



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

An den
Ausschuss für „Inneres und Heimat“ des
Deutschen Bundestages

Per E-Mail an: innenausschuss@bundestag.de

Datum: 08. Dezember 2018

**Stellungnahme zum
Gesetzentwurf der Bundesregierung:
Entwurf eines Zweiten Gesetzes zur Anpassung des
Datenschutzrechts an die Verordnung (EU) 2016/679 und zur
Umsetzung der Richtlinie (EU) 2016/680
(Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU –
2. DSAnpUG-EU), Bundestags-Drucksache 19/4674,
vorgelegt zur Anhörung des Ausschusses für „Inneres und Heimat“
des Deutschen Bundestags am 10. Dezember 2018 in Berlin**

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur Mitwirkung an der Anhörung. Wegen des großen Umfangs des Gesetzentwurfs beschränkt sich meine Stellungnahme auf grundsätzliche Erwägungen und ausgewählte Einzelfragen.

A) Notwendige Anpassungen an das EU-Datenschutzrecht und problematische Nutzung als „Omnibus“- / „Container“-Gesetz

Die EU-Datenschutzgrundverordnung (EU) 2016/679 (im Folgenden: DSGVO) gilt seit dem 25. Mai 2018 unmittelbar verbindlich (Art. 99 Abs 2). Die Richtlinie (EU) 2016/680 war ebenfalls bereits bis zum 6. Mai 2018 in das mitgliedstaatliche Recht umzusetzen. Daher ist es grundsätzlich zu begrüßen, dass die Bundesregierung jetzt (verspätete) Anstrengungen unternimmt, die noch ausstehenden Anpassungen und Umsetzungen auf den Weg zu bringen. Die Vereinheitlichung der Terminologie, die das neue EU-Datenschutzrecht mit sich bringt, ist für die weitere Harmonisierung und Fortentwicklung des Datenschutzrechts grundlegend. Die überfällige Anpassung weiterer Fachgesetze des Bundes ist daher ein wichtiges Anliegen.

Seiten insgesamt

1/5

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

hwr-berlin.de

www.hwr-berlin.de/prof/hartmut-aden

www.foeps-berlin.org



Allerdings enthält der Gesetzentwurf – anders als sein Titel suggeriert – keinesfalls nur Anpassungen an die DSGVO und Umsetzungsbestimmungen für die Richtlinie (EU) 2016/680. Vielmehr sind für einige der insgesamt 154 in den Entwurf einbezogenen Gesetze weitreichende zusätzliche Änderungen vorgesehen, die nicht auf die EU-Datenschutzreform zurückgehen, sondern mit denen rein bundespolitische Anliegen verfolgt werden.

Die Integration solcher Inhalte in einen Gesetzentwurf, die nicht mit dem eigentlichen Gesetzeszweck zu tun haben („Omnibus“- oder „Containergesetz“), ist grundsätzlich verfassungsrechtlich zulässig. Allerdings sollte diese Gesetzgebungstechnik nur für Regelungen von geringer inhaltlicher Reichweite eingesetzt werden. Für inhaltlich weitreichende Regelungen, insbesondere für solche, die zusätzliche Grundrechtseingriffe zulassen, sollte diese Regelungstechnik nicht verwendet werden. Sie ist im Hinblick auf die Anforderungen des Demokratieprinzips (Art. 20 Abs. 2 GG) an die Transparenz der Gesetzgebung problematisch. Das Gebot der Transparenz der Entwürfe und ihrer Begründungen für das parlamentarische Gesetzgebungsverfahren und gegenüber denjenigen, die von den neu zugelassenen Grundrechtseingriffen betroffen sind, erfordert vielmehr die Beratung zusätzlicher Grundrechtseingriffe in eigenständigen Gesetzgebungsverfahren.

1. Änderung des BDBOS-Gesetzes (Artikel 8 des Entwurfs)

Die vorgeschlagenen Änderungen des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOSG) gehen erheblich über die Umsetzung der Richtlinie (EU) 2016/680 (bzw. der DSGVO) hinaus und ermöglichen zusätzliche Eingriffe in das Telekommunikationsgeheimnis (Art. 10 GG). Sie sollten daher in ein eigenständiges Gesetzgebungsverfahren ausgelagert werden (s.o., A).

