



Prof. Dr. Aden, HWR Berlin • Alt-Friedrichsfelde 60 • 10315 Berlin

An den  
Innenausschuss des  
Deutschen Bundestages

Per E-Mail an: [innenausschuss@bundestag.de](mailto:innenausschuss@bundestag.de)

Datum: 25. März 2017

**Stellungnahme zum  
Gesetzentwurf der Bundesregierung:  
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), BT-Drucksache 18/11325,  
vorgelegt zur Anhörung des Innenausschusses des Deutschen  
Bundestags am 27. März 2017 in Berlin**

**Prof. Dr. Hartmut Aden**  
Fachbereich 5  
Polizei und  
Sicherheitsmanagement  
Professur für Öffentliches Recht,  
Europarecht, Politik- und  
Verwaltungswissenschaft

Stv. Direktor, Forschungsinstitut  
für Öffentliche und Private  
Sicherheit (FÖPS Berlin)

Behördlicher  
Datenschutzbeauftragter der  
HWR Berlin

Alt-Friedrichsfelde 60  
D-10315 Berlin  
T +49 (0)30 30877-2868

privat:  
Postfach 580601  
D-10415 Berlin

E-Mail: [Hartmut.Aden@hwr-berlin.de](mailto:Hartmut.Aden@hwr-berlin.de)

[www.hwr-berlin.de/prof/hartmut-aden](http://www.hwr-berlin.de/prof/hartmut-aden)

[www.foeps-berlin.org](http://www.foeps-berlin.org)

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur Mitwirkung an der Anhörung. Meine Stellungnahme beschränkt sich absprachegemäß auf die Umsetzung 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 [...]*.

Bedauerlicherweise hat diese Richtlinie in der öffentlichen Wahrnehmung seit der gemeinsamen Einbringung der Entwürfe durch die Europäische Kommission Anfang 2012 zumeist im Schatten der Datenschutzgrundverordnung gestanden. Dies ist insbesondere angesichts der hohen praktischen Relevanz zu bedauern, die der Datenaustausch zwischen Sicherheitsbehörden seit den 1990er Jahren und verstärkt im Zusammenhang mit der Terrorismusbekämpfung der letzten Jahre erlangt hat.

Das Datenschutzrecht für die polizeiliche Zusammenarbeit in der Europäischen Union entsprach bisher weder dem Stand der Zusammenarbeitspraxis noch der technischen Entwicklung. Der jetzt abzulösende Rahmenbeschluss stammt noch aus der ehemaligen „Dritten Säule“, also der



reinen Regierungszusammenarbeit. Die Technik der Datenverarbeitung und die Praxis der Zusammenarbeit zwischen den hier relevanten Behörden der Mitgliedstaaten (Polizei u. a.) haben sich in den letzten Jahren erheblich weiterentwickelt. Der transnationale Informationsaustausch hat sich in Zeiten gestiegener Risiken und Gefahren für die Sicherheit zu einem zentralen Instrument entwickelt. Die ausgeweitete Praxis ist aber auch mit Risiken für die Grundrechte der Bevölkerung verbunden, insbesondere für die informationelle Selbstbestimmung und die daran anknüpfenden Grundrechte im Strafverfahren (Unschuldsvermutung; Schutz vor willkürlichen Freiheitsentziehungen etc.). Diese Grundrechtspositionen lassen sich nur durch rigorose Maßnahmen zur Gewährleistung der Qualität der hier verarbeiteten personenbezogenen Daten schützen, die Fehlinformationen, Verwechslungen oder unberechtigte Datenverarbeitung verhindern. Solche Maßnahmen liegen zugleich im Interesse der Sicherheitsbehörden selbst, da Reibungsverluste durch veraltete oder unrichtige Daten so vermieden werden können.<sup>1</sup> Daher ist die Harmonisierung durch die Richtlinie (EU) 2016/680 ein wichtiger Schritt.

Zu ausgewählten Aspekten des Entwurfs für die Umsetzung dieser Richtlinie nehme ich im Folgenden Stellung. Der vorliegende Gesetzentwurf wirft konzeptionelle Fragen für eine adäquate, in der Praxis handhabbare Umsetzung der Richtlinienvorgaben auf (A). Er spiegelt verbliebene Unzulänglichkeiten der Richtlinie selbst wider (B), enthält aber auch diverse Mängel und nicht ausgeschöpfte Regelungspotentiale, die der Deutsche Bundestag im Rahmen des Umsetzungsspielraums noch korrigieren kann (C).

