Stand: 12. März 2018

Teil 3

Ausschussvorlage INA 19/64 – öffentlich –

Ausschussvorlage UDS 19/9 – öffentlich –

Stellungnahmen der Anzuhörenden

zu dem

Gesetzentwurf
der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit
– Drucks. 19/5728 –

14.	Transparency International Deutschland	S. 80
15.	Kommissariats der Katholischen Bischöfe im Lande Hessen	S. 83
16.	Bundesbeauftragte für Datenschutz und die Informationsfreiheit	S. 96
17.	Verband Deutscher Zeitschriftenverleger e.V. (VDZ)	S. 101
18.	Deutscher Beamtenbund und Tarifunion (dbb) Hessen	S. 112
19.	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit RLP	S. 118
20.	Die Datenschützer Rhein-Main	S. 132
21.	Mehr Demokratie e. V., Landesverband Hessen	S. 148
22.	Bundeskriminalamt Wiesbaden	S. 157
23.	Hessischer Städtetag	S. 162
24.	Deutsche Gesellschaft für Informationsfreiheit	S. 164
25.	Bund Deutscher Strafvollzugsbeamter (BSBD) Hessen	S. 169
26.	Frankfurt University of Applied Sciences, Fachbereich 02	S. 173

TRANSPARENCY INTERNATIONAL
Deutschland e.V.
Die Koalition gegen Korruption.

Stellungnahme von Transparency International Deutschland e. V. zum

Entwurf für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN (Drucksache 19/5728)

Verfasser: Caro Glandorf, Regionalgruppe Frankfurt-Rhein-Main
Datum: 06.03.2018

Wir bedanken uns für die Übersendung des Gesetzentwurfs und die Möglichkeit, dazu Stellung zu nehmen. Unsere Stellungnahme beschränkt sich auf den vierten Teil: Anspruch auf Informationszugang (§§ 80 – 89).

Transparency International arbeitet in 100 Ländern der Welt präventiv gegen Korruption in allen gesellschaftlichen Sektoren. Unsere Erfahrung bestätigt uns, dass Korruption immer dort am besten gedeiht, wo wenig Transparenz herrscht. Wir wissen uns darin im Einklang mit Ermittlungsbehörden weltweit. Wir halten mehr Transparenz nicht nur für ein wirksames Instrument, Korruption zu erschweren, sondern für eine wichtige Grundvoraussetzung, das Vertrauen der Bürgerinnen und Bürger in Politik und Verwaltung wieder erstarken zu lassen. Rechtzeitig die dazu erforderlichen Kenntnisse und technologischen Voraussetzungen zu schaffen, ebnet den Weg hin zu Open Government.

Deshalb begrüßen wir grundsätzlich den Impuls, die Auskunftsrechte der Bürgerinnen und Bürger in Hessen durch die Einführung eines Informationsfreiheitsgesetzes zu stärken. Der vorliegende Gesetzentwurf zeigt jedoch große Unzulänglichkeiten, sowohl den Anwendungsbereich als auch die Ausgestaltung der Regelungen betreffend. Anstatt eines zeitgemäßen Transparenzgesetzes mit proaktiver Veröffentlichung von Verwaltungsdokumenten wurde hier nur eine kleinteilige und nachrangige Regelung der Auskunft bei Landesbehörden geschaffen, die – anders als sonstige Informationsfreiheitsgesetze in Deutschland – nicht voraussetzungslos ist und großen Spielraum für Interpretationen zum Nachteil der Bürgerinnen und Bürger lässt. Die pauschale Nicht-Regelung der kommunalen Ebene stellt einen großen Verlust dar und macht den Entwurf zu einer vertanen Chance, allen Bürgerinnen und Bürgern Hessens dieselbe Teilhabe zu ermöglichen. Für die Korruptionsprävention entfalten Einsichtsrechte gegenüber Städten, Gemeinden und Landkreisen ihr größtes Potential. Angesichts dieser Mängel unterstützt Transparency Deutschland den vorliegenden Entwurf ausdrücklich nicht.

Im Einzelnen kommentieren wir den Entwurf wie folgt:

Zu § 80 Abs. 1: Anstatt eines zeitgemäßen Transparenzgesetzes mit proaktiver Online-Veröffentlichung von Verwaltungsdokumenten wurde hier ein Informationsfreiheitsgesetz entworfen, das die Bürgerinnen und Bürger langwierige Anfrageprozesse einleiten lässt, um Auskunft von der Verwaltung zu erhalten, die in ihrem Auftrag arbeitet. Die Informationsasymmetrie zwischen Staat und BürgerInnen wird nicht reduziert. Dies ist nicht mehr zeitgemäß; aus dem Informationsrecht des

Bürgers sollte eine Informationspflicht für die Verwaltung werden. Bearbeitung individueller Anträge bedeutet eine höhere Belastung der Behörden als eine proaktive elektronische Veröffentlichung, die in modernen Verwaltungen mit vergleichsweise wenig zusätzlichem Aufwand realisiert wird und so gleichzeitig allen Nutzern zugänglich ist. Proaktive Veröffentlichung liefert auch der Verwaltung selbst einen Nutzen, das haben Erfahrungen mit dem Hamburger Transparenzportal gezeigt. Ein nur auf Anträgen basierendes Gesetz kommt heute einer Barriere für die Digitalisierung der Gesellschaft gleich.

Zu § 80 Abs. 2: Mit dem aktuellen Entwurf würde die Informationsfreiheit nur nachrangig geregelt; andere Regelungen zur Auskunftserteilung würden in jedem Fall vorgehen. In vielen Fällen ist das öffentliche Interesse an der Offenlegung von Informationen höher einzuschätzen als z. B. das private Interesse an einer Geheimhaltung. Deswegen muss stets eine Abwägung zwischen dem öffentlichen Interesse und ggf. entgegenstehenden Belangen vorgenommen werden.

Zu § 81: Der Gesetzentwurf schränkt die informationspflichtigen Stellen unnötig ein. Nach Abs. 1 Nr. 5 gilt die Vorschrift für Forschungseinrichtungen und Hochschulen nicht in den Bereichen Forschung und Lehre. Damit werden ggf. kritische Informationen über Forschungsfinanzierungen pauschal von der Auskunft ausgenommen. Stattdessen sollten gerade Informationen über Subventions- und Zuwendungsvergaben sowie über die Annahme von Fördermitteln, Sponsoring, Spenden und Forschungsmitteln veröffentlicht werden, soweit deren Veröffentlichung nicht gegen Grundrechte verstößt. Dies kann unseres Erachtens sicherstellen, dass bei Wahrung der Wissenschafts- und Forschungsfreiheit bestimmte Grundinformationen etwa zu Drittmittelverträgen dem Informationszugang unterliegen.

Nach Abs. 1 Nr. 6 wird die kommunale Verwaltungsebene von dem vorliegenden Entwurf nicht direkt reguliert – Kommunen wird die Umsetzung des Gesetzes per Satzung freigestellt. Den meisten Informationsbedarf haben Bürgerinnen und Bürger jedoch gegenüber den Landkreisen, Städten und Gemeinden, in denen sie wohnen. Auf der kommunalen Ebene liegt auch das größte Potential für Korruptionsprävention durch Veröffentlichung von Verwaltungsdokumenten. Daher kritisieren wir diese – deutschlandweit einmalige – Auslassung scharf. Die freiwillige Umsetzung per Satzung wird im besten Fall zu einem Flickenteppich führen, in dem Bürgerinnen und Bürger aus beispielsweise Maintal, das schon eine eigene Informationsfreiheitssatzung hat, viel weitgehendere Auskunftsrechte haben als ihre Nachbarn aus Hanau, selbst wenn es die Landesregelung per Satzung übernimmt. Im schlechtesten Fall wird kein Landkreis und keine Kommune die Regelung des Landes übernehmen, weil sie für die Verwaltung problematisch und für die BürgerInnen nicht gewinnbringend ist. In der Ersten Lesung des Entwurfs wurde die Ausnahme des kommunalen Bereichs unter anderem mit dem Konnexitätsprinzip und den für das Land daraus resultierenden Kosten begründet. Wer die Teilhabe der Bürgerinnen und Bürger wirklich verbessern will, sollte diese Bedenken hintanstellen. Bürgerrechte sollten nicht gegen Kostenprognosen ausgespielt werden.

