Gesellschaft für Datenschutz
und Datensicherheit e.V.

Stellungnahme zur Evaluation des Bundesdatenschutzgesetzes (BDSG)

I. Allgemeines

Nachfolgende Stellungnahme konzentriert sich auf ausgewählte BDSG-Vorschriften, die auf Grundlage der Öffnungs- bzw. Spezifizierungsklauseln der Datenschutz-Grundverordnung (DS-GVO) ergangen sind.

II. Rechtsgrundlagen für die Datenverarbeitung

Zu Frage II. 1.

Zu § 4 BDSG

Mit § 4 BDSG regelt der deutsche Gesetzgeber einen bedeutenden Bereich der Verarbeitung personenbezogener Daten. Da die DS-GVO außer einer Erwähnung in den Erwägungsgründen keinen spezifischen Erlaubnistatbestand zur Videoüberwachung beinhaltet, gewinnt die Regelung im BDSG besondere Bedeutung und ist deswegen als sachgerechte und praxisrelevante Regelung zu begrüßen. Verantwortliche aus dem nichtöffentlichen Bereich können mit Videoüberwachungsmaßnahmen nicht nur eigene Interessen wie Verkehrssicherungspflichten oder Diebstahlsprävention verfolgen. Häufig liegen mit der Überwachung verfolgte Zwecke auch im öffentlichen Interesse. Dies ist etwa bei der Überwachung der in § 4 Abs. 1 S. 2 BDSG genannten Risikobereiche der Fall. Die Videoüberwachung gefahrträchtiger Räume durch Private erscheint häufig als unter die öffentlichen Aufgaben subsumierbar, da sie u.a. der Ermöglichung von Strafverfolgung durch Polizei und Justiz dient. Unabhängig entgegenstehender zulässiger Wertungen hat der Bundesgesetzgeber damit insbesondere im Lichte des Terroranschlags auf einem Berliner Weihnachtsmarkt Ende des Jahres 2016 eine zulässige und mit dem Unionsrecht vereinbare Gesetzgebung betrieben.

Das BVerwG setzt nach seiner Rechtsprechung zu § 4 BDSG (Urteil v. 27.03.2019 - 6 C 2.18) für die Zulässigkeit einer Videoüberwachung zu privaten Zwecken voraus, dass der Verantwortliche plausible Gründe darlegt, aus denen sich die Erforderlichkeit der Maßnahme ergibt. Die Anwendbarkeit des § 4 BDSG hat sich durch dieses Urteil unstrittig reduziert. Gleichwohl besteht weiterhin eine Zulässigkeit von Videoüberwachungen nach § 4 BDSG durch Private. Insbesondere kann die Videoüberwachung in den von § 4 Abs. 1 S. 2 BDSG erfassten hoch frequentierten Risikobereichen auch weiter durch Private zulässig erfolgen. Ersatzweise gründet sich die Rechtmäßigkeit auf Art. 6 Abs. 1 lit. f DS-GVO, wonach die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten zulässig ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Die Verarbeitung ist erforderlich, wenn der Verantwortliche zur Wahrung berechtigter, d.h. schutzwürdiger und objektiv begründbarer Interessen darauf angewiesen ist. Eine nach diesem Maßstab erforderliche Verarbeitung ist zulässig, wenn die Abwägung im jeweiligen Einzelfall ergibt, dass diese berechtigten Interessen höher zu veranschlagen sind als die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person. Somit besteht eine teleologische Kongruenz der Regelungen, die für die Rechtspraxis in aller Regel keinen Unterschied begründen kann.

Zu Frage II. 3.

Zu § 26 BDSG

Der zunehmende Einsatz Künstlicher Intelligenz (KI) wird auch Auswirkungen auf Beschäftigungsverhältnisse und die dabei anfallende Datenverarbeitung haben. Daraus folgt die Frage, ob die Regelung des technikneutral formulierten § 26 BDSG dieser technologischen Entwicklung Stand halten kann. Für alle Erlaubnistatbestände des § 26 Abs. 1 BDSG ist das Merkmal der Erforderlichkeit für die Zweckerreichung der zentrale Maßstab für die Rechtmäßigkeit der Datenverarbeitung. Für die Beurteilung der Erforderlichkeit kann auf die zu § 32 BDSG a.F. entwickelten Grundsätze zurückgegriffen werden, da mit § 26 als Fortführung des § 32 BDSG a.F. seine richterrechtliche Ausprägung und mithin das Kriterium der Erforderlichkeit bewusst erhalten blieb. Erforderlich ist die Datenverarbeitung zur Informationsgewinnung nur, wenn ein berechtigtes, billigenswertes und schutzwürdiges Interesse des Arbeitgebers an der Beantwortung seiner Fragen bzw. der sonstigen Informationsbeschaffung besteht und das Interesse des Arbeitsnehmers an der Geheimhaltung der Daten das Interesse des Arbeitgebers an ihrer Erhebung nicht überwiegt. Zum jetzigen Zeitpunkt ist

