UNIKASSEL
VERSITÄT

Fachbereich
Wirtschaftswissenschaften

Wirtschaftsrecht

Prof. Dr. Alexander Roßnagel

Universität Kassel
Nora-Platiel-Str. 5 • D - 34109 Kassel

An den Vorsitzenden
des Hauptausschusses
des Landtags Nordrhein-Westfalen
Herrn Dr. Marcus Optendrenk

Universität Kassel
Fachgebiet Öffentliches Recht,
insb. Umwelt- und Technikrecht
Henschelstr. 2
34109 Kassel

a.rossnagel@uni-kassel.de
fon +49-561 804 3130
fax +49-561 804 3737

Sekretariat: Edith Weise
fon +49-561 804 2874

13. April 2018

Schriftliche Stellungnahme zur öffentlichen Anhörung des Hauptausschusses des Landtags Nordrhein-Westfalen am 19. April 2018 zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU – NRWDSAnpUG-EU) (Drs. 17/1981)

Aus Zeitgründen kann nur zum Entwurf eines Landesdatenschutzgesetzes Stellung genommen werden, soweit dieser der Anpassung des allgemeinen Datenschutzrechts an die Datenschutz-Grundverordnung dient.

A. Zum Gesetzentwurf allgemein

Unabhängig von einzelnen Regelungen fallen an dem Entwurf drei Aspekte auf, die kritisch anzumerken sind.

1. Modernisierung des Datenschutzrechts?

Die Datenschutz-Grundverordnung verfolgt zwar das Ziel, das Datenschutzrecht angesichts der Herausforderungen der raschen technologischen Entwicklungen und der Globalisierung der Informationstechnikanwendungen zu modernisieren und den Schutz der Grundrechte zu verbessern (Erwägungsgründe 1, 2 und 4 DSGVO). Sie regelt jedoch keine einzige dieser Herausforderungen. Sie verfehlt ihr Modernisierungsziel vor allem durch ihren sehr spezifischen Ansatz der Technikneutralität. Diese ist sinnvoll, wenn sie verhindern soll, dass rechtliche Vorschriften technische Weiterentwicklungen ausschließen. Die Datenschutz-Grundverordnung übertreibt jedoch die Technikneutralität und nutzt sie in einem Sinn, dass sie im Ergebnis eine Risikoneutralität der Datenschutzvorschriften bewirkt: Keine Regelung greift die spezifischen Grundrechtsrisiken z.B. von smarten Informationstechniken im Alltag, von Smart Cars, Smart Health, Smart Homes, Smart Cities, von Big Data, Cloud Computing oder datengetriebenen Geschäftsmodellen, Lokalisierungsdiensten, Künstlicher Intelligenz und selbstlernenden Systemen auf oder löst sie gar. Die gleichen Zulässigkeitsregeln, Zweckbegrenzungen oder Rechte der betroffenen Person gelten für die wenig riskante

Kundenliste beim „Bäcker um die Ecke“ ebenso wie für diese um Potenzen risikoreicheren Datenverarbeitungsformen. Insbesondere durch abstrakte Zulässigkeitsregelungen wie in Art. 6 Abs. 1 DSGVO werden die spezifischen Grundrechtsrisiken verfehlt.

Letztlich muss für die Rechtsanwender klar sein, welche Anforderungen das Datenschutzrecht an die Verarbeitungsvorgänge stellt. Diese Zielsetzung darf einerseits nicht dazu führen, dass die Vorschriften an technische Detailmerkmale anknüpfen, so dass sie technische Weiterentwicklungen ausschließen. Andererseits dürfen technikunspezifische Regelungen nicht dazu führen, dass der demokratisch legitimierte und zur Regelung berufene Gesetzgeber sich nicht mit den besonderen Interessenlagen und Risiken sowie passenden Lösungen einer Technikanwendung auseinandersetzt. Technikbezogene Regelungen sind gerade in einem so technikgeprägten Bereich wie dem Datenschutz unabdingbar, sollen die rechtlichen Ziele erreicht werden. Daher müssen spezifische Technikfunktionen und die typischen Verarbeitungszwecke, ihre Risiken und Lösungsansätze interessengerecht und risikoadäquat geregelt werden. Nur so kann die notwendige Rechtssicherheit und Interessengerechtigkeit erreicht werden.