Zu Abs. 2: Transparency Deutschland kann nicht nachvollziehen, warum Polizei (deutschlandweit einmalig!) und Landesverfassungsschutz pauschal von der Regelung ausgenommen werden. Der in der Ersten Lesung genannte Verweis auf spezialgesetzliche Regelungen ist nichtig: Dort sind nur direkt betroffene Personen auskunftsberechtigt. Soweit es ihr allgemeines Verwaltungshandeln in Wahrnehmung von öffentlichen Aufgaben betrifft, sollten diese Stellen ebenso Informationen veröffentlichen. Gleiches gilt für die Landeskartellbehörde und die Selbstverwaltungsorganisationen der Wirtschaft.

Nach § 82 Nr. 5 besteht bei einem rein wirtschaftlichen Interesse an den Informationen kein Anspruch auf Auskunft. Dies schafft nicht nur Unsicherheit und Auslegungsaufwand – wie kann eine

Stelle das hintergründige Interesse an einer Information bewerten und auf welcher Grundlage ggf. die Auskunft verweigern? – sondern schafft auch eine problematische Präzedenz in der Geschichte der Informationsfreiheit in Deutschland: Hier wird nicht ein Jedermannsrecht gewährt, das voraussetzungslos Zugang zu amtlichen Informationen schafft, sondern Tür und Tor geöffnet für mehr oder weniger willkürliche Ablehnungen.

Als unzureichend empfinden wir auch die Kostenregelung in § 88. Die Arbeit der Behörden wird vom Steuerzahler finanziert. Daher müssen nicht nur einfache mündliche und schriftliche Auskünfte, sondern auch die Herausgabe von Dokumenten nach Anfragen an staatliche Stellen grundsätzlich gebührenfrei sein. Eine Kostendeckelung der Auslagen für Kopien oder ähnliches schafft Sicherheit für die Antragsstellenden.

Kommissariat der Katholischen Bischöfe
im Lande Hessen

per E-Mail

An den
Vorsitzenden des Innenausschusses
im Hessischen Landtag
Herrn Horst Klee MdL

Frauenlobstraße 5
65187 Wiesbaden
Telefon: (0611) 3 60 08-0
Telefax: (0611) 3 60 08-20

7. März 2018
Az. 7.2.1.3. / Kl-fe

Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN über ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung EU Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit – Drucks. 19/5728
Aktenzeichen: IA 2.1
Ihr Schreiben vom 21. Dezember 2017

Sehr geehrter Herr Klee,
sehr geehrte Damen und Herren,

herzlich danken wir für die freundliche Einladung, zu oben genanntem Gesetzentwurf eine Stellungnahme abgeben zu können. Gerne nehmen wir diese Möglichkeit wahr.

Die EU-DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Am 25. Mai 2018 wird die Verordnung unmittelbar geltendes Recht in allen Mitgliedsstaaten der Europäischen Union sein. Zeitgleich mit der Verordnung in Kraft getreten ist die Richtlinie des Europäischen Parlaments und des Rates 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 des Rates. Der vorliegende Gesetzentwurf dient der Anpassung der hessischen Regelungen.

Art. 1 Hessisches Datenschutz- und Informationsfreiheitsgesetz

§ 27 Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften

Die vorher in § 35 HDSG geregelte Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften ist in dem Entwurf in § 27 um folgenden Zusatz erweitert worden: „ … , sofern auf Grundlage geeigneter Garantien sichergestellt ist, dass bei der empfangenen Stelle eine Datenverarbeitung im Einklang mit der Verordnung … erfolgt." Diese neue Fassung trägt der Regelung des Art. 91 EU-DSGVO Rechnung.

Für die Katholische Kirche hat die Vollversammlung des Verbandes der Diözesen Deutschlands am 20.11.2017 ein neues Gesetz über den kirchlichen Datenschutz (KDG) beschlossen, das zu seiner Wirksamkeit noch der Umsetzung durch die einzelnen Diözesan-Bischöfe bedarf. Dieses wird bis Mai 2018 in den Hessischen Diözesen erfolgt sein. Außerdem ist zum 01.01.2018 für die (Erz-) Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier eine Datenschutzstelle als eine unabhängige öffentlich-rechtliche kirchliche Einrichtung entstanden. Sie führt den Namen Datenschutzbeauftragte für die (Erz-)Diözesen in Baden-Württemberg, Hessen, Rheinland-Pfalz und Saarland (Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier). Das neue KDG und die Stelle der überdiözesanen Datenschutzbeauftragten sind in Einklang mit der DSGVO geschaffen worden, um gleichwertige Regelungen für diesen Bereich zu erlassen. Daher halten wir die Vorgabe „Grundlage geeigneter Garantien sichergestellt" für erfüllt. Sollten andere Anforderungen durch den neuen Wortlaut gemeint sein, bitten wir um entsprechende Mitteilung.

Regelung zur Vollstreckung von Bußgeldbescheiden der kirchlichen Datenschutzaufsicht

Ein besonderes wichtiges Anliegen für die katholischen Bistümer ist die Aufnahme einer staatlichen Vollstreckungshilfe.

Beide Kirchen in Deutschland haben zur Umsetzung von Art. 91 Abs. 1 EU-DSGVO ihr bestehendes Datenschutzrecht einer grundlegenden Revision unterzogen, um es mit der DSGVO in Einklang zu bringen. Wie schon oben angegeben ist am 20.11.2017 von der Vollversammlung des Verbandes der Diözesen Deutschlands ein neues Gesetz über den kirchlichen Datenschutz beschlossen worden.

Zur Herstellung des erforderlichen Einklanges ist durch § 51 KDG insbesondere auch die Verhängung von Geldbußen durch die jeweils zuständige kirchliche Datenschutzaufsicht eingeführt worden. Dabei ist in § 51 Abs. 7 KDG eine – allerdings lediglich deklaratorische – Regelung zur Vollstreckbarkeit aufgenommen worden. Sie stellt klar, dass eine Vollstreckung nur auf dem Zivilrechtsweg erfolgen kann, sofern das weltliche Recht keine staatliche Vollstreckungshilfe vorsieht. Dabei dürfte unstreitig sein, dass eine Beschränkung auf die Erlangung eines vollstreckbaren Titels (Vollstreckungsbescheid oder ggf. vollstreckbare Ausfertigung eines zivilrechtlichen Urteils) unter Umständen recht langwierig sein kann und daher die Effektivität der Verhängung von Geldbußen beeinträchtigen könnte. Es wäre daher folgerichtig, im neuen Datenschutzgesetz von Hessen eine Regelung zu haben, die der kirchlichen Datenschutzaufsicht die Möglichkeit einräumt, die von ihr verhängten Geldbußen unmittelbar im Verwaltungszwangsverfahren beizutreiben.

Beispiele in anderen Bundesländern zeigen, dass eine solche staatliche Vollstreckungshilfe nicht systemwidrig ist. Ein Schreiben aus dem Innenministerium des Saarlandes vom 05.12.2017 an das dortige Katholische Büro (Anlage 1) zeigt, dass im Saarland eine grundsätzliche Offenheit für dieses Anliegen besteht.

Des Weiteren fügen wir als Anlage 2 eine Synopse über bestehende Landesregelungen zur Vollstreckungshilfe bei Friedhofsgebühren und im Kirchensteuerwesen bei. Aufgeführt sind

Regelungen, die in vier Bundesländern bestehen (Niedersachsen, Nordrhein-Westfalen, Sachsen-Anhalt und Thüringen).Diese Beispiele belegen und sprechen dafür, dass keine Systemwidrigkeit vorliegt, wenn man auch in Hessen eine solche staatliche Vollstreckungshilfe in das Gesetz aufnehmen würde.

Auf den ersten Blick scheinen die dortigen Anknüpfungen an eine zuvor staatlicherseits erfolgte Genehmigung der entsprechenden Gebührensatzung entgegen zu stehen. Diesem denkbaren Einwand ist jedoch entgegen zu halten, dass selbst dem staatlichen Datenschutzrecht ein nachprüfbarer Bußgeldkatalog infolge der notwendigen Einzelfallentscheidung wesensfremd ist. Es kommt hinzu, dass die Datenschutzgrundverordnung an keiner Stelle eine staatliche Approbation kirchlicher Datenschutzregelungen vorsieht, die Maßnahmen der kirchlichen Datenschutzaufsicht aber selbstverständlich sowohl der kirchlichen wie auch der staatlichen Justiziabilität unterliegen.