die Verarbeitung personenbezogener Daten beim Einsatz von KI im Beschäftigungsverhältnis ausreichend reguliert.

Zu § 30 BDSG

Weder DS-GVO noch BDSG definieren das in § 31 Abs. 2 BDSG enthaltene Tatbestandsmerkmal „Auskunftei". Da § 30 Abs. 1 BDSG bereits die Definition einer Auskunftei enthält,

> *„Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert […]",*

könnte der Gesetzgeber allein durch die bloße Ergänzung des Zusatzes „(Auskunftei)" hinter dem Wort „verändert" eine Legaldefinition des Tatbestandsmerkmals „Auskunftei" schaffen, auf die sich Rechtsanwender des § 31 BDSG de lege ferenda berufen könnten.

III. Datenschutzbeauftragte öffentlicher und nichtöffentlicher Stellen

Zu Frage III. 1.

Der Gesetzgeber hat sich entschieden, Benennung, Rechtsstellung und Aufgaben behördlicher Datenschutzbeauftragter in der Bundesverwaltung im Anwendungsbereich der DS-GVO, der Richtlinie (EU) 2016/680 und für die Bereiche außerhalb des Unionsrechts (z.B. für die Nachrichtendienste) einheitlich auszugestalten. Die §§ 5 bis 7 BDSG enthalten insofern einheitliche Regelungen zum Datenschutzbeauftragten für sämtliche öffentliche Stellen des Bundes. Für den Bereich der Richtlinie (EU) 2016/680 wird dabei im Sinne einer einheitlichen Regelung zum Teil über deren Vorgaben hinausgegangen.

Soweit der Anwendungsbereich der DS-GVO betroffen ist, stellt sich die Frage, ob die gewählte Regelungstechnik mit dem vom EuGH aufgestellten sog. Wiederholungsverbot vereinbar ist (vgl. dazu Heidelberger Kommentar/*Jaspers/Reif*, Art. 37 DS-GVO Rn. 6 ff.). Aus Perspektive der Rechtsanwender ist eine einheitliche Regelung jedenfalls begrüßenswert.

§ 7 Abs. 1 S. 2 BDSG bestimmt, dass im Fall eines bei einem Gericht bestellten Datenschutzbeauftragten sich dessen Aufgaben nicht auf das Handeln im Rahmen der justiziellen

Tätigkeit beziehen. Diese Regelung ist geglückter als die entsprechende DS-GVO-Regelung in Art. 37 Abs. 1 lit. a. Die nationale Regelung trägt dem Umstand Rechnung, dass der europäische Gesetzgeber tatsächlich wohl nicht die Benennungspflicht von Gerichten einschränken, sondern nur der Aufgabenbereich der dort tätigen Datenschutzbeauftragten auf Bereiche außerhalb der justiziellen Tätigkeit beschränken wollte.

Zu Irritationen führt allerdings die Einleitung der nationalen Regelung in § 7 BDSG: „Der oder dem Datenschutzbeauftragten obliegen neben den in der Verordnung (EU) 679/2016 genannten Aufgaben zumindest folgende Aufgaben: …". Der Gebrauch der Formulierung „neben den in der Verordnung (EU) 679/2016 genannten Aufgaben" legt nahe, durch § 7 BDSG würden über Art. 39 DS-GVO hinausgehende Aufgaben des Datenschutzbeauftragten begründet, was aber nicht intendiert ist. Die genannte Formulierung sollte ersatzlos gestrichen werden.