Dass es im Unionsrecht sehr wohl möglich ist, sowohl technikneutrale als auch funktions- und risikobezogene Datenschutzvorgaben vorzusehen, zeigen etwa Art. 6 der eCall-VO (EU) 2015/758, der klare Datenschutzanforderungen an die Zulässigkeit des automatisierten Notrufs stellt, oder die Regelungen zur Datenverarbeitung in der elektronischen Kommunikation, zum Schutz von Endgeräten und zur Steuerung zulässiger Werbung in den Art. 6, 8 und 16 des Entwurfs einer E-Privacy-Verordnung.

Die deutschen Gesetzgeber haben bisher weder im neuen Bundesdatenschutzgesetz noch in den Entwürfen zu den neuen Landesdatenschutzgesetzen die Risikoneutralität der Datenschutz-Grundverordnung durch geeignete risikobezogene Regelungen moderner Herausforderungen überwunden. Sie haben die Öffnungsklauseln fast ausschließlich dazu benutzt, Möglichkeiten zur Verarbeitung personenbezogener Daten zu erweitern und Rechte der betroffenen Personen zu beschränken. Damit haben sie im Ergebnis das Datenschutzniveau in Deutschland sowohl gegenüber dem bisherigen Bundesdatenschutzgesetz als auch sogar gegenüber der Datenschutz-Grundverordnung reduziert. Dies gilt im Wesentlichen auch für den Entwurf des Landesdatenschutzgesetzes Nordrhein-Westfalen. Er hat damit eine wichtige Chance für ein zukunftsfähiges Datenschutzrecht nicht aufgegriffen.

Eine positive Ausnahme bildet die Regelung in § 18 Abs. 11, die die Erhebung von Lokalisierungsdaten ohne Einwilligung der betroffenen Person nur Leitstellen und Befehlsstellen der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) erlaubt, soweit dies aus dienstlichen Gründen zur Sicherheit oder zur Koordinierung der Einsatzkräfte erforderlich ist. Soweit die amtliche Begründung (LT-Drs. 17/1981, 147) Lokalisierungen nach § 18 Abs. 1 Satz 1 jedoch für zulässig hält, sofern dies zur Durchführung des Beschäftigungsverhältnisses erforderlich ist, ist dies zu kritisieren, weil diese Generalklausel gerade nicht den besonderen Risiken von Lokalisierungsdiensten gerecht wird. Für deren Anwendung müssen besondere Regelungen getroffen werden, die hinsichtlich Zweck und Zweckbegrenzungen, Verwendungsöglichkeiten und -verboten, Speicherzeiträumen und Löschpflichten sowie weiterer Grundrechtsgefährung risikogerechte Vorkehrungen vorsehen.

2. Umsetzung von Innovationen?

Die Datenschutz-Grundverordnung orientiert sich konzeptionell weitgehend an der Datenschutzrichtlinie von 1995. Sie enthält keinen grundlegenden innovativen konzeptionellen Ansatz, weist jedoch einige sinnvolle Innovationen auf: Innovativ sind z.B. die Anforderungen an den Datenschutz durch Systemgestaltung und Voreinstellungen in Art. 25 DSGVO, die technisch-organisatorischen Maßnahmen zur Umsetzung der Datenschutzgrundsätze nach Art. 32 DSGVO, die Datenschutzfolgenabschätzung in Art. 35 DSGVO und die Zertifizierung nach Art. 42 DSGVO.