Sofern eine Aufnahme der staatlichen Vollstreckungshilfe unmittelbar in das neue Datenschutzgesetz nicht für sachdienlich gehalten wird, bitten wir um eine Aufnahme der staatlichen Vollstreckungshilfe in entsprechende Rechtsverordnungen.

Das Katholische Büro und das Evangelische Büro in Nordrhein-Westfalen haben das Anliegen einer Vollstreckungshilfe bei Geldbußen bereits in die Verbändeanhörung eingebracht. Gleiches ist für Thüringen, Mecklenburg-Vorpommern und Bayern geplant.

Als Anlage 3 fügen wir Ihnen einen Vermerk von Prof. Dr. Gernot Sydow, M. A., Institut für Europäisches Verwaltungsrecht an der Westfälischen Wilhelms-Universität Münster bei. In diesem werden die Gründe für eine staatliche Vollstreckungshilfe ausführlich dargelegt. Prof. Sydow bezieht sich zwar in seinem Vermerk auf die Rechtslage in NRW. Seine allgemeinen Ausführungen gelten aber für ganz Deutschland und damit ebenso für Hessen.

§ 82 Schutz besonderer öffentlicher und privater Belange

Die neu geschaffenen Regelungen zum Anspruch auf Informationszugang (§ 80 ff.) dürfen nicht das verfassungsrechtlich geschützte Recht auf Selbstbestimmung der Katholischen Bistümer verletzen. Daher müssen in der Schutzvorschrift des § 82 auch die öffentlich-rechtlich verfassten Religionsgesellschaften aufgenommen werden. Wir halten es deshalb für angezeigt, folgende weitere Ziffer 6 bei § 82 einzufügen:

> *„6. bei Informationen, die in Zusammenhang mit dem verfassungsrechtlich geschützten Selbstbestimmungsrecht der öffentlich-rechtlichen Religionsgesellschaften und Weltanschauungsgemeinschaften stehen, sofern die betroffene Religionsgesellschaft oder Weltanschauungsgemeinschaft nicht eingewilligt hat."*

Außerdem bitten wir um eine klarstellende Regelung in § 82 Nr. 4 dahingehend, dass unter den Begriff der „Betriebs- oder Geschäftsgeheimnisse" nicht nur solche aus der Industrie und Wirtschaft fallen, sondern der Begriff auch die Bereiche erfasst, die zum verfassungsrechtlich geschützten Selbstbestimmungsrecht der öffentlich-rechtlichen Religionsgesellschaften gehören.

Art. 2 Änderung des Hessischen Jugendstrafvollzugsgesetzes
Art. 3 Änderung des Hessischen Strafvollzugsgesetzes
Art. 4 Änderung des Hessischen Untersuchungsstrafvollzugsgesetzes
Art. 5 Änderung des Hessischen Sicherungsverwahrungsvollzugsgesetzes
Art. 6 Änderung des Hessischen Jugendarrestvollzugsgesetzes

Zur Anpassung der Vorschriften über die Verarbeitung personenbezogener Daten in den Hessischen Fachgesetzen werden neben dem Hessischen Datenschutz- und Informationsfreiheitsgesetz weitere 28 Gesetze geändert. Die Anpassung in den o. g. Gesetzen führt dazu, dass der Datenschutz hinreichend beachtet werden soll und größtenteils nunmehr unter strengeren Voraussetzungen ein Eingriff möglich ist. Dieses entspricht den gesetzlichen Vorgaben.

Jedoch sehen wir die Regelungen in den o. g. Gesetzen zur Überprüfung anstaltsfremder Personen weiterhin kritisch. Denn dadurch werden nicht nur die Rechte der Gefangenen bzw. Untergebrachten, sondern insbesondere auch die Rechte der Besucher (Recht auf informationelle Selbstbestimmung) eingeschränkt. Das BVerfG hat zwar betont, dass die Sicherheit und Ordnung in Justizvollzugsanstalten Eingriffe in Persönlichkeitsrechte rechtfertigen können. Dieser Grundsatz gilt auch für die Sicherungsverwahrung.

Die im Gesetz vorgesehene nicht anlassbezogene Überprüfung von Gefangenenbesuch (Auskunft Bundeszentralregister, Abfrage bei Polizeibehörden, Abfrage beim Landesamt für Verfassungsschutz) beachtet jedoch nach unserer Meinung nicht den Verhältnismäßigkeitsgrundsatz, nach dem jede grundrechtseinschränkende Maßnahme geeignet, erforderlich und zumutbar sein muss. Es stellt einen Verstoß gegen den Verhältnismäßigkeitsgrundsatz dar, wenn alle Besucher unter Generalverdacht gestellt werden und ohne konkreten Anlass einer Zuverlässigkeitsprüfung unterworfen werden.

Es stellt eine Umkehrung des gesetzlichen Regel-Ausnahme-Verhältnisses der Besuchsgestattung dar, wenn eine generelle Regelanfrage an die Polizei gerichtet werden kann oder wenn allein aus der Verweigerung der Datenschutzerklärung auf einen Versagensgrund geschlossen wird.

Daher sollte in den entsprechenden Regelungen gestrichen werden, dass eine Person nicht oder nur unter Beschränkung zum Besuch zugelassen wird, wenn die betroffene Person die Einwilligung in eine Zuverlässigkeitsprüfung verweigert hat. Außerdem sollte in den Gesetzestext eingefügt werden, dass eine Sicherheitsüberprüfung mit Auskunft des Bundeszentralregistergesetzes, mit Erkenntnissen der Polizeibehörden oder/und mit einer Abfrage beim Landesamt für Verfassungsschutz nur dann durchgeführt werden darf, wenn konkrete sicherheitsrelevante Erkenntnisse über diesen Besucher bekannt sind. Nur so wird durch die Konkretheit dem Verhältnismäßigkeitsgrundsatz Rechnung getragen.

Der Besuch in den Justizvollzugsanstalten und in der Sicherungsverwahrungsvollzugsanstalt erfüllt eine wichtige Funktion. Hierdurch werden soziale Kontakte aufrechterhalten und es wird den menschlichen Erfordernissen nach einer Pflege von Beziehung mit der Umwelt Rechnung getragen. Insbesondere auch im Hinblick auf junge Gefangene und Familien verweisen wir auf Art. 6 Abs. 2 GG und die besondere Bedeutung und den Schutz familiärer Kontakte.

Mit freundlichen Grüßen
i. A.

Magdalene Kläver

Rechtsanwältin Prof. Dr. Magdalene Kläver
- Justiziarin des Kommissariats -

Anlagen 1 - 3

Anlage 1

Ministerium für
Inneres, Bauen
und Sport

SAARLAND

Katholisches Büro Saarland
z.Hd. Herrn Prälat Dr. Prassel
Postfach 10 24 34
66024 Saarbrücken

Abteilung B:
Staatshoheitsangelegenheiten

Bearbeiter: Martin Mohr
Tel.: 0681 501 - 2693
Fax: 0681 501 - 2699
E-Mail:
m.mohr@innen.saarland.de
Datum: 6. Dezember 2017
Az.: B4 - 2010 - 3

Kirchliches Datenschutzrecht
Formulierungsvorschlag betreffend Vollstreckungshilfe durch staatliche Stellen des Landes
Zuletzt Ihr Schreiben vom 12. Oktober 2017

Sehr geehrter Herr Prälat Dr. Prassel,

ich komme zurück auf Ihr Schreiben vom 12. Oktober 2017, mit dem Sie um Aufnahme eines Formulierungsvorschlags in das Saarländische Datenschutzgesetz oder in das Saarländische Verwaltungsvollstreckungsgesetz gebeten haben. Der Formulierungsvorschlag soll die Vollstreckung von Geldbußen, die ein kirchlicher Datenschutzbeauftragter verhängt hat, durch die für die Verwaltungsvollstreckung zuständigen Behörden des Landes im Wege der Vollstreckungshilfe ermöglichen.
Nach erster Prüfung Ihres Anliegens kann ich Ihnen mitteilen, dass wir fachlicherseits Ihrem Anliegen gerne entgegenkommen werden. Vorbehaltlich der Zustimmung der Hausspitze ist geplant, Ihr Anliegen im Saarländischen Verwaltungsvollstreckungsgesetz sinngemäß zu berücksichtigen.

Sobald die Angelegenheit es zulässt, werden wir auf Sie zukommen.

