Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 E

Dr. Stefan Brink

LfDI Baden-Württemberg

6.12.2018

Stellungnahme gegenüber dem Deutschen Bundestag

zur BT-Drucksache 19/4674 vom 1. Oktober 2018

Die mühsame Anreise durch das Datenschutz-Deutschland des 2. DSAnpUG-EU

Seit dem 25. Mai 2018 reguliert europäisches Recht den Datenschutz. In den 70er Jahren in Deutschland entwickelt und seit 1995 mit einer umsetzungsbedürftigen europäischen Richtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31) ausgestaltet, endet so die jahrzehntelange Reise der Idee von der individuellen Entscheidung über persönliche Informationen – seit 1983 „Grundrecht auf informationelle Selbstbestimmung“ genannt – an einem absoluten Ziel- und Höhepunkt: Durch europäischen Verordnung (VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016, ABl. L 119 vom 4.5.2016, S. 1) sind jetzt alle Informationsbeziehungen zwischen Privatpersonen auf der einen und Unternehmen und Behörden auf der anderen Seite eindeutig und abschließend geregelt. Und zwar durch unmittelbar geltendes, in der ganzen Europäischen Union gleichlautendes und mit Anwendungsvorrang vor nationalen Normen ausgestattetes Recht.

Damit ist die „Reise nach Europa“ für den Datenschutz aber noch nicht an ihrem Ende. Denn gerade wegen des Anwendungsvorrangs der Europäischen Verordnung müssen jetzt noch nationale Altbestände des Datenschutzrechts aus dem Weg geräumt werden – in Deutschland waren dies etwa das „gute alte“

Bundesdatenschutzgesetz und die – zeitlich noch älteren – Landesdatenschutzgesetze.

Soweit – so einfach. Aber das Reisen in Europa ist aus zweierlei Gründen doch etwas komplizierter als das einfache Umsteigen vom nationalen D-Zug in den Trans-Europa-Express: Zum einen ist das neue europäische Verordnungsrecht sachlich nicht umfassend anwendbar, es spart etwa Bereiche wie die Datenverarbeitung durch Parlamente (Art. 2 Abs. 2 lit. a DSGVO), durch Privatpersonen für persönliche Tätigkeiten (Art. 2 Abs. 2 lit. c DSGVO, etwa das Fotografieren fürs Familienalbum) oder durch Behörden zum Zwecke der Strafverfolgung oder Strafvollstreckung (Art. 2 Abs. 2 lit. d DSGVO) aus. Hier wird weiter national geregelt. Zum anderen ist die DSGVO leider gar keine Vollregelung. Sie lässt zahlreiche Lücken, deren Ausfüllung sie ausdrücklich den Mitgliedsstaaten der EU überlässt (sog. „Öffnungsklauseln“). Damit stellt die DSGVO ihr großes Ziel, gleiches Recht in Europa gleichmäßig anzuwenden, zwar in Frage; aber so entlasteten sich Europäisches Parlament und Rat im ohnehin langwierigen und fragilen Gesetzgebungsprozess. Anstatt eine europaweit einheitliche Lösung für die Fragen der Verarbeitung von Beschäftigtendaten oder für die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten zu finden, überließ man es den Mitgliedsstaaten, hier jeweils nationale Antworten zu geben. Daraus erklärt sich, warum es auch nach dem 25. Mai 2018 noch nationales Datenschutzrecht gibt – und im föderalen Deutschland gleich in doppelter Ausführung (BDSGneu/16 LDSGneu).

1. Aufschlag

In einem ersten Aufschlag haben die Deutschen Gesetzgeber (mit leichter Verspätung) schon mal die dicksten nationalen Brocken von der Straße geschoben, sie haben das Bundesdatenschutzgesetz und die entsprechenden Ländergesetze an die Vorgaben der DSGVO angepasst und von den verbliebenen Regulierungsmöglichkeiten ausgiebig Gebrauch gemacht (Gesetz 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 – vom 30. Juni 2017, BGBl. I S. 2097). Dabei haben die nationalen Gesetzgeber allerdings nicht nur gut geräumt, sie haben auch ganz erhebliche Kollateralschäden am Straßenkörper verursacht: Die Strecke nach Europa wurde nicht schneller, sondern holperiger. Zu nennen wären da etwa ganz offensichtliche Kompetenzüberschreitungen zu Lasten der DSGVO, etwa mit § 4 BDSG zur Videoüberwachung. Mit dieser Vorschrift wird jetzt jeder Parkplatzbetreiber zum Terrorfahnder heraufgestuft und die Arbeit der Aufsichtsbehörden in den Ländern ganz erheblich (und gezielt) erschwert. Zu nennen ist auch die absurde Vorschrift des § 43 Abs. 4 BDSG, wonach Bußgelder bei Datenpannen nur noch verhängt werden können, wenn der Verantwortliche dem zustimmt (!). Auch beim Versuch, die wackeren Rechtsanwälte, Ärzte und Steuerberater dem Zugriff der furchtbaren Landesdatenschützer zu entziehen (§ 29 BDSG), leistete der Bundesgesetzgeber ganze Arbeit – die nun vom Europäischen Gerichtshof in mühsamer Kleinarbeit wieder glattgezogen werden muss. Vertragsverletzungsverfahren sind dem deutschen Gesetzgeber schon mal sicher.