Die Datenschutz-Grundverordnung regelt jedoch viele Fragen dieser innovativen Instrumente nicht und verursacht daher eine große Rechtsunsicherheit. Diese wird dazu führen, dass die Verantwortlichen von den innovativen Instrumenten nur sehr zurückhaltend oder gar keinen Gebrauch machen werden. Beispielsweise benennt Art. 25 Abs. 1 DSGVO nur sehr abstrakt das Prinzip des „Privacy by Design" und verbindet es mit fünf Vorbehalten, unter denen es überhaupt erst zur Anwendung kommen kann. Abgesehen davon, dass der Verantwortliche dieses Prinzip ohnehin nur sehr eingeschränkt umsetzen kann und sich dieses eigentlich an den Hersteller von Informationstechnik richten müsste, werden die Verantwortlichen diese Vorbehalte in der Praxis nutzen, um sich mit der Aufgabe der datenschutzgerechten Systemgestaltung gar nicht beschäftigen zu müssen. Ähnlich verhält es sich mit dem Prinzip des „Privacy by Default" in Art. 25 Abs. 2 DSGVO. Nach dieser Vorschrift sollen sich die Voreinstellungen für den Nutzer nach der Erforderlichkeit der Verarbeitung für den jeweiligen Verarbeitungszweck richten. Dies lässt dem Verantwortlichen sehr große Freiheiten, durch die Bestimmung des Zwecks die Voreinstellungen so zu wählen, dass er durch diese die gewünschten Daten erhalten kann. Ein anderes Beispiel betrifft Art. 32 Abs. 1 DSGVO. Diese Vorschrift regelt die technisch-organisatorischen Maßnahmen, um die Grundsätze des Datenschutzes und die Rechte der betroffenen Personen umzusetzen. Diese Vorschrift ist jedoch äußert unsystematisch und unklar gefasst. Dadurch kann sich jeder Verantwortliche weitgehend heraussuchen, welche Sicherheitsmaßnahmen er treffen und welche er unterlassen will. Bei dieser großen Entscheidungsfreiheit ist die Datenschutzfolgenabschätzung ein wichtigtes Intsrument, um die Risiken der Datenverarbeitung zu erkennen und die geeigneten Schutzmaßnahmen vorzusehen. Art. 35 DSGVO lässt jedoch alle wichtigen Fragen der Konkretisierung von Risiken und der Bestimmung von Schutzmaßnahmen offen. Schließlich ist die in Art. 42 DSGVO geregelte datenschutzspezifische Zertifizierung von Datenverarbeitungsvorgängen ein wichtiges Instrument, um für betroffene Personen Transparenz darüber herzustellen, welche Datenverarbeitungsvorgänge eines Verantwortlichen den Vorgaben der Datenschutz-Grundverordnung entsprechen. Doch auch hier lässt die Datenschutz-Grundverordnung viele wichtige Fragen der Durchführung der Zertifizierung offen. Zu allen diesen innovativen Instrumenten ist die Datenschutz-Grundverordnung daher ergänzungsbedürftig und erfordert Konkretisierungen durch die Mitgliedstaaten.

Die innovativen Impulse der Datenschutz-Grundverordnung nimmt der Entwurf für ein Landesdatenschutzgesetz jedoch nicht auf. Entsprechende Ergänzungen und Konkretisierungen der neuen Instrumente zu regeln, wäre aufgrund der Öffnungsklauseln des Art. 6 Abs. 2 und 3 DSGVO möglich. Außerdem kann aufgrund allgemeiner Regeln des Unionsrecht, das nur einen Anwendungs-, aber keinen Geltungsvorrang des Unionsrecht vor dem nationalen Recht vorsieht, jeder Mitgliedsstaat ergänzende und konkretisierende Regelungen treffen, die der Umsetzung der Vorgaben einer Verordnung dienen und ihnen nicht widersprechen. Solche Regelungen könnten z.B. konkrete Vorgaben zur datenschutzkonformen Systemgestaltung und zu datenschutzgerechten Voreinstellungen, die Übernahme der Ziele der Datensicherung nach dem Standarddatenschutzmodell im Rahmen des Art. 32 DSGVO, inhaltliche Vorgaben zur Risikobestimmung

und Risikobekämpfung im Rahmen der Datenschutzfolgenabschätzung nach Art. 35 DSGVO oder bestimmte Festlegungen zur Feststellung der Konformität von Datenverarbeitungsvorgängen mit der Datenschutz-Grundverordnung im Rahmen einer Zertifizierung nach Art. 42 DSGVO sein. Diese innovativen Impulse hat der Entwurf leider nicht aufgenommen.

Zwar enthält der Entwurf in § 24 eine Regelung zur Datenschutzfolgenabschätzung. Diese regelt im Wesentlichen jedoch nur, dass Folgenabschätzungen, die bereits einmal von einer Stelle durchgeführt wurden, von anderen Stellen nicht wiederholt werden müssen. Doppelarbeit zu vermeiden, ist sinnvoll. Dass dies aber als einziges regelungsbedüftiges Problem angesehen wird, lässt vermuten, dass die Datenschutzfolgenabschätzung nur als zu vermeidende Belastung und nicht als Chance und Mittel angesehen wird, Datenschutzbewusstsein in den öffentlichen Stellen zu erzeugen und den Freiraum, den die Datenschutz-Grundverordnung an vielen Stellen den Verantwortlichen einräumt, durch Selbstverantwortung auszufüllen. Datenschutzfolgenabschätzung ist die notwendige Ergänzung z.B. zu dem Freiraum, den die unbestimmte Vorschrift des § 15 den Verantwortlichen bei der Verarbeitung besonderer Kategorien personenbezogener Daten einräumt.