Mit freundlichen Grüßen
Im Auftrag

Mohr
Mohr

Anlage 2

Bundesland	Friedhofsrecht	Kirchensteuerrecht
Sachsen Anhalt	**Schlussprotokoll zu Artikel 16 des Konkordats zwischen dem Heiligen Stuhl und dem Land Sachsen-Anhalt vom 31. März 1998** *„Die Träger kirchlicher Friedhöfe können nach den für die Kommunen geltenden Grundsätzen Benutzungs- und Gebührenordnungen erlassen. Die Friedhofsgebühren werden auf Antrag des kirchlichen Trägers im Vollstreckungsverfahren durch die zuständige kommunale Vollstreckungsbehörde eingezogen. Die durch die Vollstreckungsmaßnahmen entstehenden und nicht beitreibbaren Verwaltungskosten und –auslagen sind der vollstreckungsbehörde vom kirchlichen Träger zu erstatten."*	
Nordrhein-Westfalen	**§ 4 Absatz 3 Gesetz über das Friedhofs- und Bestattungswesen (Bestattungsgesetz - BestG NRW) vom 17.06.2003** *(3) Gebühren, die eine Religionsgemeinschaft für die Benutzung ihres Friedhofs und seiner Einrichtungen erhebt, können im Verwaltungszwangsverfahren beigetrieben werden, wenn die Satzung von der nach § 2 Abs. 1 Satz 2 zuständigen Behörde genehmigt worden ist.*	**Kirchensteuergesetz** **§ 8 Absatz 1** *Die Vorschriften der Abgabenordnung und des Verwaltungszustellungsgesetzes finden in der jeweils geltenden Fassung auf die Kirchensteuern entsprechende Anwendung, soweit nicht in diesem Gesetz eine besondere Regelung getroffen ist.* **§12** *Wird die Kirchensteuer von den Kirchen selbst verwaltet, so wird die Kirchensteuer einschließlich der Nebenleistungen auf Antrag durch die Finanzämter nach den Vorschriften der Abgabenordnung oder durch die kommunalen Vollstreckungsbehörden, soweit diese die Maßstabsteuern einziehen, nach den Vorschriften über das Verwaltungszwangsverfahren beigetrieben.*

(weiter Nordrhein-Westfalen)	**Verwaltungsvorschriften zum Verwaltungsvollstreckungsgesetz (VV VwVG NRW) vom 09.10.2004** ***Nr. 2.2.2.2 Satz 6*** *Sollen andere öffentlich-rechtliche Forderungen der Kirchen und Religionsgemeinschaften als Kirchensteuern, z.B. Friedhofsgebühren, beigetrieben werden, so ist nach Nr. 2.2.3 zu verfahren.* ***Nr. 2.2.3*** *Fehlen entsprechende Vorschriften, so bestimmt die Bezirksregierung gemäß § 2 Abs. 2 Satz 2 VwVG NRW eine Vollstreckungsbehörde, und zwar für den Einzelfall - entsprechend der gesetzlichen Regelung für vergleichbare Fälle in § 4 Abs. 2 OBG - im Verwaltungswege, als allgemeine Zuständigkeitsregelung für die Dauer jedoch durch Verordnung. Zuständig ist die Bezirksregierung, in deren Bezirk die Vollstreckungsmaßnahme durchgeführt werden soll oder in deren Bezirk der Gläubiger seinen Sitz hat. Die von der Bezirksregierung bestellte Vollstreckungsbehörde muss außerhalb ihres Bereichs ggf. die Amtshilfe anderer Vollstreckungsbehörden in Anspruch nehmen.*	**Verwaltungsvorschriften zum Verwaltungsvollstreckungsgesetz (VV VwVG NRW) vom 09.10.2004** ***Nr. 2.2.2.2 Sätze 1 bis 5*** *Vollstreckungsbehörden für die Kirchen (Kirchengemeinden) und die Religionsgemeinschaften, welche die Rechte einer Körperschaft des öffentlichen Rechts haben, sind, soweit es sich um die Beitreibung von Kirchensteuern einschl. Kirchgeld handelt, grundsätzlich die Finanzämter (§§ 8 Abs. 1 und 15 Kirchensteuergesetz (KiStG) v. 22. April 1975 - SGV. NRW. 610 -). Kommunale Vollstreckungsbehörden sind nur zuständig für die Beitreibung der „Kirchensteuer vom Grundbesitz", die als Zuschlag zu den Grundsteuermessbeträgen erhoben wird. Dies gilt sowohl, wenn die Kirchensteuer vom Grundbesitz durch die Gemeinden (GV) verwaltet wird (§ 11 aaO), als auch dann, wenn sie von den Kirchen selbst verwaltet wird, die Gemeinden (GV) aber die „Maßstabsteuern" einziehen (§ 12 aaO). In beiden Fällen haben die Gemeinden (GV) das VwVG NRW anzuwenden. Das ergibt sich, unbeschadet des Hinweises auf die AO in §8 KiStG, schon aus der Gegenüberstellung der „Vorschriften über das Verwaltungszwangsverfahren" und der „Vorschriften der Abgabenordnung" in § 12 aaO.*
Niedersachsen	**§ 17 Bestattungsgesetz vom 08.12.2005** *„Bei kirchlichen Friedhofsgebühren, die aufgrund kirchenbehördlich genehmigter Gebührenordnungen durch Bescheid des Friedhofsträgers festgesetzt wurden, sind die Gemeinden zur Vollstreckungshilfe verpflichtet."*	**§ 15 Kirchensteuergesetz** *„Die Vollstreckung der staatlich genehmigten Kirchensteuer obliegt den Finanzämtern und in den Fällen des § 14 den Gemeinden, den Landkreisen oder deren Hebestellen. Diese können auch in*

		anderen Fällen die Vollstreckung durch Vereinbarung übernehmen. Die Gemeinden, Landkreise oder deren Hebestellen vollstrecken die Kirchensteuer nach den Vorschriften über das Verwaltungszwangsverfahren."
Thüringen	**Schlussprotokoll zu Artikel 17 des Vertrags zwischen dem Heiligen Stuhl und dem Freistaat Thüringen vom 11. Juni 1997** *(3) Benutzungs- und Gebührenordnungen für kirchliche Friedhöfe bedürfen der Genehmigung der für das Bestattungswesen zuständigen Behörden. Die Friedhofsgebühren werden auf Antrag des kirchlichen Rechtsträgers im Verwaltungsvollstreckungsverfahren eingezogen.*	

Anlage 3

WESTFÄLISCHE
WILHELMS-UNIVERSITÄT
MÜNSTER

Institut für Europäisches Verwaltungsrecht

Prof. Dr. Gernot Sydow, M.A., Universitätsstr. 14-16, D-48143 Münster

Prof. Dr. Gernot Sydow, M.A.

D - 48143 Münster, Universitätsstr. 14-
Tel.: 0251 / 83 - 2 19 43
E-Mail: Gernot.Sydow@uni-muenster.de

21. Dezember 2017

Vermerk:

Vollstreckung kirchlicher Bußgeldbescheide im Bereich des Datenschutzrechts

1. Die Verfasstheit der Kirchen als Körperschaften des öffentlichen Rechts verleiht ihnen hoheitliche Befugnisse, aber keine physische Zwangsgewalt. Diese liegt entsprechend dem staatlichen Gewaltmonopol ausschließlich beim Staat. Da der Staat nicht-staatlichen Institutionen mit Ausnahme von Notwehrsituationen eine zwangsweise Durchsetzung eigener Rechtspositionen verwehrt, muss er ihnen im Gegenzug für diese Zwecke effektive staatliche Verfahren zur Verfügung stellen: Vollstreckungshilfe, Gerichtsverfahren, Mahnverfahren etc. Einen Anspruch auf ein ganz bestimmtes staatliches Verfahren gibt es nicht. Es wäre aber konsequent und aus Gründen der Effektivität des Datenschutzes naheliegend, dass der Staat für die Vollstreckung kirchlicher Bußgeldbescheide im Bereich des Datenschutzrechts einen Rückgriff auf diejenigen staatlichen Organe und Verfahren ermöglicht, die der Staat auch zur Vollstreckung eigener, staatlicher Bescheide nutzt.

2. Solange das Landesrecht keine speziellen Vollstreckungsregelungen für Bußgeldbescheide kirchlicher Datenschutzbeauftragter enthält, kann eine Forderung aus einem kirchlichen Bußgeldbescheid nur im Rahmen eines staatlichen Gerichtsverfahrens tituliert und auf dieser Grundlage sodann durch die Kirchen selbst vollstreckt werden.