Ansonsten nutzte der Bundestag tatsächliche oder vermeintliche Öffnungsklauseln dazu, die Rechte der Betroffenen wo immer möglich weiter einzuschränken (§§ 32 ff. BDSG); lediglich bei der Bestellpflicht eines betrieblichen Datenschutzbeauftragten überbot der nationale Gesetzgeber die laschen Vorgaben der DSGVO (Art. 37 f.), was er aber jetzt schon wieder bereut (vgl. Bundesrats-Drucksache 430/1/18).

Als tröstlich mag man empfinden, dass noch eindeutigere Verstöße gegen Wortlaut und Geist der DSGVO anderen Regierungen überlassen blieben, etwa Österreich mit der Freistellung von Erstverstößen von der Bußgeldpflicht (Art. 83 DSGVO) oder dem Bayerischen Kabinett mit der rechtsgrundlosen Herausnahme von Vereinen aus der Bestellpflicht von Datenschutzbeauftragten. Hier endet die Reise nach Europa offensichtlich in der Sackgasse.

2. Aufschlag

Mit weitaus erheblicherer Verspätung - mehr als ein halbes Jahr nach Wirksamwerden der DS-GVO - bemüht sich nun die Bundesregierung darum, in einem zweiten (und vermeintlich letzten) Anlauf die gesamte bundesdeutsche Restrechtsmaterie DSGVO-konform zu gestalten. Sie tut dies in einem vom Innenministerium federführend zu verantwortenden „Omnibus-Gesetz“, das in einem Artikelgesetz mehr als 150 Bundesgesetze Huckepack nimmt und abändert. Es dient der Anpassung sogenannter „bereichsspezifischer Datenschutzvorschriften“ des Bundes an die DSGVO, mit dabei sind Gesetze aus allen Ressortbereichen der Bundesregierung. Dass es sich beim Datenschutzrecht mittlerweile um eine echte Querschnittsmaterie handelt, erfährt jeder, der die 563 Seiten der Bundesrats-Drucksache 430/18 vom 7. September 2018 durchblättert; betroffen sind so unterschiedliche Rechtsmaterien wie das Antiterrordatei-Gesetz, das Anti-Doping-Gesetz und das Prostituiertenschutz-Gesetz.

Dieser Mammut-Regierungsentwurf wurde am 5.9.2018 vom Bundeskabinett beschlossen und zunächst dem Bundesrat zur Beratung zugeleitet, die 1. Lesung im Deutschen Bundestag (BT-Drucksache 19/4674 vom 1. Oktober 2018) fand am 12.10.2018 statt.

Wohin geht die Reise?

Großteils bestehen die Änderungen lediglich darin, die bisherigen Vorschriften an die Terminologie der DS-GVO anzupassen. Wenig spektakulär, aber absolut notwendig sind etwa die Ersetzung der Wörter „erheben, speichern, verändern und nutzen“ durch das Wort „verarbeiten“. Dieser DS-GVO-Sprech betrifft nicht nur die Gesetzesfassade, er verdeutlicht auch den fundamentalen Wechsel der Rechtsquelle, der mit dem 25.5. vollzogen wurde: Wir alle wenden nicht länger wohlbekanntes deutsches Recht an, das der Verwaltung vertraut, von zahlreichen Kommentatoren ausgeleuchtet und von nationalen Gerichten ausgeformt wurde. Wir ergründen die europäische Bedeutung nur scheinbar bekannter Rechtsbegriffe.

„Verarbeiten“ nach § 3 Abs. 4 BDSG alter Fassung ist eben nicht identisch mit der „Verarbeitung“ des Artikel 4 Nr. 2 DSGVO. Das alte Verständnis aus den Köpfen der erfahrenen Datenschützer herauszubekommen und Platz zu machen zumindest für die Bereitschaft, vermeintlich Wohlbekanntes neu und richtig zu verstehen, ist eine Herausforderung.