### **A) Konzeptionelle Problematik der Richtlinienumsetzung in das deutsche Recht**

Problematisch ist bereits die für die Richtlinienumsetzung vorgeschlagene Systematik. Statt ein anwendungsfreundliches Datenschutzgesetz „aus einem Guss“ zu schaffen, trennt der vorliegende Gesetzentwurf die

---

<sup>1</sup> Näher hierzu: Aden, Hartmut (2014) *Koordination und Koordinationsprobleme im ambivalenten Nebeneinander: Der polizeiliche Informationsaustausch im EU-Mehrebenensystem*, in: Der moderne Staat, Zeitschrift für Public Policy, Recht und Management (7. Jg., Nr. 1), S. 55-73; ders. (2015) *Police information sharing and data protection in the European Union before and after the Treaty of Lisbon*, in: Hartmut Aden (Hrsg.), *Police Cooperation in the European Union under the Treaty of Lisbon – Opportunities and Limitations*, Baden-Baden (Nomos, Schriftenreihe des Arbeitskreises Europäische Integration, Band 83), S. 209-216.



Anpassung des deutschen Rechts an die Datenschutzgrundverordnung ganz unnötig von der Umsetzung der Richtlinie 2016/680. Gesetzgebungstechnisch ungewöhnlich schlägt der Entwurf damit „zwei Gesetze in einem“ vor. Indes verfolgte das Anfang 2012 von der Europäischen Kommission vorgelegte EU-„Datenschutzpaket“ die Intention, einen Datenschutz „aus einem Guss“ zu schaffen. Die Trennung in Richtlinie und Verordnung sollte lediglich den Mitgliedstaaten etwas größere Gestaltungsspielräume für das Datenschutzrecht im Polizei- und Strafverfolgungsbereich überlassen.

- Der vorliegende Entwurf spiegelt dagegen eher die Zuständigkeitsverteilung für die beiden EU-Rechtsakte in einer arbeitsteilig organisierten Ministerialverwaltung wider als eine ambitionierte, an der Schaffung systematischer Rechtsgrundlagen orientierte Gesetzgebung. Chancen für die Schaffung eines einheitlichen, benutzerfreundlichen Datenschutzrechts werden damit vertan. Wesentlich sinnvoller erschiene es, allgemeine Fragen wie Definitionen und Grundsätze in einem gemeinsamen allgemeinen Teil voranzustellen und sodann in einem besonderen Teil zunächst die Anpassung an die Datenschutzgrundverordnung und sodann die Umsetzung der Richtlinie vorzunehmen. Trotz des Nebeneinanders unmittelbar geltender Verordnungsinhalte und umsetzungsbedürftiger Richtlinienvorgaben ist eine Vereinheitlichung der Begrifflichkeiten und allgemeiner Prinzipien im Interesse kohärenter Rechtsanwendung sinnvoll. Dies betrifft zumindest die §§ 45 bis 47 der Entwurfsfassung. Nur so bleibt das Gesetz in der Praxis handhabbar, insbesondere auch für Polizeibedienstete auf Sachbearbeiterebene.<sup>2</sup>

**Empfehlung:** *Der Deutsche Bundestag sollte die allgemeinen Datenschutzgrundlagen aus der Richtlinie (insbesondere §§ 45 bis 47 des Entwurfs) mit Teil 1, Kapitel 1 (§ 1 bis 2) zu einem kohärenten „allgemeinen Teil“ des Gesetzes zusammenführen.*

---

<sup>2</sup> Zur Überforderung der Polizeipraxis durch überkomplizierte rechtliche Grundlagen: Aden, Hartmut (2013), *Polizei und das Recht: Stressquelle oder Stressvermeidung?*, in: Rainer Prätorius & Lena Lehmann (Hrsg.), *Polizei unter Stress?*, Frankfurt/Main: Verlag für Polizeiwissenschaft, S. 15-34.