3. Die Titulation einer Forderung aus einem Bußgeldbescheid in einem staatlichen Gerichtsverfahren erfordert zwingend einen zeitlichen und finanziellen Mehraufwand. Damit wären Einbußen in der Effektivität des kirchlichen Datenschutzes verbunden. Das würde der Zielsetzung der europäischen Datenschutz-Grundverordnung nicht gerecht werden, die von einer prinzipiellen Gleichwertigkeit staatlicher und kirchlicher Datenschutzkonzeptionen ausgeht und deswegen im kirchlichen Bereich eine Surrogation der staatlichen Da-

tenschutzaufsicht durch eine ebenso unabhängige und effektiv arbeitende kirchliche Datenschutzaufsicht ermöglicht (Art. 91 DSGVO).

4. Ohne eine wirksame Möglichkeit zur Vollstreckung kirchlicher Bußgeldbescheide im Bereich des Datenschutzrechts entstünde ein Wertungswiderspruch: Art. 91 Abs. 1 DSGVO würde zwar prima facie akzeptieren, dass kirchliche Datenschutzregeln anwendbar sind, die materiell der DSGVO gleichkommen. Dafür würde aber ein Durchsetzungsdefizit in Kauf genommen. Denn sofern im kirchlichen Bereich niemand ernsthaft fürchten müsste, für Normverstöße mit einem Bußgeld belegt zu werden, das zeitnah beigetrieben werden kann, dürfte auch die Bereitschaft sinken, sich datenschutzkonform zu verhalten.

5. Hinzu tritt der unionsrechtliche Grundgedanke des effet utile nach Art. 4 Abs. 3 EUV, nach dem unionsrechtlichen Normen zu größtmöglicher Wirkung verholfen werden soll. Art. 91 Abs. 1 DSGVO will einerseits ein bestimmtes materielles Datenschutzniveau auch in den Kirchen absichern, andererseits aber dem verfassungsrechtlichen Selbstbestimmungsrecht der Kirchen Rechnung tragen, dem insb. auch das Recht zur Rechtsetzung in eigenen Angelegenheiten unterfällt. Will man wegen des effet utile beide in Art. 91 Abs. 1 DSGVO niedergelegte Ziele bestmöglich verwirklichen, muss dem kirchlichen Recht eine dem staatlichen Recht vergleichbare Durchschlagskraft zugesprochen werden.

6. Das nordrhein-westfälische Landesrecht kennt bereits im Friedhofsgebührenrecht (§ 4 Abs. 3 FriedhofsG NRW) sowie im Kirchensteuerrecht (§ 12 KirchensteuerG NRW) den Mechanismus, dass kirchliche Bescheide durch staatliche Stellen ohne ein neuerliches Titulierungsverfahren vollstreckt werden. Auch weitere Länder wie Niedersachsen und Thüringen haben derartige Regelungen geschaffen. Mit der Einführung solcher Regelungen auch für Bußgeldbescheide kirchlicher Datenschutzbeauftragter würde demnach lediglich ein etabliertes Regelungskonzept auf ein weiteres Rechtsgebiet erstreckt.

7. Regelmäßig wird der Staat, bevor er seine Zwangsgewalt zur Durchsetzung von Forderungen von Privatpersonen oder nicht-staatlicher Institutionen gegenüber Dritten einsetzt, die Berechtigung der behaupteten Forderung am Maßstab des staatlichen Rechts prüfen müssen. In der Regel erfolgt dies als Vollprüfung im Rahmen eines gerichtlichen Klageverfahrens. Nur in Ausnahmefällen kann der Staat auf Basis einer staatlichen Gesetzgebung von einer Vollprüfung absehen und Feststellungen oder Entscheidungen nichtstaatlicher Stellen für das staatliche Vollstreckungsverfahren für bindend erklären. Das kommt z.B. bei der Vollstreckung privater Schiedsurteile oder auch von Bußgeldbescheiden kirchlicher Datenschutzbeauftragter in Betracht. Für einen solchen Ansatz hat sich Nordrhein-Westfalen im Friedhofsrecht entschieden, indem gem. § 4 Abs. 3 FriedhofsG NRW Gebührenordnungen zunächst der staatlichen Zustimmung bedürfen, bevor Bescheide auf dieser Grundlage staatlich vollstreckbar sind.

8. Eine solche staatliche Anerkennung der kirchlichen Normen, auf deren Grundlage zu vollstreckende Bußgeldbescheide beruhen können, erscheint auch für die zu schaffenden Regelungen über die Bußgelder kirchlicher Datenschutzbeauftragter als ein realisierbarer Weg: Einerseits kann der Staat damit sicherstellen, dass die Bußgeldandrohungen kirchlicher Datenschutzaufsichten abstrakt verhältnismäßig sind und auf Regelungen beruhen, die dem staatlichen bzw. europäischen Datenschutzrecht entsprechen. Andererseits kann der Staat auf eine kleinteilige und ressourcenaufwändige Kontrolle jedes einzelnen Bußgeldbescheids verzichten, sodass das Vollstreckungsverfahren insgesamt effizient ausgestaltet wird.

9. Staatliche Vollstreckungsmaßnahmen stellen einen Grundrechtseingriff für den mit dem Bußgeld Beschwerten dar, zu dessen Rechtfertigung es wegen des Gesetzesvorbehalts eines Parlamentsgesetzes bedarf. Es muss jedenfalls das Wesentliche regeln. Die Möglichkeit für kirchliche Datenschutzaufsichten, staatliche Vollstreckungsorgane in Anspruch zu nehmen, ist eine wesentliche, der Gesetzesform bedürftige Regelung.

10. Nach § 1 Abs. 1 S. 2 VwVG NRW gilt das VwVG NRW auch für die Beitreibung von Forderungen öffentlich-rechtlicher Natur solcher Stellen und Personen, denen durch Gesetz hoheitliche Aufgaben übertragen sind. Diese Norm ist für Fälle der Beleihung nach deutschem Recht geschaffen worden.

11. Es spricht nichts dagegen, unter diese Norm auch eine Konstellation wie in Art. 91 DSGVO zu subsumieren, in der nicht-staatliche Stellen oder Personen auf europarechtlicher Grundlage hoheitliche Aufgaben wahrnehmen können und in diesem Rahmen durch Erlass von Bußgeldbescheiden öffentlich-rechtliche Forderungen begründen, die der Beitreibung bedürfen. Eine solche Erweiterung des Anwendungsbereichs staatlicher Normen über den ursprünglichen staatlichen Kontext hinaus auf europarechtlich geregelte Konstellationen ist in sämtlichen Rechtsgebieten ständige Praxis und von der Normauslegung gedeckt.

12. Der Gesetzesvorbehalt erfordert demnach keine neue staatliche Regelung auf Ebene des formellen Gesetzes, um eine Vollstreckung kirchlicher Bußgeldbescheide im Bereich des Datenschutzrechts zu ermöglichen. Ihm wird durch das VwVG NRW hinreichend Rechnung getragen. Der Landesgesetzgeber wäre selbstverständlich nicht gehindert, eine weitere, speziellere Regelung, etwa im Landesdatenschutzgesetz, zu schaffen, die speziell auf die Vollstreckung von Bußgeldbescheiden kirchlicher Datenschutzaufsichten Bezug nimmt.

13. Auf der Grundlage des § 1 Abs. 1 S. 2 VwVG NRW können Einzelheiten über die Zu-

ständigkeiten, das Verfahren, die Kostentragung einer Vollstreckung kirchlicher Bußgeldbescheide zulässigerweise in Ministerialverordnungen geregelt werden. Dieser Regelungstechnik folgt bereits das Kirchensteuerrecht in NRW: In § 12 KirchensteuerG wird die grundsätzliche Möglichkeit der staatlichen Beitreibung von Kirchensteuern eröffnet; alles Weitere findet sich dann in Verwaltungsvorschriften, die ohne Mitwirkung des parlamentarischen Gesetzgebers erlassen worden sind (dort in den VV VwVG).

(Gernot Sydow)

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 07.03.2018

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Hessischen Landtags

am 15. März 2018

zum

Gesetzentwurf der Fraktionen der CDU und Bündnis 90/DIE Grünen für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit

A. Einleitung

Den o. a. Gesetzentwurf habe ich vor allem unter dem Gesichtspunkt geprüft, inwieweit die darin vorgesehenen Regelungen das Bund-Länder-Verhältnis und die Zusammenarbeit zwischen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem Hessischen Datenschutzbeauftragten insbesondere in EU-Angelegenheiten berühren. Des Weiteren habe ich die europarechtlichen Aspekte des Art. 1 des Gesetzentwurfs, mit dem ein neues Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) geschaffen wird, in den Blick genommen.