Ein positives Beispiel ist § 3 Abs. 2 Satz 1. Diese Vorschrift enthält mit dem Gebot, die Datenverarbeitung so zu organisieren, dass die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist, eine spezifische Anforderung zur datenschutzgerechten Systemgestaltung. Der Entwurf sollte viel mehr solche Regelungen enthalten, die als Beispiel datenschutzförderlicher Systemgestaltung und datenschutzfreundlicher Voreinstellungen dienen können. Dies kann aber auch in künftigen bereichsspezifischen Gesetzen nachgeholt werden.

3. Ausreichender Grundrechtsschutz?

Der Entwurf verfolgt bei der Einschränkung von Grundsätzen der Datenverarbeitung und von Rechten der betroffenern Person unterschiedlichen Regelungskonzeptionen. In einer Reihe von Vorschriften – z.B. den §§ 3 Abs. 2 Satz 3, 9 Abs. 2 Nr. 5, 11 Abs. 1 Nr. 3, 14, 17 Abs. 2 Nr. 2 und Abs. 4 Nr. 2 sowie 20 Abs. 1 und 3 – lässt er eine Zweckänderung, eine Einschränkung der Betroffenenrechte oder eine Datenverarbeitung zu, wenn das öffentliche Interesse oder die berechtigten Interessen Dritter die schutzwürdigen Interessen der betroffenern Person im Einzelfall überwiegen. In anderen Vorschriften – z.B. in §§ 9 Abs. 2 Nr. 6 und Abs. 3, 11 Abs. 1 Nr. 2, 12 Abs. 2 Nr. 3, 13 Nr. 1 bis 3, 17 Abs. 5 – räumt der Entwurf dagegen dem öffentlichen Interesse oder den berechtigten Interessen Dritter immer Vorrang vor den schutzwürdigen Interessen der betroffenen Personen ein, ohne im Einzelfall eine Abwägung zu fordern, welche Interessen in der konkreten Fallkonstellation überwiegen.

In dem ersten Regelungsmodell wird der Entwurf den betroffenen Grundrechten und den öffentlichen Interessen auch im Einzelfall gerecht, weil er den Interessen an einer Einschränkung von Datenschutzgrundsätzen und Datenschutzrechten der betroffenen Personen nur dann Vorrang einräumt, wenn sie von ihrem inhaltlichen Gewicht her auch im Einzelfall überwiegen. Im zweiten Regelungsmodell wird ihnen immer ein Vorrang eingeräumt. Eine Prüfung und Abwägung der betroffenen Interessen, Grundrechte und Freiheiten findet in diesen Fällen nicht statt. Dieses Regelungsmodell schränkt das Grundrecht auf informationelle Selbstbestimmung sowie die Grundsätze und Rechte nach der Datenschutz-Grundverordnung ein, auch wenn sie im Einzelfall überwiegen. Das ist jedoch mit dem in Unions- und im deutschen Recht gleichermaßen geltenden Prinzip der Verhältnismäßigkeit nicht zu vereinbaren. Daher muss das zweite Regelungsmo-

dell dem ersten angepasst werden. In all diesen Fällen muss auch eine Abwägung stattfinden, ob das öffentliche Interesse oder das Interesse einer dritten Person, das zurücktretende Interesse der betroffenen Person im konkreten Einzelfall überwiegt. Hierauf wird im Einzelfall jeweils hingewiesen.

B. Zu einzelnen Vorschriften des Entwurfs

Im Folgenden erfolgen kurze Bewertungen, Bemerkungen und Hinweise zu einzelnen Vorschriften des Gesetzentwurfs, soweit sie das Landesdatenschutzgesetz an die Datenschutz-Grundverordnung anpassen.