Problematisch ist insbesondere die in § 19 Abs. 4 (Entwurfassung) vorgesehene Speicherung von Verkehrsdaten für 75 Tage. Der Digitalfunk der Sicherheitsbehörden wird von einer großen, sogar weiter steigenden Zahl von Personen genutzt. Daher umfassen die Verkehrsdaten große Mengen an personenbezogenen Kommunikationsdaten der beteiligten Mitarbeiterinnen und Mitarbeiter sowie möglicherweise in die Kommunikation eingebundener außenstehender Personen. Keiner der in § 19 Abs. 1 bis 3 der Entwurfassung genannten Zwecke erfordert eine undifferenzierte Speicherung sämtlicher Verkehrsdaten über einen mit 75 Tagen relativ langen Zeitraum. Daher dürfte eine so weitreichende Speicherung nicht mit



dem Zweckbindungsgrundsatz (Art. 10 GG; Art. 7 und 8 EU-Grundrechtecharta, für Polizei und Strafjustiz konkretisiert durch Art. 1 Nr. 4 b und c RL (EU) 2016/680) vereinbar sein. Alternativ sollten im Sinne des Vorrangs von *Privacy by Design*-Lösungen technische Konzepte zum Erreichen der in § 19 Ziele entwickelt werden, die mit weit weniger personenbezogenen Daten auskommen und dann im Hinblick auf den Zweckbindungsgrundsatz eher verhältnismäßig wären.

2. Änderungen des BSI-Gesetzes (Art. 13 des Entwurfs)

Auch die vorgeschlagenen Änderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) enthalten zusätzliche Eingriffsgrundlagen für weitreichende Grundrechtseingriffe, die über die Anpassung an das EU-Datenschutzrecht hinausgehen. Hier werden bereichsspezifische Datenerhebungs- und Datenschutzvorschriften für das IT-Sicherheitsrecht erst neu geschaffen, was grundsätzlich zu begrüßen ist.

Die Vorschrift gestattet allerdings weitreichende Formen der Datenverarbeitung für sehr unspezifisch formulierte Zwecke („Sammlung, Auswertung oder Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für die Informationstechnik“). Möglichkeiten, die Zwecke präziser zu fassen und deutlich zu machen, inwiefern für Zwecke der Informationssicherheit überhaupt Daten mit Personenbezug erforderlich sind, bleiben hier ungenutzt.

Auch diese weitreichenden Änderungen sollten in ein gesondertes Gesetzgebungsverfahren verschoben und dort im Hinblick auf den Zweckbindungsgrundsatz präzisiert werden.

Empfehlung: *Der Deutsche Bundestag sollte Regelungen, die nicht im Zusammenhang mit der Anpassung bzw. Umsetzung datenschutzrechtlicher Bestimmungen im Hinblick auf das EU-Datenschutzrecht stehen, in ein eigenständiges Gesetzgebungsverfahren auslagern.*

C. Beispiele für problematische Einzelregelungen

Auch zahlreiche Einzelregelungen des vorliegenden Entwurfs sind problematisch, da teils bestehende Defizite nicht hinreichend abgestellt werden und teils neue Unklarheiten entstehen. Dies betrifft auch die in der Fachliteratur breit diskutierten Defizite der Umsetzung des EU-Datenschutz-



rechts im Bundesdatenschutzgesetz 2018. Darüber hinaus seien folgende Beispiele angeführt:

1. Bundesmeldegesetz (Art. 16 des Entwurfs)

Mit den Melderegistern verfügen bundesdeutsche Behörden über weitreichende Informationssammlungen über die Bevölkerung. Das Bundesmeldegesetz (BMG) enthält in seiner bisherigen Fassung zahlreiche, teils sehr problematische Befugnisse der Meldebehörden zur Datenübermittlung an öffentliche und nicht-öffentliche Stellen. Beispielhaft seien hier die besonders problematischen Regelungen des § 44 Abs. 3 BMG zur Übermittlung von Melderegisterdaten an Private zu Zwecken der Werbung oder des Adresshandels genannt. Diese Regelung wurde zwar geändert, aber im Kern beibehalten. Im Hinblick auf die Anforderungen des Art. 7 DSGVO an eine informierte Einwilligung wären hier zumindest konkretisierte behördliche Pflichten zur Prüfung der Voraussetzungen dieser DSGVO-Vorschrift erforderlich gewesen. Noch besser wäre ein vollständiges Verbot der Datenübermittlung an Private für Zwecke der Werbung und des Adresshandels, da kein legitimer Allgemeinwohlzweck für diese staatliche Dienstleistung an Private mit negativen Rückwirkungen auf den Grundrechtsschutz besteht.

2. Postgesetz (Art. 134 des Entwurfs)

Die Änderungen des Postgesetzes integrieren die bislang in der Postdienste-Datenschutzverordnung (PSDV) enthaltenen Vorschriften in das Postgesetz. Dies ist im Interesse der Übersichtlichkeit grundsätzlich zu begrüßen. Die Neuregelung enthält allerdings Mängel. So war bislang nach § 7 Abs. 3 PSDV ein Widerspruchsrecht für Postfachinhaber gegen die Weitergabe ihrer Daten vorgesehen. Dieses Widerspruchsrecht wurde in der Entwurfsfassung (§ 41a Abs. 2 PostG-Entwurf) gestrichen, ohne es durch eine Einwilligungserfordernis zu ersetzen.

In der Regelung zur Erhebung von Daten aus Ausweispapieren fehlt zudem der im Hinblick auf die Durchsetzung des Grundsatzes der Verhältnismäßigkeit gebotene explizite Hinweis auf die Erforderlichkeit für das Erreichen des legitimen Zwecks als Voraussetzung für die Datenerhebung (§ 41b Abs. 1 PostG-Entwurf).



D. Nach der Reform ist vor der Reform: Zukünftige „Baustellen“ für die Weiterentwicklung des Datenschutzrechts

Der umfangreiche Gesetzentwurf, der dem Deutschen Bundestag jetzt vorliegt, ist nur eine Etappe von mehreren hin zu einem modernen Datenschutzrecht.

1. E-Privacy-Verordnung

Anfang 2017 veröffentlichte die Europäische Kommission einen Verordnungsentwurf,¹ der die veraltete ePrivacy-Verordnung 2002/58/EG ablösen soll. Der Vorschlag befindet sich gegenwärtig noch im EU-Gesetzgebungsverfahren. Für die elektronische Kommunikation wird diese Verordnung die DSGVO zukünftig ergänzen und konkretisieren. Dies wird auch umfangreiche weitere Änderungen im deutschen Datenschutzrecht nach sich ziehen.

2. Evaluation der Datenverarbeitungspraxis und Nutzung von technischen Datenschutzlösungen

Der vorliegende Gesetzentwurf, der eine große Zahl von Fachgesetzen betrifft, zeigt erneut, wie ausdifferenziert das bereichsspezifische Datenschutzrecht in Deutschland ist. Die durch die DSGVO und die Richtlinie (EU) 2016/680 veranlassten Vereinheitlichungen sind indes nur ein Schritt von mehreren hin zu einem effektiven und modernen Datenschutzrecht in Deutschland. Erforderlich ist auch eine kritische Evaluation der zahlreichen Zweckänderungs- und Datenübermittlungsbefugnisse, die in den diversen Fachgesetzen vorgesehen sind. Über die praktische Nutzung dieser Befugnisse und ihre Auswirkungen auf die Betroffenen ist nur wenig bekannt. Für das zukünftige gesetzgeberische Nachsteuern und die Entwicklung technischer Datenschutzlösungen sind daher mehr empirische Informationen über die Datenverarbeitungspraxis bundesdeutscher Behörden erforderlich.

Gesamtfazit: Ich empfehle dem Deutschen Bundestag, den Entwurf nur nach gründlicher Überarbeitung zu verabschieden und die nicht mit dem EU-Datenschutzrecht zusammenhängenden „Container“-/„Omnibus“-Elemente aus dem Entwurf herauszunehmen.

Gez. Prof. Dr. Hartmut Aden

¹ COM(2017) 10 final.