



Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD e.V. Heinrich-Böll-Ring 10 53119 Bonn

Landtag Nordrhein-Westfalen (NRW)
Platz des Landtags 1
40221 Düsseldorf

Via Mail: anhoerung@landtag.nrw.de

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

**STELLUNGNAHME
17/488**

Alle Abg

Bonn, 06.04.2018

Schriftliche Stellungnahme zum Gesetzesentwurf zur Anpassung des allgemeinen Datenschutzrechtes an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Drs. 17/1981)

Bezugnehmend auf Ihr Schreiben vom 19.3.2018 nimmt die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) zum Gesetzesentwurf zur Anpassung des allgemeinen Datenschutzrechtes an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Drs. 17/1981) wie folgt Stellung:

I. Bedarf einer nationalen Gesetzgebung

Zur Anpassung an die EU-Datenschutz-Grundverordnung (DS-GVO) sind nationale Regelungen weiterhin möglich und zum Teil sogar verpflichtend vorgeschrieben. Überdies begründet die umzusetzende Richtlinie (RL) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI (JIRL) einen legislativen Handlungsbedarf. Diese Form des Rechtsakts verlangt automatisch die Implementierung im nationalen Recht. Nach Art. 63 JIRL sind die der RL unterfallenden Staaten verpflichtet, die einzelstaatlichen Rechts- und Verwaltungsvorschriften zur Umsetzung der RL zu erlassen. Der Landesgesetzgeber kommt mit dem vorliegenden Gesetzentwurf dieser Pflicht nach und versucht den eröffneten Gestaltungsrahmen zu nutzen. Dies ist zu begrüßen.

Das Ziel der DS-GVO ist die Vollharmonisierung der Regelungen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten der Europäischen Union (EU). Diese Zielvorgabe kann jedoch mit der DS-GVO nicht vollumfänglich erreicht werden. Zwar stellt die Grundverordnung unmittelbar anwendbares Datenschutzrecht dar, gleichwohl sind die Mitgliedstaaten an vielen Stellen weiterhin in der Pflicht nationale Regelungen vorzusehen. Dies gilt im Besonderen für die Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt

GDD e.V.

T +49 228 96 96 75 00

F +49 228 96 96 75 25

info@gdd.de

www.gdd.de

Vorstand

Prof. Dr. Rolf Schwartmann
(Vorsitzender)

Dr. Dirk Bornemann

Barbara Broers

Harald Eul

Prof. Dr. Rainer W. Gerling

Gabriela Krader

Prof. Dr. Michael Meier

Thomas Müthlein

Prof. Dr. Gregor Thüsing

Dr. Martin Zilkens

Prof. Peter Gola

(Ehrevorsitzender)

Geschäftsführer

Andreas Jaspers,

Rechtsanwalt

Bankverbindungen

Postbank Köln, BLZ: 370 100 50, Konto-Nr.: 179 49 45 01, IBAN: DE24 3701 0050 0179 494501, BIC: PBNKDEFF

Sparkasse KölnBonn, BLZ: 370 501 98, Konto-Nr.: 19 00 78 12 69, IBAN: DE49 3705 0198 1900 7812 69, BIC: COLSDE33



erfolgt. So gesehen, stellt die DS-GVO eine „hinkende Verordnung“ oder einen Hybrid aus Richtlinie und Verordnung dar.

