Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)824 D

S t e l l u n g n a h m e

zum Gesetzentwurf der Bunderegierung

Entwurf eines Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU)

BT-Drucksache 18/11325

erstellt von
Rechtsanwalt Andreas Jaspers,
Geschäftsführer der **G**esellschaft für
Datenschutz und **D**atensicherheit e.V.

I. Grundsätzliches

Grundsätzlich ist Kernregelung des DSAnpUG-EU, die Neufassung des BDSG, zu begrüßen, weil es dazu beiträgt, die zu Recht kritisierte Unterkomplexität der DS-GVO durch differenzierte und am bisherigen BDSG orientierte Regelungen zu konkretisieren und praxisgerecht auszugestalten.

Ein verfassungsrechtliches Kernproblem ist die Kompetenz der Mitgliedstaaten bei der Ausfüllung von Öffnungsklauseln in der Grundverordnung. Der Entwurf legt diese Klauseln aus, um Rechtssicherheit zu schaffen. Dies ist sinnvoll, da die Zulässigkeitsnormen und die Ausgestaltung der Betroffenenrechte in der DS-GVO oftmals nur unter großem administrativen Aufwand oder gar nicht umsetzbar sind. Dem Vorwurf, die Neufassung des BDSG konterkariere den Willen der DS-GVO, lässt sich entgegenhalten, dass die „Grund"-Verordnung als neuartige Verordnungsform mit ihren zahlreichen Öffnungen und verordnungsuntypischen, sehr weiten Formulierungen, den Mitgliedstaaten gerade ermöglichen will, Konkretisierungen zu schaffen.

Der deutsche Gesetzgeber entscheidet mit der Neufassung des BDSG über wirtschaftlich und politisch sehr relevante Fragen. Damit regelt er im Rahmen der Öffnungsklauseln Sachverhalte, die ansonsten nach der DS-GVO die Datenschutzaufsichtsbehörden der EU im sehr mächtig ausgestalteten Datenschutzausschuss entscheiden würden. Den Aufsichtsbehörden fehlt jedoch weitgehend die demokratische Legitimation für Entscheidungen zur Datenverarbeitung von grundsätzlicher Bedeutung. Die Entscheidungen des Datenschutzausschusses kann in Regel abschließend erst der EuGH überprüfen. So gesehen schafft der Ansatz des Entwurfs der Bunderegierung neben Rechtssicherheit in der Anwendung der Normen in Deutschland zumindest im Anwendungsbereich des Rechts innerhalb der Öffnungsklauseln auch mehr demokratische Legitimation.

II. Zu Vorschriften in der Neufassung des BDSG

1. Zulässigkeit der Datenverarbeitung

Zur Zweckänderung

Die Regelung des § 24 BDSG-E gestattet nicht öffentlichen Stellen, unter bestimmten Voraussetzungen die Verarbeitung personenbezogener Daten über die restriktiven Kompatibilitätsanforderungen des Art 6 Abs. 4 DS-GVO hinaus zu einem anderen Zweck, als zu demjenigen, zu dem die Daten erhoben wurden.

Die Nummern 1 und 2 des Abs. 1 (Gefahrenabwehr, Geltendmachung rechtlicher Ansprüche) bilden hierbei im Wesentlichen die bestehende Rechtslage ab.

Eine Begrenzung der Nr. 2 auf zivilrechtliche Ansprüche des Verantwortlichen, die vom Bundesrat vorgeschlagen wird (BR-Drs. 110/17 Nr. 21), greift zu kurz. Interessengerecht ist es, Verantwortliche zu berechtigen, auch bei öffentlich-rechtlichen Ansprüchen personenbezogene Daten zu übermitteln.