## **B) Defizite in der EU-Richtlinie und Korrekturmöglichkeiten im Rahmen der deutschen Gesetzgebung**

Einige Defizite des vorliegenden Gesetzentwurfs sind bereits in der Richtlinie (EU) 2016/680 angelegt. Da es sich um eine Richtlinie handelt, kann der Deutsche Bundestag diese Defizite jedenfalls teilweise durch eigene gesetzgeberische Impulse kompensieren. Zwei dieser Defizite seien hier exemplarisch hervorgehoben.

### **1. Fehlende Anwendbarkeit für die EU-Agenturen und ihre Zusammenarbeit mit den mitgliedstaatlichen Behörden**

Gemäß Art. 2 Abs. 2 der RL (EU) 2016/680 bezieht sich ihr Anwendungsbereich nicht auf die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union. Damit sind auch die für Sicherheitsfragen eingerichteten EU-Agenturen (insbesondere Europol, Frontex, eu-LISA, CEPOL) nicht erfasst. Dies ist vor dem Hintergrund der ursprünglichen Absicht, einen einheitlichen Datenschutzrahmen in der EU zu schaffen, inkonsequent – und angesichts einer bisher für jede Agentur unterschiedliche Datenschutzarchitektur<sup>3</sup> bedauerlich. Hier wird die EU-Gesetzgebung in einem weiteren Gesetzgebungsschritt für mehr Kohärenz und einheitlich höhere Schutzstandards sorgen müssen.

Dies hindert indes den Deutschen Bundestag nicht daran, bereits jetzt einheitliche (Mindest-)Standards für den Datenaustausch der Sicherheitsbehörden des Bundes mit EU-Agenturen „vor die Klammer zu ziehen“.

### **2. Verweis auf mitgliedstaatliche Gesetze: zu viele „Hintertüren“ für die Datenverarbeitungspraxis**

Die Richtlinie verfolgt die regulatorische Grundlinie, dass die Datenverarbeitung von Sicherheitsbehörden durch rechtliche Grundlagen legitimiert werden kann und muss. Dieser regulatorische Ansatz ist als solcher nicht zu beanstanden und angesichts der hohen Bedeutung der Ressource Information für Sicherheitsbehörden kaum vermeidlich. Erforderlich wären dagegen klarere materiell-rechtliche Grenzen für die Datenerhebung und -verarbeitung. Diese müssen nun von der mitgliedstaatlichen Gesetzgebung etabliert werden – die Richtlinie enthält zahlreiche Verweisungen

---

<sup>3</sup> Näher hierzu Aden, Hartmut (2014) *Koordination und Koordinationsprobleme im ambivalenten Nebeneinander: Der polizeiliche Informationsaustausch im EU-Mehrebenensystem*, a.a.O.



auf mitgliedstaatliche Gesetze. Auch für das deutsche Recht gibt es hier noch erheblichen Entwicklungsbedarf. Der vorliegende Gesetzentwurf liefert hierfür leider keine über die Mindestvorgaben der Richtlinie hinausgehenden Ansätze.

### **C) Nachbesserungsmöglichkeiten des Deutschen Bundestags für die Richtlinienumsetzung**

Der Deutsche Bundestag hat im Gesetzgebungsverfahren die Chance, eine Reihe konkreter Verbesserungen an dem vorliegenden Entwurf vorzunehmen. Einige hiervon seien exemplarisch aufgeführt.

#### **1. Nicht nur den Richtlinientext abschreiben, sondern die Umsetzung in die deutsche Rechtssystematik gewährleisten**

Der vorliegende Entwurf orientiert sich bis in Detailformulierungen hinein stark am Text der Richtlinie. Dies entspricht einer bedauerlichen Tendenz, die auch auf anderen Rechtsgebieten zu beobachten ist: Aus Sorge vor Interpretationsstreitigkeiten, eventuellen Vertragsverletzungsverfahren und manchmal auch vor einer über die EU-Vorgaben hinausgehenden Umsetzung werden Richtlinieninhalte wörtlich in die Umsetzungsgesetzgebung übernommen. Dabei ist es gerade der Sinn einer Richtlinie gemäß Art. 288 AEUV, den Mitgliedstaaten die Einpassung in ihre spezifische Rechtssystematik und –terminologie zu ermöglichen.