II. Grenzen der nationalen Gesetzgebung

Bei der nationalen Ausgestaltung und Anpassung an das EU-Datenschutzrecht sollten die Grenzen des legislativen Gestaltungsspielraums bekannt sein. Für die Unionsmitglieder gilt es bei Nutzung der Öffnungsklauseln innerhalb der Regelungsdichte der DS-GVO zu verbleiben. Die Öffnungsklauseln der DS-GVO determinieren maßgeblich den Rahmen für den nationalen Gestaltungsspielraum. Innerhalb dieser Regelungsgrenzen besteht eine Zulässigkeit und mitunter eine Pflicht zur Konkretisierung und Spezifizierung in Form von zu erlassendem Recht. Die Vereinbarkeit mit dem Unionsrecht bei der Ausgestaltung der Öffnungsklausel hängt entscheidend davon ab, wie sich das Verhältnis zwischen der unmittelbar geltenden DS-GVO und den nationalen Bestimmungen darstellt. Hierzu ist das sekundärrechtliche Schutzniveau als Maßstab für einzelstaatliche Vorschriften zu würdigen. Die Ausfüllung von Öffnungsklauseln soll das von der DS-GVO ausgehende Schutzniveau nicht erhöhen, sondern konkretisierenden und spezifizierenden Charakter haben, der zu keinen Abweichungen des übergeordneten supranationalen Rechts führt. Kollidieren nationale und europäische Regelungen, so gilt ein Anwendungsvorrang des Unionsrechts vor nationalem Recht.

Eine weitere Grenze stellt der Regelungsbereich der DS-GVO dar. Solange eine unionsrechtliche Vorschrift einen Sachverhalt nicht abschließend regelt, können auch nationale Regelungen bestehen bleiben und insbesondere auch eigene Vorgaben erlauben. Schließlich mangelt es der EU u. a. auch an der Kompetenz, um beispielsweise Bereiche wie den Gesundheits- oder Beschäftigtendatenschutz selbst abschließend regeln zu können. Die Mitgliedstaaten müssen hier den ihnen verbleibenden Gestaltungsspielraum durch den Erlass von Datenschutzbestimmungen nutzen. Danach ergibt sich die Gesetzgebungskompetenz der Länder im Datenschutzrecht im Besonderen für den Bereich des Rundfunks oder innerhalb der klassischen Landesmaterien des Polizei-, Kommunal- und Schulrechts, aber auch im Gesundheitswesen. Außerhalb des Regelungsbereichs der DS-GVO ist ein Konflikt zwischen europäischem und nationalem Recht ausgeschlossen.

Für den Datenschutz der nicht-öffentlichen Stellen besitzen die Länder grundsätzlich keine Gesetzgebungskompetenz. Diese liegt allein beim Bundesgesetzgeber.

Da die Grenzen des legislativen Gestaltungsspielraum insgesamt nicht klar konturiert sind, können Regelungslücken und nicht mit Unionsrecht vereinbarende Vorschriften die Folge sein. Für den Landesgesetzgeber gilt es daher solche Kollisionen zu vermeiden. Auch im Sinne der praktikablen Rechtsanwendung sollten widersprüchliche Regelungen vermieden werden, um nicht noch mehr Rechtsunsicherheit bei der Verarbeitung personenbezogener Daten zu erzeugen.

III. Regelungsgeflecht ab Mai 2018

Auch nach der EU-Datenschutzreform mit der unmittelbar anwendbaren DS-GVO im Zentrum bleibt das Datenschutzrecht ein Regelungsgeflecht. Das Zusammenspiel der verschiedenen Datenschutzregime ist komplex. Sowohl von Seiten der EU-Ebene, der



Bundesebene und der Landesebene gibt es Datenschutzregelungen. Durch das gesamte Mehrebenensystem hindurch verläuft zusätzlich die Differenzierung zwischen allgemeiner datenschutzrechtlicher und bereichsspezifischer Regelung. Diese Differenzierung schlägt sich auch auf den vorliegenden Gesetzesentwurf nieder, wonach die Art. 2-10 eine Anpassung des Fachrechts mit Datenschutzbezügen zur Folge haben.

Da vom Landesrecht nicht geregelt, entfällt zumindest eine Unterscheidung zwischen Vorschriften für die Datenverarbeitung durch öffentliche und nicht-öffentliche Stellen als weitere Komplexität innerhalb des Regelungsgeflechts.

IV. Ausgewählte Regelungsbereiche in Art. 1

Aufgrund des Umfangs des Gesetzesentwurfs sind die Ausführungen auf ausgewählte Regelungsbereiche des Gesetzesentwurfes beschränkt.