§ 3 Zulässigkeit der Verarbeitung personenbezogener Daten

§ 3 Abs. 1 wiederholt den Wortlaut des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO und könnte daher gegen das Normwiederholungsverbot verstoßen. Regelungen zur Zulässigkeit der Datenverarbeitung im Anwendungsbereich des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO sind nach Art. 6 Abs. 3 Satz 1 DSGVO durch das Recht der Mitgliedstaaten festzulegen. Da Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO somit die eigentliche Erlaubnis nicht festlegt, sondern der Mitgliedstaat, besteht keine Unklarheit über den Charakter der Erlaubnis. Sie wird durch den Gesetzgeber des Landes Nordrhein-Westfalen festgelegt.

§ 3 Abs. 2 Satz 1 enthält mit dem Gebot, die Datenverarbeitung so zu organisieren, dass die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist, eine sinnvolle Regelung zur Gewährleistung der Zweckbindung. Die Ausnahme des Satzes 2 ist nachvollziehbar und das Verwertungsverbot in Satz 3 ist konsequent.

§ 4 Begriffsbestimmung

Art. 4 DSGVO definiert nicht den Begriff der Anonymisierung, obwohl Erwägungsgrund 26 diesen Begriff erwähnt und mehrere Vorschriften (z.B. Art. 89 Abs. 1 Satz 4 DSGVO) sich auf Anonymisierung beziehen. Dies verursacht große Rechtsunsicherheit. Es ist daher zu begrüßen, dass § 4 den Begriff der Anonymisierung ergänzend zur Datenschutz-Grundverordnung definiert.

§ 7 Erhebung personenbezogener Daten bei dritten Personen und nicht-öffentlichen Stellen

Nach § 7 Satz 1 hat der Erhebende dritten Personen oder einer nicht-öffentlichen Stelle, bei der personenbezogene Daten einer betroffenen Person erhoben werden, diese nur auf Verlangen über den Erhebungszweck zu informieren (soweit dadurch schutzwürdige Belange der betroffenen Person nicht beeinträchtigt werden). Nach Satz 2 hat er die dritte Person beziehungsweise die nicht-öffentliche Stelle auf ihre Pflicht zur Auskunft oder die Freiwilligkeit ihrer Angaben nur dann hinzuweisen, wenn „die Daten aufgrund einer Rechtsvorschrift erhoben (werden), die sie zur Auskunft verpflichtet". Die Regelung des Satzes 2 ist unlogisch: Wenn die Informationspflicht nur besteht, wenn eine Auskunftspflicht der dritten Person oder der nicht-öffentliche Stelle besteht, kann sie nicht für die Freiwilligkeit der Auskunft gelten. Beide Regelungen enthalten jedoch Einschränkungen, die der gebotenen Transparenz der Datenverarbeitung (Art. 5 Abs. 1 lit. a DSGVO) (amtliche Begründung, LT-Drs. 17/1981, 136: „größtmögliches Maß an Transparenz"), an der die dritte Person oder die nicht-öffentliche Stelle durch ihre Auskunft oder Datenübermittlung mitwirken, nicht entsprechen. Die Information über die Verpflichtung oder Freiwilligkeit der Mitteilung und über den Erhebungszweck sollte immer erteilt werden. Eine Ausnahme sollte nur bestehen, wenn durch diese Information die schutzwürdigen Belange der betroffenen Person beeinträchtigt werden.

§ 9 Zulässigkeit der Datenverarbeitung im Hinblick auf die Zweckbindung

§ 9 Abs. 2 ermöglicht, die personenbezogenen Daten zu anderen Zwecken als zu denjenigen zu verarbeiten, zu denen sie erhoben worden sind. Eine Regelung zur zulässigen Zweckänderung ist nach der Öffnungsklausel des Art. 6 Abs. 4 DSGVO zulässig. § 9 Abs. 2 lässt allerdings offen, wer die Datenverarbeitung zu einem anderen Zweck vornehmen darf. Da der Begriff der Datenverarbeitung nach Art. 4 Nr. 2 DSGVO alle möglichen Formen des Umgangs mit personenbezogenen Daten erfasst, sind ohne nähere Eingrenzungen – z.B. auf den erhebenden Verantwortlichen – durch diese Regelungen alle Formen u.a. der Übermittlung, der Offenlegung, des Abfragens, der Verwendung, der Verbreitung, der Bereitstellung, des Abgleichs oder der Verknüpfung zulässig. Die nach § 9 Abs. 2 zulässigen Zweckänderndungen grenzen die möglichen Empfänger der Übermittlungen und die möglichen Berechtigten der zweckändernden Datenverarbeitung nur sehr indirekt ein und lassen weitgehend offen, wer diese Zweckänderungen vornehmen darf. Die Vorschrift ist wegen der Weite des Verarbeitungsbegriffs und fehlender Präzisierungen der Berechtigten und zulässiger Bearbeitungsformen zu unbestimmt. Sie sollte festlegen, dass nur der erhebende Verantwortliche Zweckänderungen vornehmen darf.