Materielle Änderungen finden sich im Gesetzentwurf natürlich auch: Wieder nutzt die Bundesregierung die Öffnungsklauseln der DS-GVO, um Betroffenenrechte auf Auskunft oder Löschung einzuschränken. Dabei ist wie bereits beim 1. Anpassungsgesetz nicht immer ganz klar, ob die Voraussetzungen für diese Beschränkungen, wie sie in Artikel 23 Absatz 1 DS-GVO festgelegt sind, auch in jedem Falle vorliegen. Solche Unterschreitungen des Schutzniveaus der DSGVO sind nämlich nur dann zulässig, „sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt“. Das wäre in jedem Einzelfall zu prüfen. Zudem muss jede einschränkende Gesetzgebungsmaßnahme „insbesondere gegebenenfalls spezifische Vorschriften enthalten“, jedenfalls hinsichtlich der Zwecke der Verarbeitung und mittels Garantien gegen Missbrauch oder unrechtmäßige Übermittlung der Daten (Art. 23 Abs. 2 DS-GVO). Es liegt sehr nahe, dass der EuGH in den kommenden Jahren klare Vorgaben für solche Rechtsbeschränkungen entwickeln wird – und dass auch der deutsche Gesetzgeber hiervon betroffen sein wird.

Erster Kandidat für solche Korrekturen wird der im 2. DSAnpUG-EU an zahlreichen Stellen zu findende Ausschluss des Auskunftsrechts nach Artikel 15 DS-GVO sein, der unser Bürgerrecht auf Kenntnis von Verarbeiter und Verarbeitung bereits dann einschränkt, „wenn die Auskunftserteilung die ordnungsgemäße Aufgabenerfüllung gefährden würde“. Dieser Maßstab ist offensichtlich so niedrig angesetzt, dass zahllose Datenverarbeitungen durch öffentliche Stellen künftig „unter dem Radar“ segeln würden. Das kann nicht richtig sein – und ist von der DS-GVO auch nicht gewollt. Wie schon beim 1. DSAnpUG-EU verpasst die Bundesregierung damit

erneut die Chance, den Datenschutz als Grundrechtsschutz auf ein insgesamt höheres Niveau zu heben.

Darüber hinaus finden sich breit über die 563 Seiten des Gesetzentwurfs verteilt Einzelbestimmungen zu Datenverarbeitungen, die der Bundesregierung schon immer „ein Anliegen“ waren. Aus der Vielzahl problematischer Einzelregelungen seien nur die datenschutzrechtlich problematischsten hervorgehoben:

- Teilweise werden bei Gelegenheit der Rechtsanpassung eigenständige Rechtsgrundlagen mit dem Ziel geschaffen, weitreichendere Verarbeitungen personenbezogener Daten zu gestatten als bislang erlaubt, etwa nach dem Telekommunikationsgesetz. Mit § 19 Absatz 4 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS-Gesetz - BDBOSG) soll so zugunsten der Bundesanstalt für den Digitalfunk eine Vorratsdatenspeicherung für Verkehrsdaten eingeführt werden, die sage und schreibe alle Daten der vergangenen 75 Tage umfasst. Das ist eine – auch mit Blick auf vorliegende und noch ausstehende Entscheidungen des Bundesverfassungsgerichts und des EuGH zur Grundproblematik jeder anlasslosen massenhaften Datenspeicherung – steile Ansage.

- Zumindest unschön ist eine Neuregelung im Soldatengesetz, die vorsieht, dass Meldebehörden personenbezogene Daten deutscher Staatsangehöriger, die im nächsten Jahr volljährig werden, an das Bundesamt für Personalmanagement der Bundeswehr übermitteln dürfen. Gedanklich scheint die Bundesregierung die allgemeine Wehrpflicht also noch nicht realisiert zu haben. Dass Betroffene der Übermittlung vorab widersprechen können, ist da nur ein schwacher Trost.

- Ähnlich unsauber ist die vorgesehene Neuregelung im IHK-Gesetz, wonach die Industrie- und Handelskammern personenbezogene Daten ihrer Kammermitglieder an nicht-öffentliche Stellen übermitteln dürfen, wenn die

Kammermitglieder dem nicht widersprechen. Zu Zeiten, in denen der Kammerzwang keineswegs völlig akzeptiert ist, tun sich die IHKs mit solchen Eingriffen in Mitgliederrechte sicherlich keinen Gefallen.