Zu § 4:

Zusätzlich zu den in Art. 4 DS-GVO enthaltenen Begriffsbestimmungen sieht der Gesetzesentwurf mit § 4 eine weitere Legaldefinition vor. Eine Definition der "Anonymisieren" erscheint zwar wünschenswert, doch es ist nicht offenkundig, inwiefern eine Befugnis besteht, zusätzlich zur DS-GVO weitere Begriffe landesgesetzlich zu definieren. Verfahren der Anonymisierung kommen in der Praxis zweifellos vor. Schlussendlich betreibt der Landesgesetzgeber hier keine nationale Gesetzgebung innerhalb des Anwendungsbereichs der DS-GVO, denn „diese Verordnung betrifft nicht die Verarbeitung solcher anonymer Daten“ (ErwG. 26 DS-GVO).

Zu § 5 Abs. 6:

Im Sinne der Schaffung eines einheitlichen Schutzniveaus innerhalb der EU (ErwG. 10 DS-GVO) ist es zu begrüßen, dass der Anwendungsbereich auf alle bisher dem DSGVO NRW a.F. unterstehenden öffentlichen Stellen erstreckt wird, selbst wenn deren Tätigkeit nicht originär dem Anwendungsbereich der DS-GVO unterfällt.

Zu § 9 Abs. 1:

Diese gesetzgeberische Tätigkeit ist dahingehend zu begrüßen, dass von den in Art. 6 Abs. 2 und 3 DS-GVO bestehenden Befugnissen Gebrauch gemacht wird. Das Sekundärrecht erlaubt den Mitgliedstaaten in dem gesetzten Rahmen, Datenschutzvorschriften in Bezug auf die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder öffentlicher Aufgaben zu erlassen. Mit § 9 Abs. 1 schafft der Landesgesetzgeber zur DS-GVO zusätzliche Rechtmäßigkeitstatbestände, die für die öffentliche Verarbeitung personenbezogener Daten nötig erscheinen.



Zu § 11:

In Ermangelung einer unionalen Regelungskompetenz, obliegt es allein den Mitgliedsstaaten Beschränkungen der Betroffenenrechte mit Blick auf die öffentliche Sicherheit und die Abwehr von Gefährdungen vorzunehmen. So erlaubt Art. 23 DS-GVO Beschränkungen von Transparenzrechten Betroffener gesetzlich zu regeln. Der Erlass von entsprechendem Landesrecht ist zu begrüßen, um eine bedingungslose Informationsgewährung im Sinne der Art. 13 und 14 DS-GVO dort zu vermeiden, wo die staatliche Aufgabenerfüllung gegenüber der transparenten Datenverarbeitung vorrangig ist. Gleichwohl wird die grundsätzliche Anforderung an eine transparente Datenverarbeitung damit nicht obsolet. Jede nach Art. 23 Abs. 1 DS-GVO zulässige Beschränkungsregelung muss formellen, aber vor allem materiellen Anforderungen, wie entsprechenden kompensatorischen Maßnahmen, genügen.

Im vorliegenden Gesetzesentwurf ist eine Beschränkung der Informationspflicht nach Art. 23 DS-GVO zulässigerweise vorgesehen. Der legislative Gestaltungsspielraum erlaubt dem Gesetzgeber aber nicht nur die Informationspflicht nach Art. 13 Abs. 3 und Art. 14 Abs. 1, 2 und 4 DS-GVO zu beschränken. Vielmehr kann die Informationspflicht nach Art. 13 und 14 DS-GVO insgesamt unter den Voraussetzungen des Art. 23 Abs. 1 DS-GVO beschränkt werden. So sieht es etwa auch die Freie und Hansestadt Hamburg in ihrem Entwurf zum Hamburgisches Datenschutzgesetz (§ 15) oder der Freistaat Thüringen in seinem Entwurf zum Thüringer Datenschutzgesetz (§ 20) vor. Mit Blick auf denkbare Beispiele wie die Bekämpfung von Bränden, Umweltkatastrophen oder Notarzteinsätzen zeigt sich, dass in solchen Fällen die Informationserteilung in Gänze zurücktreten kann und nicht nur unter den Bedingungen des Art. 13 Abs. 3 DS-GVO. Es sollte überdacht werden, ob diesen Beispielen im Sinne der praktikablen Informationsgewährung öffentlicher Stellen bei der Erfüllung ihrer Aufgaben nicht gefolgt werden soll.