Diese Ansprüche sollten auch nicht auf Ansprüche des Verantwortlichen gegenüber der betroffenen Person beschränkt bleiben, wie es vom Bundesrat gefordert wird (BR-Drs. 110/17 Nr. 22). Da nachträgliche Datenweitergaben an Dritte in der Regel nicht mit dem Erhebungszweck kompatibel sind, bedarf es einer Regelung, die auch bei berechtigten Ansprüche Dritter hierzu eine Rechtsgrundlage bieten. Als Beispiel können Gläubigeranfragen zur Zwangsvollstreckung oder Schadensersatzansprüche Dritter gegen eigene Arbeitnehmer genannt werden. Grenzen der Weiterverarbeitung werden im Regierungsentwurf des § 24 Abs. 1 BDSG-E durch die Interessenabwägung gesetzt.

Zum Beschäftigtendatenschutz

§ 26 BDSG-E setzt die in Art. 88 DS-GVO enthaltene Öffnungsklausel für Datenverarbeitungen im Beschäftigungskontext um. Dieses ist als Schritt zu mehr Rechtssicherheit zu begrüßen. Mit der bisher ergangenen arbeitsgerichtlichen Rechtsprechung und dem umfangreichen Schrifttum ist ein stabiles Fundament für die zukünftige Rechtsanwendung gelegt.

In der Kommunikation mit den Beschäftigten sollte der zunehmenden Bedeutung von digitalen Arbeitsabläufen Rechnung getragen werden und deshalb die Textform statt Schriftform in Absatz 2 bei der Einwilligung als Voraussetzung normiert werden.

Die in § 26 Abs. 3 BDSG-E enthaltene Regelung zur Verarbeitung sensibler Daten im Beschäftigungsverhältnis zur Erfüllung gesetzlicher Pflichten sollte zur Klarstellung auch den Zweck „Pflichten aus dem Steuerrecht“ als Rechtfertigungsgrund aufnehmen, da z.B. die Verarbeitung von Daten über den Familienstand und die Religionszugehörigkeit im Rahmen des Beschäftigungsverhältnisses gewährleistet bleiben muss.

Klarstellende Bedeutung hat auch die Reglung in § 26 Abs. 4 BDSG-E, wonach die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses auch auf der Grundlage von Kollektivvereinbarungen zulässig bleibt. Dies entspricht auch Erwägungsgrund 155 DS-GVO.

Zu Datenübermittlungen an Auskunfteien und zum Scoring

Die Regelung in § 31 BDSG-E nimmt die Vorschriften des derzeit geltenden BDSG auf (§§ 28a, 28b BDSG). Der Rekurs auf etablierte Verfahrensweisen als Schritt zu mehr Rechtssicherheit - sowohl zugunsten der Betroffenen als auch der verantwortlichen Stellen - ist zu begrüßen.

2. Pflichten der Verantwortlichen

Zu den Transparenzpflichten

§ 33 Abs. 1 Nr. 2 lit. a BDSG-E schränkt die Pflicht zur Information der betroffenen Person bei Zweckänderungen ein, sofern die Informationserteilung voraussichtlich die Verwirklichung der Ziele der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss. Dies ist praxisgerecht, da anderenfalls investigative Maßnahmen bei Verdacht auf kriminelle Handlungen dem Betroffenen angekündigt werden müssten.

Zusätzlich sollten die bisherigen Ausnahmeregelungen des § 33 Abs. 2 Nr. 2, Nr. 7a, und 7b, 8a und 8b BDSG zu gesetzlichen Aufbewahrungspflichten und zur Übernahme von Daten aus öffentlichen Quellen übernommen werden. Viele Unternehmen (z.B. Kreditinstitute) sind aufgrund der Vorgaben zur Compliance und zur Geldwäschebekämpfung gehalten, Daten auch aus öffentlichen Quellen zu erheben. Eine Unterrichtung der davon Betroffenen könnte im Spannungsfeld zu den Zwecken Compliance und Geldwäschebekämpfung stehen. Deshalb sollten diese bisherigen Ausnahmetatbestände fortgeführt werden, zumindest bei Verfolgung der genannten Zwecke.