- Manches Mal ist auch das Schweigen des Gesetzentwurfes beredt: Anders als noch im Referentenentwurf vorgesehen, findet sich im Regierungsentwurf zur Änderung des SGB V nicht mehr die Möglichkeit, gegen die gesetzlichen Krankenkassen bei Datenschutzverstößen erhebliche Bußgelder zu verhängen. Glückwunsch an die erfolgreichen Lobbyisten.

- Das gilt auch für den mit Blick auf die gerade scheiternden Verhandlungen zur ePrivacy-Verordnung besonders relevanten Anpassungen und Neuregelungen des Telekommunikationsgesetzes TKG. Anders als noch im Referentenentwurf vorgesehen, findet man im Entwurf nun keinerlei Regelungen zum Verhältnis von TKG und DSGVO mehr – und damit hängt eine unabhängige Datenschutzaufsicht in diesem wichtigen Bereich weiter in der Luft.

- Mehrfach wird die durch die DS-GVO grundsätzlich verbotene Verarbeitung sensitiver Daten (vgl. Art. 9 Abs. 1 DS-GVO) durchbrochen. So sollen nun auch nicht-öffentliche Stellen zur Verarbeitung solcher Daten grundsätzlich befugt sein, wenn dies aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist (§ 22 Absatz 1 Nummer 1 Buchstabe d BDSG). Damit werden etwa die Voraussetzungen dafür geschaffen, dass sensible Informationen durch zivilgesellschaftliche Träger im Rahmen von Deradikalisierungsprogrammen verarbeitet und im Einzelfall an die Sicherheitsbehörden weitergegeben werden können. Auch wenn man dies vom Grundansatz als legitimes Interesse ansieht, lässt die ungewöhnlich weite sprachliche Fassung erheblich weitergehende Anwendungsbereiche erwarten und befürchten.

Im Asylgesetz und im Aufenthaltsgesetz soll zudem die Verarbeitung sensitiver Daten freigegeben werden, „soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist“. Diese weite und strukturlose Formulierung widerspricht eindeutig der Öffnungsklausel des Artikel 9 Absatz 1 Buchstabe g DSGVO. Zudem sind nirgends spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der Betroffenen vorgesehen.

Auch hier zeigt sich wieder: Wer Grundrechte einschränken möchte, fängt damit bei Außenseitergruppen an: Bei Straftatverdächtigen, Asylsuchenden, Ausländern. Der weitere Weg solche Grundrechtsverluste ist dann vorgezeichnet: über „extensive“ Grundrechtsnutzer wie Demonstranten, Meinungsinhaber und Reisende bis hinein in den Kern unserer Gesellschaft.

Fazit

Insgesamt gesehen bleiben beim geneigten Leser dieses Werkes drei Eindrücke hängen:

1. Ein solches Mammutprojekt vollständig zu durchdringen, ist weder dem Parlament, noch der kritischen Öffentlichkeit möglich. Ob dies nun der komplexen Materie oder dem überschießenden Regulierungsinteresse der Bundesregierung geschuldet ist, bleibt letztlich gleich. Rationale Gesetzgebung wird so nicht funktionieren. Abhilfe wäre nur möglich, indem sich die Regierung jeder materiellen Nutzung von Öffnungsklauseln enthält (ja, das wäre durchaus möglich!) oder zumindest eine klare Trennung von terminologischen und ideologischen Änderungsanliegen vornimmt.

2. Anstatt den Schwung der DSGVO aufzugreifen und zu begreifen, dass die Zukunft der Datenverarbeitung aus europäischer Sicht und als globales Alleinstellungsmerkmal nur in einer unauflöslichen Verbindung von Digitalisierung und Datenschutz liegen kann, ergeht sich der Entwurf in einem Kleinklein der Beschränkung von Betroffenenrechten. So agieren nicht inspirierte Gestalter, so agieren Kleinkrämer.

3. Der lange Weg des Datenschutzes nach Europa kann nur gelingen, wenn die nationalen Straßen von Ballast und Unrat geräumt werden und der „Omnibus zur EU“ freie Fahrt bekommt. Dabei sind alle nationalen Vorschriften, die nicht EU-rechtskonform ausgestaltet sind, von Übel, denn sie verzögern, wo Tempo gefragt ist und sie verunsichern, wo Klarheit Not tut. Auch mit diesem 2. Gesetzentwurf steht die Bundesregierung weiter auf der Bremse.