Zu §§ 15 und 16:

Die Vorschriften dienen als Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten und füllen Art. 9 Abs. 2 DS-GVO aus. Diese gesetzgeberische Tätigkeit ist dahingehend zu begrüßen, dass von den in Art. 9 DS-GVO bestehenden Öffnungsklauseln Gebrauch gemacht wird.

Zu § 18:

Mit § 18 zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses beabsichtigt der Landesgesetzgeber die Öffnungsklausel des Art. 88 DS-GVO auszufüllen. Da dieser Bereich von der EU aufgrund mangelnder Kompetenz auch nicht vereinheitlicht geregelt werden kann, ist es außerordentlich begrüßenswert, dass der Landesgesetzgeber von seiner Möglichkeit Gebrauch macht und die Datenverarbeitung im Beschäftigungskontext selbstständig regelt.



Zu § 20:

Die Vorschrift orientiert sich stark an § 4 BDSG-neu. Die Länder regeln die Voraussetzungen für die Videoüberwachung öffentlich zugänglicher Räume durch öffentliche Stellen des Landes, der Gemeinden oder Landkreise zum Zweck der Aufgabenerfüllung der jeweiligen öffentlichen Stelle, zur Wahrnehmung des öffentlichen Hausrechts, zum Schutz des Eigentums oder Besitzes oder zur Kontrolle von Zugangsberechtigten. Dabei verzichtet der Gesetzesentwurf sinnvollerweise auf die Exklusivität der Rechtsgrundlage für die Videoüberwachung, indem nicht die Verwendung „ist nur zulässig, wenn“ benutzt wird, sondern stattdessen von „ist zulässig, wenn“ gesprochen wird.

In Hinsicht auf die Transparenz geht der Gesetzgeber den einzig praktikablen Weg der gestuften Informationsgewährung. Er bewertet neben der Videoüberwachung selbst, die Angaben nach Art. 13 Abs. 1 lit. a (Verantwortlicher und Vertreter), lit. b (ggf. bestellter Datenschutzbeauftragter) und lit. c (Zwecke und Rechtsgrundlage) als Informationen der 1. Stufe. Bei dieser Regelung handelt es sich der Gesetzesbegründung nach nicht um eine denkbare Beschränkung der Informationspflicht nach Art. 23 DS-GVO, sondern um eine spezifische Bestimmung der Transparenz. Komplementär dazu ist darauf hinzuweisen, wo die betroffenen Personen die weiteren Informationen nach Art. 13 DS-GVO erhalten können, um den unionsrechtlichen Anforderungen zu entsprechen.

Zu § 24:

Der Landesgesetzgeber regelt mit § 24, dass bei der Einführung neuer Verarbeitungsvorgänge eine (erneute) Datenschutz-Folgenabschätzung durch die jeweilige öffentliche Stelle nichtdurchgeführt werden soll, sofern eine solche Überprüfung bereits durch die oberste Landesbehörde für wesensgleiche Verfahren durchgeführt wurde. Durch diese Möglichkeit sollen die Behörden und öffentlichen Stellen entlastet und ein ökonomisches Arbeiten gewährleistet werden. Der Ordnungsgeber sieht die Vermeidung doppelter Datenschutz-Folgenabschätzung für solche Fälle, in den bereits eine Datenschutz-Folgenabschätzung erfolgte, ausdrücklich vor. Für den praktikablen Umgang mit dem Schutz personenbezogener Daten ist diese Regelung ausdrücklich zu begrüßen.