§ 9 Abs. 2 Nr. 6 lässt eine Zweckänderung zu, wenn sie „im öffentlichen Interesse … liegt oder zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und die betroffene Person in diesen Fällen der Datenverarbeitung nicht widersprochen hat“. Diese Regelung wäre grundsätzlich nur dann vertretbar, wenn sichergestellt wäre, dass die betroffene Person immer über diese Zweckänderung informiert ist. Ohne Information über die Zweckänderung hilft ihr das Recht, ihr zu widersprechen, nichts. Nach der sehr weiten Ausnahme des § 9 Abs. 3 wird ihr die Information aber vorbehalten, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde. Dies kann immer auch im Fall des § 9 Abs. 2 Nr. 6 der Fall sein. Die Möglichkeit des Widerspruchs läuft dadurch ins Leere.

Die Regelung des § 9 Abs. 2 Nr. 6 berücksichtigt außerdem unzureichend die Grundrechte der betroffenen Person, weil sie kein Überwiegen des öffentlichen Interesses oder der berechtigten Interessen des Dritten über die schutzwürdigen Interessen der betroffenen Person fordert. Nach dieser Regelung wäre eine Zweckänderung auch dann zulässig, wenn die Interessen der betroffenen Person im Einzelfall schutzwürdiger sind als das öffentliche Interesse oder die berechtigten Interessen des Dritten. Wie in § 9 Abs. 2 Nr. 5 sollte daher auch in Nr. 6 eine Abwägung der Interessen im Einzelfall gefordert werden (s. allgemein A. 3.).

Auch § 9 Abs. 3 berücksichtigt unzureichend die Grundrechte der betroffenen Person. Die Vorschrift schließt eine Information der betroffenen Person über die Zweckänderung kategorisch aus, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde, ohne dies im Einzelfall mit den schutzwürdigen Interessen der betroffenen Person abzuwägen. Sie schließt die Information also auch dann aus, wenn wenn die Interessen der betroffenen Person im Einzelfall schutzwürdiger sind. Dies widerspricht dem Grundsatz der Verhältnismäßigkeit. Für § 9 Abs. 3 sollte daher eine Abwägung der Interessen im Einzelfall gefordert werden (s. allgemein A. 3.).

Nach § 9 Abs. 4 Nr. 2 ist eine Zweckänderung zulässig, wenn sie für die Bearbeitung eines von der betroffenen Person gestellten Antrags erforderlich ist. Zweck der Datenverarbeitung ist in diesem Fall die Be-

arbeitung des Antrags. Jede Datenverarbeitung, die dafür erforderlich ist, dient diesem Zweck. Eine Zweckänderung ist für die Bearbeitung des Antrags nicht notwendig. Diese Ausnahme erscheint daher überflüssig.

§ 11 Beschränkung der Informationspflicht bei der Erhebung von personenbezogenen Daten nach Art. 13 und 14 DSGVO

Nach § 11 Abs. 1 Nr. 2 entfällt die Informationspflicht nach Art. 13 Abs. 3 und Art. 14 Abs. 1, 2 und 4 DSGVO, soweit und solange die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind, ohne dass im Einzelfall eine Interessenabwägung stattfindet. Nach dieser Regelung wäre eine Einschränkung der Informationspflicht also auch dann zulässig, wenn die Interessen der betroffenen Person im Einzelfall schutzwürdiger sind als die Rechte und Freiheiten der anderen Person. Dies widerspricht dem Grundsatz der Verhältnismäßigkeit. Wie in § 11 Abs. 1 Nr. 3 sollte daher auch in Nr. 2 eine Abwägung der Interessen im Einzelfall gefordert werden (s. allgemein A. 3.).