Der o. a. Gesetzentwurf enthält aus meiner Sicht keine Regelungen, die sich nachteilig auf die Zusammenarbeit der Datenschutzaufsichtsbehörden des Bundes und der Länder auswirken könnten. Vor diesem Hintergrund beschränkt sich meine Stellungnahme auf die Frage, inwieweit Art. 1 des o. a. Gesetzentwurfes mit den einschlägigen europarechtlichen Bestimmungen im Einklang steht. Bei den Regelungen zur Auftragsverarbeitung (§ 3 Abs. 2 HDSIG-E), zur Videoüberwachung (§ 4 HDSIG-E) sowie bei einzelnen Einschränkungen von Betroffenenrechten (§§ 31 ff. HDSIG-E) bestehen zumindest Zweifel, ob sie sich im Rahmen der in der Datenschutz-

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Grundverordnung vorgesehenen Öffnungsklauseln bewegen und daher als europarechtlich zulässig anzusehen sind. Im Einzelnen bemerke ich Folgendes:

B. Auftragsverarbeitung (§ 3 Abs. 2 HDSIG-E)

Durch § 3 Abs. 2 S. 1 HDSIG-E werden Verantwortliche verpflichtet, sicherzustellen, dass Auftragsverarbeiter, auf die das HDSIG keine Anwendung findet, die Vorschriften des HDSIG beachten. Damit wird laut Gesetzesbegründung die bestehende Regelung des § 4 Abs. 3 S. 1 HDSG teilweise übernommen, um sicherzustellen, dass „der Schutz der Rechte betroffener Personen nicht durch ggf. abweichende gesetzliche Regelungen gemindert wird, wenn der Auftragsverarbeiter seinen Sitz außerhalb Hessens hat.“ Meines Erachtens ist diese Regelung zum einen überflüssig, denn sowohl die Grundsätze der Datenverarbeitung (Art. 28 DSGVO) als auch der Schutz der Rechte der Betroffenen (Kapitel III DSGVO) ergeben sich künftig unmittelbar aus der DSGVO. Sie sind damit unabhängig von einem Sitz des Auftragsverarbeiters in Hessen zu beachten. Zum anderen ist die Regelung auch europarechtlich zumindest zweifelhaft, denn eine entsprechende Öffnungsklausel in der DSGVO ist nicht ersichtlich. So hat etwa der Bundesgesetzgeber in dem ab 25.5.2018 geltenden neuen Bundesdatenschutzgesetz von jeglichen Regelungen zur Auftragsverarbeitung Abstand genommen.

Gemäß § 3 Abs. 2 S. 2 HDSIG-E soll in Anlehnung an den geltenden § 4 Abs. 4 HDSG die Durchführung von Wartungsarbeiten in die Auftragsverarbeitung mit einbezogen werden. Ich habe starke Zweifel, ob diese Regelung europarechtlich zulässig ist, denn die Definition des Begriffs „Auftragsverarbeiters“ wird unmittelbar in Art. 4 Nr. 8 DSGVO vorgenommen. Gleiches gilt für den Begriff des „Verantwortlichen“ (Art. 4 Nr. 7 DSGVO) und somit für die Abgrenzung zwischen den beiden Rechtsinstituten. Zwar sind die entsprechenden Definitionen in der DSGVO nicht umfassend und bedürfen an der einen oder anderen Stelle der Präzisierung. Diese darf jedoch aus europarechtlicher Sicht nicht durch die nationalen Gesetzgeber vorgenommen werden, denn dadurch würde die durch die DSGVO unmittelbar bezweckte einheitliche Rechtsanwendung in Europa (vgl. Erwägungsgrund 10 DSGVO) beeinträchtigt.

Was Auftragsdatenverarbeitung ist und was nicht, kann – auch im öffentlichen Bereich – in Deutschland nicht anders beurteilt werden als in Spanien und in Hessen nicht anders als in Bayern. In diesem Zusammenhang weise ich auch auf die von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in Form von Kurzpapieren veröffentlichten Auslegungs- und Anwendungshinweise zur

Datenschutz-Grundverordnung hin. Im Kurzpapier zur Auftragsverarbeitung nach Art. 28 DSGVO vertritt die Konferenz zu der Frage, ob Wartungsarbeiten als Auftragsverarbeitung anzusehen sind, je nach Gegenstand der beauftragten Arbeiten und ob dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, eine differenzierte Position. Wartungsarbeiten fallen demnach nicht in jedem Falle als Auftragsverarbeitung in den Anwendungsbereich des Art. 28 DSGVO.

C. Videoüberwachung (§ 4 HDSIG-E)

Die Vorschrift zur Videoüberwachung ist aus meiner Sicht ebenso problematisch, wie die entsprechende Regelung im neuen Bundesdatenschutzgesetz (§ 4 BDSG-neu) und z. T. möglicherweise aus europarechtlichen Gründen unanwendbar. Wie im BDSG werde laut Gesetzesbegründung zu § 4 Abs. 1 Nr. 3 HDSIG-E die Interessenabwägung nach Art. 6 Abs. 1 lit. f) DSGVO konkretisiert. Art. 6 Abs. 1 lit. f) DSGVO gibt jedoch keinen Regelungsspielraum und dürfte daher als abschließend anzusehen sein. Die DSGVO erlaubt insoweit einen angemessenen Ausgleich zwischen den berechtigten Interessen der Verantwortlichen an einer Videoüberwachung und dem Schutz der Persönlichkeitsrechte der Betroffenen, ohne dass es einer konkretisierenden Regelung durch den nationalen Gesetzgeber bedarf. Die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder hat daher in ihren Grundsatzpositionen und Forderungen zur neuen Legislaturperiode des Deutschen Bundestages gefordert, § 4 BDSG-neu zu streichen, soweit die Regelung eine Konkretisierung des Art. 6 Abs. 1 Satz 1 lit. f) DSGVO betrifft.

Zudem ist zu bedenken, dass das Hessische Datenschutz- und Informationsfreiheitsgesetz gem. § 1 Abs. 1 HDSIG-E nur für öffentliche Stellen gilt. Im Bereich der Verarbeitung personenbezogener Daten durch öffentliche Stellen ist für eine Interessenabwägung kein Raum, wie Art. 6 Abs. 1 Satz 2 DSGVO ausdrücklich klarstellt. § 4 Abs. 1 Nr. 3 HDSIG-E sollte dementsprechend gestrichen werden.

D. Einschränkungen von Betroffenenrechten (§§ 31 ff. HDSIG-E)

In den §§ 31-35 des Gesetzentwurfs sind verschiedene Einschränkungen von Betroffenenrechten (Informationspflicht, Auskunftsrecht, Recht auf Löschung, Widerspruchsrecht) vorgesehen. Die Beschränkungen orientieren sich weitgehend, aber nicht vollständig an den in den §§ 32-36 BDSG-neu enthaltenen Regelungen.

Grundsätzlich sind Beschränkungen von Betroffenenrechten durch die jeweiligen nationalen Gesetzgeber zwar auf Grundlage des Art. 23 DSGVO möglich. Beschränkungen dürfen aber nicht den Wesensgehalt der Grundrechte und Grundfreiheiten tangieren, müssen in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahmen darstellen sowie die in Art. 23 Abs. 1 DSGVO aufgezählten Ziele sicherstellen. Diesen Voraussetzungen nicht genügende, übermäßige Einschnitte in die Betroffenenrechte widersprechen dem Schutzcharakter der DSGVO und sind unzulässig.