Zu § 25:

Dem in der DS-GVO verfassten und von der Unionsgerichtsbarkeit bestätigten Gedanken der völligen Unabhängigkeit der Aufsichtsbehörden muss der Landesgesetzgeber Folge leisten. Für die Errichtung jeder Länderaufsicht sind nach Art. 54 Abs. 1 lit. a DS-GVO entsprechende Rechtsvorschriften zu erlassen. Damit ist den Landesgesetzgebern aufgrund der nach Art. 51 Abs. 1 i. V. m Abs. 3 DS-GVO zulässigen föderalen Aufsichtsstruktur ein obligatorischer Regelungsauftrag auferlegt. Innerhalb dessen besitzen die Länder einen, wenn auch nur eng begrenzten, Spezifizierungsspielraum. Das zeigt sich daran, dass die meisten Bundesländer gleichermaßen wie der Bund ihrer Aufsicht aufgrund der Vereinbarkeit mit unionsrechtlichen Vorgaben die Rechtsstellung einer obersten Landesbehörde verleihen. So sieht es der Entwurf mit § 25 Abs. 2 S. 3 auch für NRW vor.



Das von Art. 54 Abs. 1 lit. b DS-GVO ausgehende Regelungsgebot erstreckt sich auch auf die sonstigen Voraussetzungen für die Ernennung als Landesdatenschutzbeauftragten. Europarechtlich verlangt werden nach Art. 53 Abs. 2 DS-GVO Qualifikation, Erfahrung und Sachkunde „insbesondere im Bereich des Schutzes personenbezogener Daten“. Es erscheint ebenso rechtssicher wie angemessen die unionsrechtlichen Vorgaben, Fachkunde und Erfahrung, aus Art. 53 Abs. 2 DS-GVO in § 25 Abs. 1 S. 4 zu übernehmen. Ferner ist die kumulative Anforderung „Qualifikation“ in das einzelstaatliche Recht zu implementieren. Hierfür geht der Landesgesetzgeber den Weg „die Befähigung zum Richteramt oder zu der Laufbahngruppe 2, zweites Einstiegsamt“ zu verlangen. Fraglich ist, ob von einem künftigen Landesdatenschutzbeauftragten verlangt werden kann, dass er solche dienstrechtlichen Voraussetzungen erfüllt. Diese Spezifizierung dürfte die vom Ordnungsgeber offen gelassenen Grenzen überschreiten. Ein Ausschluss aufgrund einer laufbahnrechtlichen Anforderung erscheint nicht mit den sekundärrechtlich vorrangigen Anforderungen vereinbar. Die unionsrechtlichen Vorgaben des Art. 53 Abs. 2 DS-GVO (Qualifikation, Erfahrung und Sachkunde) können teleologisch nicht ausschließlich bei Vorliegen dienstrechtlicher Anforderung erfüllbar sein.

Die DS-GVO wird nicht zum Anlass genommen, die Einordnung des Landesbeauftragten für den Datenschutz dahingehend zu ändern, dass er ab dem 25. Mai aus dem Beamtenverhältnis ausscheidet. Im Sinne der Unabhängigkeit des Landesbeauftragten ist dies zu begrüßen.

Von Bedeutung wird der Aspekt des Anstellungsverhältnisses auch bei der Ausgestaltung der in Art. 54 Abs. 2 S. 2 DS-GVO normierten Verschwiegenheitspflicht durch die Länder. Sind die Behördenleiter verbeamtet, ergibt sich die Verschwiegenheitspflicht grundsätzlich aus den Landesbeamtenengesetzen. Damit ist keine weitere Regelung im Landesdatenschutzgesetz in dieser Hinsicht erforderlich.

Zu § 31 Abs. 1:

Mit Rücksicht auf eine effiziente organisatorische Ausgestaltung der Funktion der behördlichen Datenschutzbeauftragten ist die gesetzlich erlaubte Bestellung eines Stellvertreters oder auch mehrerer Stellvertreter sehr begrüßenswert. Eine solche Stellvertretung kann die oder den Datenschutzbeauftragten bei zeitweiliger Abwesenheit wie etwa während des Urlaubs, einer Dienstreise oder bei Erkrankungen vertreten.

