzniveau war aber nicht nur Ziel der europäischen Datenschutzgrundverordnung, sondern ist auch von Vorteil für die Unternehmen.

Zu 3.
Die zentralen Gerechtigkeitsfragen der zur Zeit auf den Markt kommenden oder bereits im Einsatz befindlichen Big Data und Profilingmethoden bedürfen zusätzlicher konkreter Regelungen im Fachrecht, weil nur aus dem jeweiligen konkreten Anwendungsbereich, dem Zweck und der einsetzenden Wirtschaftsbranche die notwendige Risikoabwägung erfolgen kann. Daher erscheint der Vorschlag insbesondere der Verbraucherzentrale Bundesverband vom 23. Februar 2017 (vgl. dazu auch die Dokumentation der Anhörung des Innenausschusses des Deutschen Bundestages) problemangemessen, neben den Regelungen der EU-Datenschutzgrundverordnung auch im zukünftigen nationalen Fachrecht konkretisierende verbraucherrechtliche Bestimmungen zu treffen. Denn ein modernes Datenschutzrecht muss Grundlage sein, automatisierte Diskriminierung zu verhindern.

Zu 4.
Im Bereich der großen Anzahl von Berufsgeheimnisträgern darf es keinesfalls zu pauschalisierenden Einschränkungen der Kontrollbefugnisse der Datenschutzaufsichtsbehörden kommen. Damit entstünden weitgehend kontrollfreie Räume ausgerechnet in so informationssensiblen Bereichen wie Krankenhäusern sowie dem Gesundheitssystem insgesamt. Solche Verkürzungen der Aufsichtsrechte sind auch mit der besonderen und gewachsenen Rolle der Datenschutzaufsicht als grundrechtliches Schutzelement des Datenschutzes nicht vereinbar.

Zu 5.
Die vielfältigen und von zahlreichen Verbänden wie dem Deutschen Richterbund geäußerten Zweifel an der Verfassungsmäßigkeit der nunmehr verschärften Regelung der Videoüberwachung privater Stellen bedürfen weiterhin der Berücksichtigung. Der Durchgriff auf und die Indienstnahme Privater für öffentliche Überwachungszwecke ist unzulässig.

Zu 6.
Die seit annähernd 20 Jahren kontrovers diskutierte Schaffung eines europäischen Beschäftigtendatenschutzes, mit dem die besonderen Risiken Beschäftigter im Über-Unterordnungsverhältnis in informationeller Hinsicht aufgegriffen werden könnten, braucht die entschiedene Unterstützung der Bundesregierung. Eine europäische Regelung würde angesichts des hohen Grades wirtschaftlicher Verflechtungen von Betriebsstrukturen den effektiveren Ansatz bieten.

Zu 7:
Soweit und solange eine europäische Lösung nicht erreichbar erscheint, sollte das in der 17. Wahlperiode am Widerstand von FDP und Wirtschaftsverbänden gescheiterte Vorhaben eines nationalen Beschäftigtendatenschutzgesetzes wieder aufgegriffen werden. Dabei sind neben zahlreichen weiteren Problemfeldern insbesondere die unter a. bis e. angeführten, erhebliche Risiken für die Beschäftigten bildenden Probleme und Vorgehensweisen gesetzlich zu regulieren. Der europäische Gesetzgeber hat in Anerkennung der nationalen Unterschiede eine entsprechend weite Öffnungsklausel bereitgestellt.

Zu 8:
Die Erweiterung der Sanktionsmöglichkeiten der Bundesbeauftragten ist europarechtlich geboten und wird entsprechend seit Jahren auch auf nationaler Ebene gefordert, um auch im Bereich der Behörden eindeutig als rechtswidrig festgestellte Praktiken, so etwa im Bereich der besonders und wiederholt auffällig gewordenen Geheimdienste, abstellen zu können.

Zu 9:
Die Bundesbeauftragte für Datenschutz weist zu Recht in ihrer Stellungnahme darauf hin, dass für die von ihr verfügbaren Verwaltungsanordnungen auch die Möglichkeit sofortiger Vollziehung bestehen muss, um etwa in Fällen der Gefahr im Verzug, etwa bei offenkundigen und rechtswidrigen Sicherheitslücken, entsprechend umgehend auf das Abstellen der rechtswidrigen Praxis hinwirken zu können.

Zu 10:
Die pauschalisierenden Regelungen des „§ 49 neu“ entsprechen einer fehlgeleiteten Umsetzung der JI-Richtlinie, bei der zum Teil im Wortlaut gleiche Formulierungen übernommen werden, ohne die bisherige nationale Rechtslage der konkreten Regelung von Zweckänderungen im jeweiligen Fachrecht zu berücksichtigen. Damit entstehen vermeidbare neue Auslegungswidersprüche und Unklarheiten.

Zu 11:
Die Forderung entspricht langjährigen Forderungen bereits der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, wonach die Konzeption der IT-Sicherheit im Datenschutzrecht methodisch-konzeptionell als auch begrifflich modernisiert werden muss.

Zu 12:
Eine pauschalisierende Verwendbarkeit von Protokolldaten für Strafverfolgungszwecke ist mit den ausnahmsweise bestehenden Zugriffsmöglichkeiten auf die ansonsten strikt zweckgebundenen Protokollierungsdateien nicht vereinbar und unverhältnismäßig.

Zu 13:
Offenbar versucht die Bundesregierung einmal mehr im Geheimdienstbereich, ihre rechtswidrige Praxis der Unterbindung des Zutritts von Räumlichkeiten der NSA durch die Bundesbeauftragte für Datenschutz (in Bad Aibling) im Nachhinein zu legalisieren. Diese Beschränkung der Rechte oberster Bundesorgane bei der Ausübung ihrer Kontrolltätigkeit auf deutschem Boden gegenüber „Mächten fremder Staaten“ ist völlig inakzeptabel und zurückzunehmen.

Zu 14:
Wie bei o. g. Nr. 13. versucht auch hier die Bundesregierung, eine im Rahmen der Snowden-Enthüllungen für sie äußerst peinlich verlaufene Unterrichtung des Deutschen Bundestages bzw. des 1. Untersuchungsausschusses durch die Bundesbeauftragte für den Datenschutz von einer Prüfung in einer BND-Außenstelle durch das Verbot der Unterrichtung zukünftig unmöglich zu machen. Dieser Vorstoß beschränkt die Parlamentsrechte in völlig unangemessener Weise mit dem Ziel, die ohnehin rechtsstaatlich hochproblematische, umfassende Geheimhaltung geheimdienstlicher Arbeit weiter zu verstärken und damit eine effektive, verfassungsrechtlich gebotene Kontrolle durch Demokratie und Öffentlichkeit zu verhindern.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
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 0722-8333