Vor diesem Hintergrund habe ich Zweifel an der Zulässigkeit der folgenden, im Entwurf des Hessisches Datenschutz- und Informationsfreiheitsgesetz enthaltenen Regelungen der Beschränkung von Betroffenenrechten:

Gem. § 31 Abs. 1 S. 1 Nr. 2 li c) HDSIG-E soll die Informationspflicht nach Art. 13 Abs. 3 DSGVO, also bei einer Weiterverarbeitung zu einem anderen Zweck als dem, zu dem die Daten erhoben wurden, dann nicht gelten, wenn die Information die Rechte oder Freiheiten Dritter gefährden würde und das Interesse des Verantwortlichen an der Nichterteilung der Information das Informationsinteresse der betroffenen Person überwiegt. Zwar werden in Art. 23 Abs. 1 lit. i) DSGVO die Rechte und Freiheiten Dritter ausdrücklich als legitimer Zweck einer Einschränkung von Betroffenenrechte genannt. Gleichwohl halte ich die vorgesehen Regelung, die im neuen BDSG auch keine Entsprechung hat, nicht für gerechtfertigt: Art. 23 Abs. 1 DSGVO lässt solche Regelungen nur zu, wenn sie in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind. Es wird nicht deutlich, dass diese Voraussetzungen hier erfüllt sind. Vielmehr wird allein auf Grundlage einer Interessenabwägung nicht näher bestimmten Rechten und Freiheiten Dritter Vorrang vor dem Informationsanspruch von einer zweckändernden Datenverarbeitung Betroffener eingeräumt. Hinzukommt, dass bereits eine Gefährdung der Rechte und Freiheiten Dritter ausreichen soll, eine tatsächliche Beeinträchtigung also gar nicht vorliegen muss.

Auch § 31 Abs. 1 S.1 Nr. 3 HDSIG-E (Beschränkung der Informationspflicht bei einer Gefährdung der vertraulichen Übermittlung von Daten an öffentliche Stellen) sollte gestrichen werden. Die Norm eröffnet einen weiten Spielraum. Die Begründung stellt klar, dass sich die Ausnahme auf Fälle bezieht, in denen eine Informationserteilung zu einer Vereitelung oder ernsthaften Beeinträchtigung des Verarbeitungszwecks führen würde. Dies ist aber m.E. durch § 31 Absatz 1 S. 1 Nummer 2 lit. a) HDSIG-E (Gefährdung der Aufgabenerfüllung öffentlicher Stellen) und lit b) (Gefährdung der öffentlichen Sicherheit und Ordnung) bereits ausreichend abgedeckt. „Vertraulichkeit“ als solche ist kein Schutzgut i. S. v. Art. 23 Abs. 1 DSGVO, vielmehr sind bestimmte Zwecke der Datenverarbeitung zu schützen, was – wie dargelegt – bereits durch andere Tatbestände sichergestellt wird.

Ähnliche Bedenken habe ich auch bei den Einschränkungen des Auskunftsrechts gemäß § 33 Abs. 1 Nr. 2 HDSIG-E. Die Einschränkung soll u.a. gelten, wenn Daten nur aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder diese ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen. Schon bei der entsprechenden Regelung im Bundesrecht (§ 34 Abs. 1 Nr. 2 BDSG-neu) ist aus meiner Sicht fraglich, ob sie den strengen Anforderungen des Art. 23 DSGVO genügt. In der nun für Hessen vorgesehen Regelung fehlt jedoch sogar die im BDSG-neu enthaltene zusätzliche Voraussetzung, wonach das Auskunftsrecht in den in Nr. 2 a) und b) beschriebenen Fällen nur dann entfällt, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Was den hessischen Gesetzentwurf angeht, gibt es aus meiner Sicht überhaupt keinen Grund, weshalb das Auskunftsrecht betroffener Personen nicht bestehen soll, wenn Daten wegen gesetzlicher Aufbewahrungsfristen nicht gelöscht werden dürfen oder sie nur zu Zwecken der Datensicherung gespeichert werden. Auch dann haben Betroffene ein berechtigtes, von der DSGVO anerkanntes Interesse daran, zu erfahren, welche ihrer Daten zu welchen Zwecken verarbeitet werden. Der in der Gesetzesbegründung enthaltene Verweis auf das bestehende Hessische Datenschutzrecht vermag die Beschränkung des Auskunftsrechts nicht zu rechtfertigen.

DJV-Landesverband Hessen e.V.
Landesfachbereich Medien ver.di Hessen
SZV Südwestdeutscher Zeitschriftenverlegerverband e.V.
Verband Hessischer Zeitungsverleger e.V.

BDZV Bundesverband Deutscher Zeitungsverleger e. V.
dju Deutsche Journalisten- und Journalistinnen-Union
DJV Deutscher Journalisten-Verband
Deutscher Presserat
VDZ Verband Deutscher Zeitschriftenverleger e. V.

Stellungnahme

(Stand: 6. März 2018)

zur

Neufassung des § 10 des hessischen Pressegesetzes
durch Art. 14 des
Gesetzentwurfes der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit,

Drucksache 19/5728 des Hessischen Landtags v. 5.12.2017

– im Folgenden: Gesetzentwurf –

zugleich:

Stellungnahme
zur Vorbereitung der mündlichen Anhörung im Hessischen Landtag
am 15. März 2018

Geltendes Recht: § 10 des Hessischen Pressegesetzes in der Fassung der Bekanntmachung vom 12. Dezember 2003 (GVBl. 2004 I S. 2), zuletzt geändert durch Gesetz vom 13. Dezember 2012 (GVBl. S. 622) – im Folgenden § 10 HPresseG, lautet:

§ 10 HPresseG

Soweit Unternehmen oder Hilfsunternehmen der Presse personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken erheben, verarbeiten oder nutzen, gelten von den Vorschriften des Bundesdatenschutzgesetzes in der jeweils geltenden Fassung nur die §§ 5, 9 und § 38a sowie § 7 mit der Maßgabe, dass nur für Schäden gehaftet wird, die durch eine Verletzung des Datengeheimnisses nach § 5 des Bundesdatenschutzgesetzes oder durch unzureichende technische oder organisatorische Maßnahmen im Sinne des § 9 des Bundesdatenschutzgesetzes eintreten.

Gesetzentwurf: Die vorgeschlagene Neufassung des § 10 HPresseG durch Art. 14 des Gesetzentwurfes auf Drs. 19/5728 – im Folgenden § 10 HPresseG-Entwurf – lautet:

§ 10 HPresseG-Entwurf

[1]Soweit Unternehmen und Hilfsunternehmen der Presse personenbezogene Daten zu journalistischen oder literarischen Zwecken verarbeiten, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). [2]Bei der Aufnahme ihrer Tätigkeit sind diese Personen auf das Datengeheimnis zu verpflichten. [3]Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. [4]Im Übrigen finden für die Datenverarbeitung zu journalistischen oder literarischen Zwecken außer den Kapiteln I, X und XI nur Art. 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Art. 24 Abs. 1 Satz 1 und Abs. 2, Art. 32 Abs. 1 Buchst. b bis d, Abs. 2 und 4 und Art. 82 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) sowie § 83 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) in der jeweils geltenden Fassung Anwendung. [5]Art. 82 der Verordnung (EU) 2016/679 findet nur bei einem Verstoß gegen Art. 5 Abs. 1 Buchst. f, Art. 24 Abs. 1 Satz 1 und Abs. 2 sowie Art. 32 Abs. 1 Buchst. b bis d, Abs. 2 und 4 der Verordnung (EU) Nr. 2016/679 Anwendung. [6]§ 83 des Bundesdatenschutzgesetzes findet mit der Maßgabe Anwendung, dass nur für eine Verletzung des Datengeheimnisses nach Satz 1 bis 3 gehaftet wird.

A Wesentliche Aussagen

Die Landes- und Bundesverbände der Journalisten und Presseverleger begrüßen den Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN zur Änderung des § 10 des hessischen Pressegesetzes mit Nachdruck.

Der Entwurf schreibt unverzichtbaren Schutz der redaktionellen Pressefreiheit durch Umstellung auf das ab Mai 2018 geltende Datenschutzrecht ohne Abstriche fort. Unverändert gelten nach § 10 HPresseG-Entwurf für die redaktionelle Datenverarbeitung nur Datengeheimnis und Datensicherheit. Und ebenso unverändert sind diese beiden Verpflichtungen nur durch Gerichte im Wege der Unterlassung- oder Schadensersatzklage durchsetzbar, nicht aber durch behördliche Aufsicht. Schließlich kommt ebenso unverändert die Beschwerde bei der redaktionellen Selbstkontrolle des Presserates als von Verlagen und Journalisten freiwillig eingeräumte Möglichkeit der Selbstkorrektur hinzu, ist aber keine rechtliche Bedingung der Freiheit von behördlicher Aufsicht.

Der so skizzierte Schutz der Redaktionen gegen Datenschutzrecht und datenschutzbehördliche Aufsicht ist unverzichtbar für den Erhalt der Pressefreiheit in Deutschland und Europa.