Zu § 32:

Da sich die EU-Mitgliedstaaten hinsichtlich der Möglichkeit Bußgelder gegen öffentliche Stellen zu verhängen nicht einigen konnten, findet sich mit Art. 83 Abs. 7 DS-GVO eine Öffnungsklausel in der Grundverordnung wieder. Dieser Ausgestaltungsspielraum gewährt in Deutschland neben dem Bund auch den Ländern das Recht Vorschriften dafür festzulegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen Geldbußen verhängt werden können.



Die Regelung nach § 32, keine Bußgelder gegen öffentliche Stellen auszusprechen, erstreckt sich nicht auf öffentlich-rechtliche Unternehmen, die im Wettbewerb mit anderen Verarbeitern stehen. Ansonsten erhielten diese gegenüber ihren Wettbewerbern einen Vorteil. Mit der vorgesehenen Regelung ist diese Besserstellung sinnvollerweise ausgeschlossen.

Zu § 33:

Das nationale Recht kann nur Bußgeldvorschriften innerhalb des vom Verordnungsgeber überlassenen Bereichs, der von der für die Geldbußen ausschließlich geltenden Öffnungsklausel (Art. 83 Abs. 7 DS-GVO) geregelt ist, implementieren. Art. 84 DS-GVO kann nicht als Grundlage für anderweitige Bußgeldtatbestände im einzelstaatlichen Recht herangezogen werden. Es ist daher nicht mit dem Unionsrecht vereinbar Bußgeldtatbestände gegenüber Mitarbeitern von Behörden oder sonstigen öffentlichen Stellen – wie in § 33 Abs. 1 und 2 geplant – zu normieren. Dies mag zwar eine Sanktionslücke zur Folge haben, aber abseits der unionsrechtlich harmonisierten Geldbußen bei Datenschutzverstößen gem. Art. 83 DS-GVO kann das einzelstaatliche Recht keine weiteren Bußgeldregeln schaffen.

Zu § 34:

Der Landesgesetzgeber kommt mit § 34 seiner Pflicht nach, die obligatorische Öffnungsklausel des Art. 84 Abs. 1 DS-GVO auszufüllen und Sanktionen zu normieren. In Anknüpfung an die Vorläuferbestimmung (§ 33 Abs. 2 DSG NRW a. F.) fällt die Entscheidung auf strafrechtliche Rechtsfolgen. Es erscheint begrüßenswert, dass dieses Sanktionsregime keine Verschärfung erfahren hat.

Zu §§ 35-69:

Mit den §§ 35 bis 69 setzt der Landesgesetzgeber die Regelungen der JIRL gemeinsam mit den Anpassungen zur DS-GVO in einem Gesetz um. Anders als bei der DS-GVO sind die Regelungen der JIRL zwingend im einzelstaatlichen Recht zu implementieren. Gleichwohl schafft die JIRL aufgrund der Wahl ihres Rechtsaktes als RL nur eine Mindestharmonisierung der Datenschutzvorgaben innerhalb des entsprechenden Anwendungsbereichs (Art. 2 JIRL). Ziel ist ein für den Betroffenen unionsweit einheitlicher Schutz (ErwG. 15 JIRL).

V. Zu Art. 2-10

Der Gesetzesentwurf sieht mehrere Gesetzesänderungen vor. Es ist geboten neben dem allgemeinen Datenschutzgesetz überdies Anpassungen von Datenschutzbezügen im Fachrecht vorzunehmen. Die notwendigen Änderungen im Fachrecht innerhalb eines gemeinsamen Gesetzesentwurfes neben der kompletten Neugestaltung des all-



Gesellschaft für Datenschutz
und Datensicherheit e.V.

gemeinen Landesdatenschutzrechts vorzunehmen ist ebenso ambitioniert wie sinnvoll. Gleichwohl handelt es sich hierbei nur um Gesetze aus dem Zuständigkeitsbereich des Ministeriums des Innern, was einen verbleibenden Anpassungsbedarf stark vermuten lässt.

Prof. Dr. Rolf Schwartmann
Vorstandsvorsitzender der GDD e. V.

Dr. Tobias Jacquemain, LL.M.
Wiss. Referent der GDD e. V.