Zu Frage III. 2. a) und b)

Datenschutzbeauftragte stellen die effektivste und kostengünstigste Lösung für Wirtschaft und Staat dar, um die Einhaltung datenschutzrechtlicher Vorgaben bei privaten wie öffentlichen datenverarbeitenden Stellen zu gewährleisten. Datenschutzbeauftragte sind aktive Berater in der Weise, dass sie an der Legalisierung legitimer Verarbeitungen mitwirken und Lösungswege aufzeigen. Sie unterstützen bei konkreten datenschutzrechtlichen Fragen, Prozesseinführungen bzw. -änderungen und bringen hierbei ihre Expertise hinsichtlich der konkreten betrieblichen Prozesse und Gegebenheiten ein. Dies vermögen die staatlichen Aufsichtsbehörden angesichts fehlender betrieblicher Kenntnisse und personeller Ressourcen nicht zu gewährleisten.

Der personelle bzw. finanzielle Aufwand, der mit der Benennung eines Datenschutzbeauftragten verbunden ist, ist dabei im Grundsatz selbst für kleinere Unternehmen verhältnismäßig, denn solchen Stellen reicht typischerweise ein (interner) Teilzeitdatenschutzbeauftragter bzw. ein externer Datenschutzbeauftragter, der mit einem überschaubaren Tageskontingent pro Jahr zum Einsatz kommt. Ohnedies gilt das Prinzip: „Somebody has to do the job". Auch ohne Datenschutzbeauftragten entfällt die Pflicht zur Einhaltung datenschutzrechtlicher Vorgaben nicht. Fachabteilungen bzw. -bereiche sind dann vielmehr mit dieser Verantwortung auf sich allein gestellt und müssen sich die notwendige Expertise vollumfänglich selbst aneignen, da die fachkundige Unterstützung durch den Datenschutzbeauftragten fehlt. Dies führt i.d.R. zu erheblichem Mehraufwand gegenüber dem zentral

verfügbaren Know-how des Datenschutzbeauftragten. Es ist folglich eine Fehlvorstellung anzunehmen, mit der Erhöhung des Schwellenwerts für die Benennung von Datenschutzbeauftragten sei für KMU eine wesentliche Entlastung zu erreichen.

Stattdessen zeigt die Erfahrung der GDD und auch eine aktuelle Untersuchung der Ruhr-Universität Bochum (https://t1p.de/itoy), dass im Falle der Nichtbenennung eines Datenschutzbeauftragten oft niemand die Überwachung und Beratung hinsichtlich der Datenschutzpflichten wahrnimmt. Dies ist nicht nur aus Sicht der Personen kritisch, deren personenbezogene Daten verarbeitet werden. Angesichts der immensen Bußgeldrahmen der DS-GVO ist dies auch für die Unternehmen selbst riskant, denn Datenschutzbeauftragte helfen auch bei der Reduzierung von Unternehmensrisiken.

Zusammenfassend lässt sich festhalten, dass aus unserer Sicht keine wesentlichen Erleichterungen mit der Änderung des § 38 Abs. 1 Satz 1 BDSG einhergegangen sind und durch eine Änderung des Schwellenwerts für die Benennung von Datenschutzbeauftragten auch gar nicht zu erreichen sind, weil sich hierdurch an den europarechtlich vorgegebenen datenschutzrechtlichen Pflichten, die im Grundsatz für alle Unternehmen und Vereine gelten, nichts ändert. Hilfestellung für kleine Organisationen und Vereine lassen sich zusätzlich dadurch erreichen, dass die zuständigen Stellen Orientierungshilfen, Muster und Standards veröffentlichen, die auf deren praktische Bedürfnisse zugeschnitten sind.

IV. Zusammenarbeit, Zuständigkeiten und Befugnisse der Aufsichtsbehörden

Zu Fragen IV. 1. und 2.

Unterschiedliche Rechtsauffassungen der Datenschutzaufsichtsbehörden und eine verschiedene Vollzugs- und Bußgeldpraxis führen zu einer praktisch erheblichen Ungleichbehandlung von datenverarbeitenden Stellen. Dies wirkt sich insbesondere für Unternehmen aus, die personenbezogene Daten verarbeiten, denn aus deren Sicht begründet die unterschiedliche Behandlung ggf. auch einen Wettbewerbsvorteil bzw. -nachteil im Vergleich zu Konkurrenzunternehmen in anderen Bundesländern.