Zur Auskunft

Die in § 34 Abs. 1 BDSG-E vorgesehenen Ausnahmen zur Auskunft knüpfen an den heutigen § 33 Abs. 2 BDSG an und nehmen Daten von der Auskunftspflicht aus, die nur aufgrund von Aufbewahrungsvorschriften gespeichert sind. Diese Daten sind zu sperren, d.h. aus dem produktiven Datenbestand zu entfernen und ggfs. zu archivieren. Bei gesetzlichen Aufbewahrungsvorschriften ergibt sich

dies aus § 35 Abs. 1 i.V.m. Art. 17 Abs. 3 DS-GVO, bei satzungsmäßigen oder vertraglichen Aufbewahrungsvorschriften aus der Pflicht zum Ausschluss der Verarbeitung durch geeignete technische und organisatorische Maßnahmen gem. § 24 Abs. 1 Nr. 2 BDSG-E. Weder für das Unternehmen noch für den Betroffenen haben diese gesperrten Daten eine persönlichkeitsrechtsbeeinträchtigende Wirkung. Eine zweckwidrige Weiterverarbeitung dieser gesperrten Daten unter Bußgeldbewährung ist im Gegensatz zur Darstellung des Bundesrates nicht zu befürchten. Das Auskunftsrecht auch auf nur aufbewahrungspflichtige Daten zu erweitern, würde einen unverhältnismäßigen Aufwand bedeuten. Dasselbe gilt für Daten, die nur zu Zwecken der Datensicherung oder Datenschutzkontrolle gespeichert sind (siehe nachfolgend).

Zur Löschung

Das Recht auf Löschung wird in § 35 BDSG-E auf die Sperrvorschriften des § 35 Abs. 3 BDSG zurückgeführt. Insofern wird aus der Einschränkung der Verarbeitung nach Art. 18 DS-GVO, die nur als Betroffenenrecht ausgestaltet ist, eine ergänzende Pflicht des Verantwortlichen. Praxisrelevanz hat dieser Rückgriff auf das BDSG z.B. bei der Datensicherung. Sämtliche, z.T. umfangreiche Tages-, Wochen- und Monatssicherungen müssten für ein zu löschendes Datum mit großem administrativen Aufwand der IT korrigiert werden. Dies wäre unverhältnismäßig. Konsequent ist insofern auch die Beibehaltung der Sperrpflicht nicht nur bei gesetzlichen (Art. 17 Abs. 3 lit. b DS-GVO), sondern auch bei vertraglichen oder satzungsmäßigen Aufbewahrungspflichten. Dadurch werden Pflichtenkollisionen vermieden.

Ein weiterer Gesichtspunkt von Praxisrelevanz dieser Vorschrift ist Gestaltung von Datenbanken. Dort sind Daten mit unterschiedlichen Zweckbestimmungen aus Gründen der referenziellen Integrität miteinander verknüpft. Eine Teillöschung ist deshalb bei Standardanwendungen aufgrund ihrer Architektur systemtechnisch nicht möglich. Für diesen Fall muss ebenfalls eine Berufung auf § 35 BDSG-E möglich sein.

3. Aufsichtsbehörden und Sanktionen

One-stop-shop in Deutschland

Wie auch vom Bundesrat unter Ziffer 12 zu § 19 BDSG-E (vgl. BR-Drs.110/17) vorgeschlagen, sollte der „one-stop-shop“-Ansatz der DS-GVO auch bei innerstaatlichen Sachverhalten mit bundesweiter Bedeutung etabliert werden. Denn für grenzüberschreitende Sachverhalte innerhalb der Europäischen Union gelten spezielle Bestimmungen zur grenzüberschreitenden Zusammenarbeit der Aufsichtsbehörden (vgl. Artikel 56 und 60 ff. DS-GVO). Dementsprechend sollte § 19 BDSG-E wie vom Bundesrat vorgeschlagen ergänzt werden, um eine Regelung zur federführenden Zuständigkeit einer Datenschutzbehörde in den Fällen zu erhalten, in denen Aufsichtsfragen über die Grenzen eines Bundeslandes hinaus Bedeutung haben (z.B. bundesweit agierende Unternehmen oder länderübergreifend einheitlich nutzbare Produkte).