Beispiel: In Art. 3 Abs. 1c der RL (EU) 2016/680 heißt es: „Die Mitgliedstaaten sehen vor, dass personenbezogene Daten dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind.“ Diese sprachlich missglückte Formulierung der offiziellen deutschsprachigen Richtlinienfassung wurde einfach in den vorliegenden Entwurf hineinkopiert. In § 47 Nr. 3 des Entwurfs heißt es: Personenbezogene Daten müssen „dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein.“ In der deutschen Rechtssystematik müsste eine für die Rechtsanwendung in den Sicherheitsbehörden ohne Weiteres verständliche Formulierung dagegen ungefähr wie folgt lauten: Personenbezogene Daten „dürfen nur verarbeitet werden, soweit diese Verarbeitung für das Erreichen des Verarbeitungszwecks (zwingend) erforderlich ist und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck steht.“



Dieses Beispiel zeigt, dass der gesamte Entwurf noch einmal gründlich bezüglich seiner Übereinstimmung mit der deutschen Rechtssystematik und –terminologie überprüft werden sollte.

**Empfehlung:** *Der Deutsche Bundestag sollte die wörtlich aus der deutschsprachigen Richtlinienfassung übernommenen Formulierungen des Gesetzentwurfs einer gründlichen Überprüfung auf ihre Vereinbarkeit mit der deutschen Rechtssystematik und –terminologie unterziehen.*

## **2. Zweckänderungsvorschrift (§ 49) nicht mit dem Bestimmtheitsgebot vereinbar**

Die Zweckbindung folgt unmittelbar aus dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und auf Schutz personenbezogener Daten (Art. 8 EU-Grundrechte-Charta). Sie ist damit ein zentraler Grundsatz für die Datenverarbeitung in Deutschland und in der EU, auch und gerade für den Sicherheitsbereich. Sicherheitsbehörden können für einen bestimmten Zweck erhobene Daten nicht nach Belieben für andere Zwecke verwenden. Zweckänderungen stellen vielmehr erneute Grundrechtseingriffe dar und bedürfen daher einer klaren gesetzlichen Grundlage. Art. 9 der RL (EU) 2016/680 regelt dies den üblichen Standards entsprechend.

Die Umsetzung in § 49 des Entwurfs genügt nicht den Anforderungen des grundgesetzlichen Bestimmtheitsgebots. Der pauschale Verweis in § 49 Satz 1 (Entwurfassung) auf die in § 45 genannten „Zwecke“ ist viel zu allgemein und unbestimmt. Denn dort sind die nur sehr allgemein genannten Zwecke „Verhütung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten“ genannt. Die neue Regelung würde es ermöglichen, im Rahmen des Verhältnismäßigen vorhandene Datenbestände zwischen diesen verschiedenen Aufgabenbereichen und Zweckbestimmungen hin- und herzuschieben. Eine solche Zweckänderungsgeneralklausel fiel sogar erheblich hinter den heutigen Stand der spezialgesetzlichen Zweckänderungsvorschriften in der Strafprozessordnung, den Polizeigesetzen und anderen Fachgesetzen zurück. Das Bestimmtheitsgebot erfordert vielmehr spezialgesetzliche Zweckänderungsregelungen. Im Hinblick auf das Wesentlichkeitsprinzip für gravierende Grundrechtseingriffe können diese nur in anderen Parlamentsgesetzen erlassen werden. Das neue Bundesdatenschutzgesetz sollte ausschließlich auf diese verweisen.



**Empfehlung:** *Der Deutsche Bundestag sollte die Entwurfsfassung des § 49 durch einen Verweis auf spezialgesetzliche, vom Parlament zu erlassene Regelungen ersetzen, in denen die Zwecke, zu denen Daten ebenfalls verarbeitet werden dürfen, im Sinne des Bestimmtheitsgebots präzise zu benennen sind.*

### **3. Besonders sensible Daten:**

Die Verarbeitung besonders sensibler personenbezogener Daten stellt für die Betroffenen einen schweren Grundrechtseingriff dar: Informationen zur rassischen und ethnischen Herkunft, zu religiösen oder weltanschaulichen Überzeugungen, genetische und biometrische Daten sowie Informationen zur Gesundheit oder zum Sexualleben dürfen daher auch von Sicherheitsbehörden nur ausnahmsweise und mit besonderer Vorsicht verarbeitet werden. Art. 10 der RL (EU) 2016/680 erkennt an, dass dieser Ausnahmeharakter auch einer besonderen rechtlichen Absicherung bedarf.