Zwar ist seit Inkrafttreten der DS-GVO im Jahr 2016 eine deutlich stärkere Koordinierung der Aufsichtsbehörden festzustellen als zuvor. Festzustellen ist aber auch, dass gemeinsame Verlautbarungen sich primär auf unter den Behörden unstreitige Fragestellungen

beziehen. Sofern zu Fragestellungen kein Konsens erzielt werden kann, gibt es keine gemeinsame Positionierung oder der Disput wird, wie zuletzt im besonders praxisrelevanten Fall des Einsatzes von Microsoft Office 365 (https://www.lda.bayern.de/meia/pm/20201002_office365.pdf), sogar öffentlich ausgetragen.

Es sprechen gleichwohl gewichtige Gründe gegen eine zentrale Datenschutzaufsicht und für eine Beibehaltung der aktuellen Strukturen. So können von dezentralen Strukturen insbesondere kleine und mittlere Unternehmen profitieren, denn eine zentrale Aufsicht wird für Unternehmen dieser Größenordnung nicht im gleichen Maße ansprechbar sein. Ohnedies ist der Datenschutz ein gesamteuropäisches Thema und eine Vereinheitlichung muss primär auf dieser Ebene erfolgen, also über den Europäischen Datenschutzausschuss (EDSA). Vor allem perspektivisch, d.h. mit zunehmender Konkretisierung der DS-GVO-Vorgaben durch den EDSA dürfte die nationale Aufsichtsstruktur daher eher untergeordnete Bedeutung haben.

Um das für den Übergang aber durchaus noch virulente Problem der unterschiedlichen nationalen Aufsichtspraxis in den Griff zu bekommen, sollte die Zusammenarbeit der nationalen Behörden stärker formalisiert werden, insbesondere ein Mechanismus zum Treffen von verbindlichen Beschlüssen in Konfliktfragen vergleichbar dem Kohärenzverfahren auf europäischer Ebene (Artt. 63, 65 DS-GVO) bzw. dem Verfahren nach § 18 BDSG (Zusammenarbeit der nationalen Aufsichtsbehörden in Angelegenheiten der Europäischen Union) eingeführt werden.

Zu Fragen IV. 3.

Der zu einer innerstaatlichen Zuständigkeitskonzentration führende § 40 Abs. 2 BDSG hat sich aus Sicht der GDD grundsätzlich bewährt. Die Bestimmung führt zu mehr Rechtssicherheit im Hinblick auf die Aufsichtszuständigkeit sowie zur Entlastung von Unternehmen wie Behörden.

V. Betroffenenrechte

Zu Frage V. 1.

Zu § 32 BDSG

Die Pflicht zur Information gem. Art. 13 Abs. 1 DS-GVO erscheint über die in § 32 BDSG genannten Fällen hinaus auch in Situationen nicht automatisierter Verarbeitung personenbezogener Daten entbehrlich, in denen die Verarbeitung

- ausschließlich zur Vertragsdurchführung/-anbahnung oder zur Erfüllung rechtlicher Pflichten (z.B. Aufbewahrungsvorschriften) erfolgt und
- Verantwortliche keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 verarbeiten (z.B. handschriftliche Rechnung im Blumenladen/in der Bäckerei).

Auch unter Abstellung auf den Erwartungshorizont der betroffenen Personen wird man unterstellen können, dass diese in typischen Verkaufssituationen grundsätzlich mit entsprechenden Verarbeitungen ihrer personenbezogenen Daten rechnen.

Dass die Vorhersehbarkeit einer Datenverarbeitung direkten Einfluss auf deren rechtliche Beurteilung hat, zeigt auch der in Erwägungsgrund Nr. 47 S. 3 und 4 DS-GVO im Zusammenhang mit Art. 6 Abs. 1 lit. f DS-GVO geäußerte Gesichtspunkt der „reasonable expectations of privacy“. Die Reduktion des Formalismus im alltäglichen Datenschutz wäre auch eine geeignete Maßnahme, um die Akzeptanz des Datenschutzes zu erhöhen.

Zu § 35 BDSG

Aus technischen Gründen ist bei Einsatz bestimmter am Markt verfügbarer Datenbanksysteme derzeit faktisch keine Löschung von Datensätzen möglich, ohne dass hierdurch u.U. die Konsistenz der gesamten Datenbank gefährdet wird.