§ 12 Beschränkung des Auskunftsrechts der betroffenen Person nach Art. 15 DSGVO

Nach § 12 Abs. 2 Nr. 3 kann die Auskunftserteilung nach Art. 15 DSGVO abgelehnt werden, „soweit und solange die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung … wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind". Eine Interessenabwägung im Einzelfall ist nicht vorgesehen. Nach dieser Regelung wäre eine Verweigerung der Auskunft also auch dann zulässig, wenn die Interessen der betroffenen Person im Einzelfall schutzwürdiger sind als die Rechte und Freiheiten der anderen Person. Dies verstößt gegen den Grundsatz der Verhältnismäßigkeit. Die Verweigerung der Auskunft sollte daher auch von einer Abwägung der Interessen im Einzelfall abhängig gemacht werden (s. allgemein A. 3.).

§ 13 Beschränkung der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen nach Art. 34 DSGVO

Nach § 13 kann der Verantwortliche von der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person absehen, „soweit und solange
1. die Informationen die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind oder
3. die Information die Sicherheit von IT-Systemen gefährden würde".
Eine Interessenabwägung im Einzelfall ist nicht vorgesehen. Nach diesen drei Ausnahmen wäre eine Nichtbenachrichtung also auch dann zulässig, wenn die möglichen Schäden der – unter Umständen sehr vielen betroffenen Personen – im Einzelfall als schwerwiegender einzuschätzen wären als die Nachteile für die öffentliche Sicherheit oder das Wohl des Bundes oder eines Landes, für die Rechte und Freiheiten anderer Personen oder für die Sicherheit von IT-Systemen. Dies widerspricht dem Grundsatz der Verhältnismäßigkeit. Wie in § 14 sollte daher auch in § 13 eine Abwägung der Interessen im Einzelfall gefordert werden (s. allgemein A. 3.).

§ 14 Beschränkung des Widerspruchsrechts

§ 14 schließt das Recht auf Widerspruch gemäß Art. 21 Abs. 1 DSGVO gegenüber einer öffentlichen Stelle aus, „soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der be-

troffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet". Diese Vorschrift berücksichtigt vorbildlich die Abwägung im Einzelfall. Dies kontrastiert mit § 13 in besonderer Weise deswegen, weil hier nicht nur – wie in anderen Vorschriften – ein „öffentliches Interesse",sondern sogar ein „zwingendes öffentliches Interesse" gefordert wird, das aber trotz seines zwingenden Charakters im Einzelfall die Interessen der betroffenen Person überwiegen muss.

Wie in §§ 11 bis 13 sollte auch in § 14 in der Überschrift der Artikel des eingeschränkten Rechts genannt werden: „Beschränkung des Widerspruchsrechts nach Artikel 21 der Verordnung (EU) 2016/679".

§ 15 Garantien zum Schutz personenbezogener Daten und anderer Grundrechte

§ 15 listet neun sinnvolle technisch-organisatorischen Maßnahmen auf, um besondere Kategorien personenbezogener Daten zu schützen. Die Wirkung dieser Vorschrift wird jedoch deutlich dadurch gemindert, dass sie die technisch-organisatorischen Maßnahmen unter acht Vorbehalte stellt und die Auswahl, den Umfang und die Intensität dieser Maßnahmen ohne nähere Bestimmungen dem Verantwortlichen überlässt. Jeder Grad an größerer Bestimmtheit würde der Duchsetzung des Datenschutzrechts erheblich helfen. Diese mangelnde Bestimmtheit ist auch deswegen problematisch, weil die genannten Maßnahmen als „geeignete Garantien" (s. z.B. Art. 9 Abs. 2 lit. b und d DSGVO) oder als „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" (s. z.B. Art. 9 Abs. 2 lit. g, i und j DSGVO) angesehen werden, die Vorschrift dafür aber keine klaren Vorgaben liefert, sondern die technisch-organisatorischen Maßnahmen dem Verantwortlichen überlässt.