Die vorgeschlagene Umsetzungsregelung in § 48 des Entwurfs könnte so interpretiert werden, dass eine Verarbeitung solcher Daten bereits dann zulässig ist, wenn die dort genannten Voraussetzungen und nur beispielhaft aufgeführten Verfahrensvorkehrungen getroffen werden. Dies würde indes der Schwere des Grundrechtseingriffs durch die Verarbeitung derartiger Daten nicht gerecht. Vielmehr sind im Hinblick auf das grundgesetzliche Bestimmtheitsgebot die Zwecke, für die solche Daten ausnahmsweise erhoben und weiter verarbeitet werden dürfen, in den Fachgesetzen konkret darzulegen. Wegen der Eingriffsintensität erfordert das Wesentlichkeitsprinzip auch hier parlamentsgesetzliche Regelungen.

**Empfehlung:** *Der Deutsche Bundestag sollte klarstellen, dass die Verarbeitung besonders sensibler Daten (Art. 10 der RL (EU) 2016/680) nur zulässig ist, wenn der konkrete Zweck in einem Parlamentsgesetz (Fachgesetz) zugelassen ist.*

### **4. Auskunftsrechte: Rechte der Betroffenen klarer sichern**

Die Auskunftsrechte der betroffenen Personen sind in Art. 14 und 15 der RL (EU) 2016/680 geregelt und in Deutschland zusätzlich durch das Grundrecht auf informationelle Selbstbestimmung geschützt. Art. 15 ermöglicht zwar Einschränkungen des Auskunftsrechts. Diese sind aber im Lichte der grundrechtlichen Verbürgungen auszugestalten.



In § 57 Abs. 7 der Entwurfsfassung wird eine Konstruktion gewählt, in der die oder der Bundesdatenschutzbeauftragte in Fällen der Auskunftsverweigerung die mit der Auskunftserteilung verbundene Kontrolle bezüglich der Korrektheit der Daten und der Rechtmäßigkeit der Verarbeitung für die Betroffenen wahrnimmt. Diese Konstruktion ist grundsätzlich geeignet, das Spannungsverhältnis zwischen berechtigten Auskunfts- und Kontrollbegehren der Betroffenen und in manchen Fällen berechtigten Geheimhaltungsanliegen der Sicherheitsbehörden aufzulösen. Die Ausnahmeklausel, nach der diese Stellvertretung im Einzelfall durch die zuständige oberste Bundesbehörde wegen Gefährdung „der Sicherheit des Bundes oder eines Landes“ verweigert werden kann (Abs. 7 Satz 3), ist dagegen nicht mit dem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vereinbar. Denn die oder der Bundesbeauftragte verfügt über genügend vertrauenswürdige und sicherheitsüberprüftes Personal, um diese Aufgabe auch in solchen besonderen Fällen zuverlässig zu erfüllen. Die Ausnahmeklausel ist daher verfassungsrechtlich nicht gerechtfertigt. Auch in dem hier maßgeblichen Art. 17 der RL (EU) 2016/680 ist eine solche Ausnahme nicht vorgesehen, so dass die Umsetzung insofern auch nicht den Anforderungen des EU-Rechts genügt.

Darüber hinaus böte es sich an, dass der Deutsche Bundestag die Rechte der Betroffenen dadurch stärkt, dass die oder der Bundesdatenschutzbeauftragte für diese und andere Fälle ein Klagerecht gegen aus ihrer Sicht rechtswidrige Behördenentscheidungen erhält.

**Empfehlung:** *Der Deutsche Bundestag sollte die Sicherheitsklausel aus § 57 Abs. 7 Satz 3 des Entwurfs streichen und der oder dem Bundesdatenschutzbeauftragten zudem ein Klagerecht zur Durchsetzung von Betroffenenrechten einräumen.*

**Fazit:** Ich empfehle dem Deutschen Bundestag, den Entwurf nur nach gründlicher Überarbeitung zu verabschieden.

Gez. Prof. Dr. Hartmut Aden