Aufgrund der sich aus den Datenschutzvorschriften ergebenden Verpflichtung, bei Vorliegen bestimmter Voraussetzungen personenbezogene Daten zu löschen, folgt insoweit, dass in vielen Betrieben, die diese Datenbanken einsetzen, derzeit seitens der Verantwortlichen unverschuldet illegale Zustände bestehen, die diese nicht ohne unzumutbaren Aufwand selbst beseitigen können.

Softwarehersteller sind angesichts der gesetzlichen Anforderungen gehalten, entsprechende Funktionalitäten in ihren Datenbanken nachzurüsten. Bis Verantwortliche jedoch diese teils noch ausstehenden Produktnachbesserungen implementieren konnten, erscheint es aus Sicht der GDD geboten, die in § 35 BDSG bislang auf „nicht automatisierte Datenverarbeitung“ begrenzte Befugnis, unter den Voraussetzungen des § 35 Abs. 1 BDSG

anstelle der Löschung personenbezogener Daten eine Einschränkung ihrer Verarbeitung (Art. 18 DS-GVO) vorzunehmen, auch auf Fälle automatisierter Verarbeitung zu erstrecken.

VI. Haftung und Sanktionen

Zu Frage VIII. 1.

Zu § 41 BDSG

Wegen des deutlich erhöhten Bußgeldrahmens im Vergleich zur früheren Rechtslage ist Art. 83
DS-GVO eine der bedeutsamsten Normen der DS-GVO. Da es auf Unionsebene kein allgemeines Ordnungswidrigkeitenrecht gibt, was konkretisierend zur Verhängung von Bußgeldern bei Datenschutzverstößen nach Art. 83 DS-GVO hinzugezogen werden könnte, ist es konsequent, das deutsche Gesetz über Ordnungswidrigkeiten (OWiG) für anwendbar zu erklären (§ 41 Abs. 1 S. 1 BDSG).

Das OWiG enthält Regelungen sowohl hinsichtlich der Zurechnung von Verstößen gegenüber juristischen Personen (§ 30 OWiG) als auch zur Frage nach der Verhängung von Bußgeldern ggü. handelnden Akteuren, wie etwa Stellvertretern oder Betriebsinhabern (§§ 9, 130 OWiG). Gegen Unternehmen kann nach geltendem deutschen Recht kein Bußgeld verhängt werden, wenn nicht die Voraussetzungen des § 30 oder § 130 OWiG erfüllt sind. Die reine Feststellung eines Datenschutzverstoßes reicht nicht aus, um ein Bußgeld gegen das Unternehmen zu verhängen. Die Sanktionierung des Unternehmens setzt zusätzlich voraus, dass das Unternehmen für diesen Verstoß auch verantwortlich ist. Von großer praktischer Bedeutung ist daher zu konkretisieren, welche Grundlagen die Sanktionierung bestimmen, wenn der datenschutzrechtlich Verantwortliche bzw. Auftragsverarbeiter eine juristische Person ist. Dafür bedarf es der Klarstellung, ob die DS-GVO die Durchführung des Bußgeldverfahrens und mithin die Zurechnung von Verstößen selbst regelt oder eine Konkretisierung durch den nationalen Gesetzgeber zulässig erscheint oder gar zu erfolgen hat.

Zu § 43 BDSG

§ 43 Abs. 4 BDSG bestimmt, dass die verpflichtende Meldung einer Datenschutzverletzung nach Art. 33 f. DS-GVO nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden gegen diesen oder seine Angehörigen (§ 52 Abs. 1 StPO) verwendet werden darf. Die Regelung entspricht europarechtlich gebotenen Verfahrensgarantien und korrespondiert mit der sich aus dem höherrangigen Europarecht ergebenen Schutzwirkung. Soweit Verantwortliche sich selbst bezichtigen müssten, würde dies gegen die GRCh, die EMRK wie auch gegen § 43 BDSG verstoßen. Im Ergebnis darf der unmittelbare Meldegegenstand nach Art. 33 f. DS-GVO nicht sanktioniert werden und vor allem nicht zu einer Geldbuße führen. Da Meldungen nach Art. 33 f. DS-GVO in der Vergangenheit Anlass für die Einleitung von Bußgeldverfahren waren, ist die Regelung in § 43 Abs. 4 BDSG von besonderer Bedeutung und sollte beibehalten werden.

Bonn, den 11.01.2021

Gesellschaft für Datenschutz und Datensicherheit e.V.
Heinrich-Böll-Ring 10, 53119 Bonn
info@gdd.de | www.gdd.de