§ 16 Verarbeitung besonderer Kategorien personenbezogener Daten

Nach § 16 Abs. 1 Nr. 3 ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, „soweit sie zum Zwecke der Gesundheitsvorsorge, zur medizinischen Diagnostik" und anderen Gesundheitszwecken „erforderlich ist, sofern die Verarbeitung dieser Daten durch ärztliches oder sonstiges Personal erfolgt, das einer entsprechenden Geheimhaltungspflicht unterliegt". Bei einer Datenverarbeitung durch ärztliches Personal wird die Geheimhaltung durch § 203 StGB geschützt. Dieser Schutz darf durch den Einbezug sonstigen Personals nicht verschlechtert werden. Der Wortlaut der Vorschrift stellt dies jedoch nicht sicher, sondern ermöglicht auch, sonstiges Personal mit der Datenverarbeitung zu betrauen, das nicht § 203 Abs. 4 StGB unterliegt. Nach der Neufassung des § 203 Abs. 3 und 4 StGB soll die Datenverarbeitung im Auftrag erleichtert und der „Gleichklang" zwischen Strafrecht und Datenschutzrecht erleichtert werden. Dies wird durch die Wortwahl der Vorschrift wieder gefährdet. Um dies zu verhindern und einen gleichmäßigen Schutz zu gewährleisten, sollten in den Text der Nr. 3 ein Bezug zu § 203 StGB aufgenommen werden: „ … sonstiges Personal erfolgt, das einer entsprechenden *strafrechtlich geschützten* Geheimhaltungspflicht unterliegt".

§ 17 Datenverarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken

Nach § 17 Abs. 1 Satz 3 kann die Datenerfassung, Anonymisierung oder Pseudonymisierung auch durch die mit der Forschung befassten Personen erfolgen, wenn sie zuvor nach dem Verpflichtungsgesetz zur Verschwiegenheit verpflichtet worden sind. Soweit die forschende Tätigkeit – wie bei Ärzten – zu deren § 203 StGB unterliegenden Berufsausübung gehört, sollte bei den sonstigen mit der Forschung befassten Personen darauf geachtet werden, dass auch ihnen gegenüber der strafrechtliche Schutz gemäß § 203 Abs. 4 StGB besteht.

Das Gleiche gilt für die Übermittlung der personenbezogenen Daten nach Abs. 6 an Empfänger, für die dieses Gesetz keine Anwendung findet.

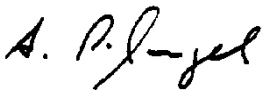
§ 20 Videoüberwachung

§ 20 Abs. 4 fordert, die nach Abs. 1 erhobenen Daten der Videoüberwachung „unverzüglich, spätestens jedoch vier Wochen nach ihrer Erhebung, zu löschen". Die Frist von vier Wochen erscheint zu lang. Ob die Daten zur Abwehr von Gefahren für die öffentliche Sicherheit, zur Verfolgung von Straftaten oder zur Geltendmachung von Rechtsansprüchen gegenüber der betroffenen Person erforderlich sind und damit nach Satz 2 nicht gelöscht werden müssen, lässt sich erheblich früher feststellen. Eine Speicherfrist von vier Wochen erscheint daher nicht verhältnismäßig.

§ 25 Errichtung und Rechtsstellung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit

Nach § 25 Abs. 4 ist für die beamtenrechtlichen Angelegenheiten der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit in Person das für Inneres zuständige Ministerium zuständig. Zwar unterliegt dieses der Maßgabe, dass die Wahrnehmung der Zuständigkeit die Unabhängigkeit der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit nicht beeinträchtigen darf. Dennoch ist zu fragen, ob diese Regelung der von Art. 52 DSGVO geforderten und vom Europäischen Gerichtshof sehr streng ausgeformten „absoluten Unabhängigkeit" der Aufsichtsbehörde entspricht. Hier könnte auch überlegt werden, ob der Lantagspräsident die zuständige Aufsichtsbehörde sein könnte, da die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit nach § 25 Abs. 1 vom Landtag gewählt wird und der Lantagspräsident nach § 25 Abs. 5 ohnehin Aufsichtsaufgaben und -befugnisse hat.

Eine vergleichbare Regelung findet sich z.B. in § 13 Abs. 2 BDSG und in §§ 16 Abs. 3 und 17 Abs. 2 des Landesdatenschutzgesetzes Brandenburg, §§ 21 und 22 des Hamburgischen Datenschutzgesetzes sowie § 11 Abs. 6 des Hessischen Landesdatenschutz- und Informationsfreiheitsgesetzes. Eine Aufsicht durch das Ministeriumn des Innern, das durch die oder den Landesdatenschutzbeauftragten kontrolliert werden soll, sieht – soweit ersichtlich – bisher kein anderes Bundesland vor.



(Prof. Dr. Alexander Roßnagel)