Akkreditierung von Zertifizierungsstellen

Eine klare Zuständigkeitsregelung für die Durchführung der Akkreditierung ist zu begrüßen. Da die Zertifizierung in der DS-GVO eine zentrale Position einnimmt, ist es wichtig, die Akkreditierungshürde und die daraus entstehenden Kosten für die mittelständische Wirtschaft im Blick zu halten und von einer Überregulierung Abstand zu nehmen.

Der in § 39 BDSG-E vorgeschlagene zweistufige Akkreditierungsweg über die Deutsche Akkreditierungsstelle GmbH (DAkkS) und die zuständige Datenschutzaufsichtsbehörde führt aber zu mehr Bü-

rokratie und Kosten für die zu zertifizierenden Unternehmen. In der Sache erscheint dieser Weg auch nicht notwendig zu sein, denn Art. 43 Abs. 1 DS-GVO sieht ausdrücklich eine einstufige Akkreditierung bei einer Datenschutzaufsichtsbehörde vor.

Stand bei der Errichtung einer deutschen Akkreditierungsstelle Produktprüfungen im Vordergrund (Erg. 48 VERORDNUNG (EG) Nr. 765/2008), so handelt es sich beim Datenschutz in erster Linie um eine Prüfung von Abläufen. Insofern hängt die Prüfqualität von dem verwendeten Prüfstandard ab und nicht von der Arbeit im "Laboren". Dazu haben die deutschen Datenschutzaufsichtsbehörden selber umfassendes Know-how aufgebaut, belegt durch Projekte wie z.B. das „Datenschutzsiegel in Nordrhein-Westfalen“, „Gütesiegel Datenschutz M-V“ und die Arbeiten des ULD. Insofern erscheint eine einstufige Akkreditierung direkt bei den Datenschutzaufsichtsbehörden sachgerechter und im Interesse von bezahlbaren Zertifikaten auch für die mittelständische Wirtschaft geboten.

Zu den Sanktionen

Die Art. 33 und 34 DS-GVO verpflichten den Verantwortlichen zur Meldung von Datenschutzvorfällen. Zugleich garantieren jedoch Art. 14 Abs. 3 lit. g IPbpR und Art. 6 Abs. 1 Satz 1 MRK die Selbstbelastungsfreiheit, den sog. nemo-tenetur-Grundsatz. § 42 Abs. 4 BDSG-E und § 43 Abs. 2 BDSG-E führen deswegen die derzeit geltende Regelung in § 42a Satz 6 BDSG fort, wonach solche Meldungen nicht in Bußgeld- oder Strafverfahren verwendet werden dürfen. Die GDD begrüßt, dass dem Konflikt zwischen Meldepflicht und Selbstbelastungsfreiheit auf diese Weise Rechnung getragen werden soll.

Die geplanten Vorschriften berücksichtigen jedoch nicht, dass Meldepflichtiger und Bußgeldpflichtiger nicht identisch sein müssen. Ist der Verantwortliche etwa eine juristische Person, kann immer noch gegen den persönlich Handelnden vorgegangen werden. Von daher ist ein weitreichendes Verwendungsverbot gesetzlich zu verankern, wie es derzeit nach herrschender Meinung in § 42a Satz 6 BDSG und § 97 Abs. 1 Satz 3 InsO interpretiert wird.

4. Zum Datenschutzbeauftragten

Begrüßenswert ist, dass die bislang geltenden Bestellvoraussetzungen für einen betrieblichen Datenschutzbeauftragten unverändert übernommen werden sollen. Mit Blick auf seine unabhängige Aufgabenwahrnehmung wurde auch der besondere Kündigungsschutz beibehalten. Ebenso wurde die besondere Schweigepflicht, die zugleich ein Schweigerecht ist, adaptiert.

Bonn, den 22.März 2017