Zu Recht geht der Gesetzentwurf davon aus, dass die Datenschutzgrundverordnung keinerlei neue Einschränkung dieses sogenannten Presseprivilegs verlangt. Und ebenso zu Recht geht er davon aus, dass es auch keine legitimen politischen Gründe gibt, den Schutz der Pressefreiheit gegen Datenschutzrecht und -aufsicht zu beschneiden.

Mit Art. 85 Abs. 1 und Abs. 2 DSGVO hat Deutschland das Ziel erreicht, dass in der EU-Datenschutzgrundverordnung *„das für Presse- und Medienfreiheit unabdingbare Medienprivileg effektiv ausgestaltet wird“* (S. 104 KV vom Dezember 2013). Art. 85 DSGVO erweitert sogar die Befugnis der Mitgliedsstaaten zu eigenen Rechtsvorschriften im Bereich der journalistischen Datenverarbeitung und gestatten es jedenfalls, die bestehenden Regelungen zum Schutz redaktioneller Presse- und Medienfreiheit ohne Abstriche beizubehalten.

In diesem Sinne erklärt der Bundesgesetzgeber, der wegen Wegfalls der Bundesrahmengesetzgebungskompetenz für die Presse im BDSG (neu) kein dem § 41 BDSG (alt) entsprechendes Medienprivileg mehr normieren kann, er, der Bundesgesetzgeber, gehe *„davon aus, dass die insofern zuständigen Landesgesetzgeber das Pressprivileg* ***wie bisher*** *absichern werden“* (BT-Drs. 18/11325 vom 24.02.2017, S. 79, Hervorhebung nur hier).

§ 10 HPresseG-Entwurf wird diesem Anspruch gerecht, indem er die geltenden Vorgaben zu Datensicherheit und Datengeheimnis sowie entsprechender Haftungsregeln durch Verweise auf entsprechende Normen in Datenschutzgrundverordnung (DSGVO) und BDSG (neu) aktualisiert und dabei klarstellt, dass DSGVO und BDSG (neu) im Übrigen auf

die Verarbeitung personenbezogener Daten zu journalistischen Zwecken keine Anwendung finden.

Im Einzelnen:

1. Die Freiheit der Presse setzt voraus, dass weder Datenschutzrecht noch Datenschutzaufsicht auf die redaktionelle Arbeit von der Recherche bis zur Veröffentlichung Anwendung finden (ausführlich dazu „Arbeitspapier zur Umsetzung des Art. 85 der DSGVO“, Anhang, unter A).

Das stellt § 10 des geltenden hessischen Pressegesetzes ebenso wie § 10 HPresseG-Entwurf sicher, indem beide Normen die redaktionelle Datenverarbeitung nur zu Datensicherheit und Datengeheimnis verpflichten, d. h. zum Schutz der Redaktionsdaten gegen Zweckentfremdung und gegen unbefugte Kenntnisnahme durch Dritte. Dabei besteht im Falle einer Pflichtverletzung die – scharfe – Sanktion gerichtlich durchsetzbarer Schadensersatz- und Unterlassungsansprüche. Das wird de lege lata durch § 10 HPresseG i. V. m. § 7 BDSG bzw. §§ 823 Abs. 2, 1004 BGB angeordnet. Und es bleibt auch de lege ferenda so, wobei § 10 HPresseG-Entwurf allein die Anspruchsgrundlage für den datenschutzrechtlichen Schadensersatzanspruch von § 7 BDSG auf Art. 82 DSGVO (Datensicherheitsverletzungen) bzw. auf § 83 BDSG neu (Datengeheimnisverletzungen) umstellen muss.

Hingegen gibt es völlig zu Recht auch nach § 10 HPresseG-Entwurf keine Zuständigkeit von Datenschutzaufsichtsbehörden zur Überwachung der Redaktionen, was ein wesentliches Element der Pressefreiheit ausmacht. Auch ist diese Freiheit der gedruckten Presse von staatlicher Datenschutzaufsicht gemäß § 10 HPresseG-Entwurf ebenso unbedingt wie schon gemäß § 10 HPresseG. Die freiwillige Selbstkontrolle des Presserates kommt – wie im Bereich des Streites um Verletzung von Persönlichkeitsrechten im Falle der Veröffentlichung personenbezogener Daten durch Presseartikel – als Möglichkeit hinzu, ist aber natürlich keine Bedingung der Freiheit von staatlicher Aufsicht über die Redaktionen. Diese Freiheit der redaktionellen Arbeit der Presse von behördlicher Aufsicht über die inhaltliche Arbeit der Redaktionen ist wesentliches Element der Pressefreiheit seit dem Inkrafttreten des Reichspressegesetzes im Jahre 1874.

2. § 10 HPresseG-Entwurf ist europarechtskonform. Die Freiheit der Redaktionen von behördlicher Aufsicht ist unter der neuen EU-Datenschutzgrundverordnung ebenso europarechtskonform wie unter der noch geltenden EU-RiLi 95/46/EG. Wie das als weiterer Anhang zu dieser Stellungnahme übersandte *Rechtsgutachten von Prof. Dr. Matthias Cornils*, Universität Mainz[1], ausführlich belegt, räumen Art. 85 Abs. 1 und 2 DSGVO den Mitgliedstaaten sogar weitergehende Regelungsmöglichkeiten ein als das geltende Recht.

[1] Professor Dr. Matthias Cornils, Johannes Gutenberg-Universität Mainz, stv. Direktor des Mainzer Medieninstituts: „Das datenschutzrechtliche Medienprivileg unter Behördenaufsicht? Der unionsrechtliche Rahmen für die Anpassung der medienrechtlichen Bereichsausnahmen (in § 9c, § 57 RStV-E und den Landespressegesetzen) an die EU-Datenschutz-Grundverordnung“.

Demnach ist die unveränderte Beibehaltung des Presseprivilegs durch § 10 HPresseG-Entwurf und insbesondere auch der Ausschluss der Art. 77, 78 und 83 DSGVO europarechtlich zulässig.

Zu Recht geht die Begründung zu § 10 HPresseG-Entwurf davon aus, dass die EU-Datenschutzgrundverordnung jedenfalls keinerlei neue Einschränkung des sog. Medienprivilegs verlangt. Art. 85 DSGVO zwingt insbesondere keinesfalls dazu, im Bereich redaktioneller Datenverarbeitung neben dem Weg zu den Gerichten eine behördliche Aufsicht einzuführen. So können unverändert Beschwerderechte zu Aufsichtsbehörden etc. und damit auch die in Kapitel VIII der DSGVO enthaltenen Art. 77, 78 und 83 DSGVO ausgeschlossen werden. Das ist schon aufgrund des Art. 85 Abs. 2 DSGVO möglich. Es ergibt sich aber darüber hinaus auch aus Art. 85 Abs. 1 DSGVO (ausführlich zur Europarechtskonformität der Beibehaltung der geltenden bedingungslosen Freiheit der Redaktionen von datenschutzbehördlicher Aufsicht unten unter B)

3. Ebenso zu Recht erkennt der Entwurf auch keine sonstigen, bspw. politischen Gründe, den Schutz der Pressefreiheit gegenüber Datenschutzrecht und Datenschutzaufsicht weiter zu beschneiden als bisher (auch dazu noch näher unter B).

4. Schließlich sieht § 10 HPresseG-Entwurf zu Recht davon ab, zusätzlich zu den äußerungsrechtlichen und gerichtlich durchsetzbaren Ansprüchen spezifische datenschutzrechtliche Auskunfts-, Berichtigungs- und Löschungsansprüche gegenüber Redaktionsdaten einzuführen. Derartige Ansprüche sind nach wie vor nicht nur nicht sinnvoll, sondern letztlich unangemessen.

B Europarechtliche Zulässigkeit und medienpolitische Notwendigkeit der Beibehaltung der geltenden Pressefreiheit - Anwendbarkeit nur von Datensicherheit, Datengeheimnis und entsprechender Haftungsregelung

Pressefreiheit setzt voraus, dass weder Datenschutzrecht noch Datenschutzaufsicht auf die redaktionelle Verarbeitung personenbezogener Daten Anwendung finden. Diese Existenzbedingung von Pressefreiheit sichert für die gedruckte Presse in Hessen § 10 des geltenden Pressegesetzes.

Möglich sind dabei alleine Vorgaben zu Datensicherheit und Datengeheimnis, die die Verarbeitung journalistischer Daten zu anderen als eben journalistischen Zwecken untersagen. Das Inkrafttreten der DSGVO im Mai 2018 verlangt eine Umstellung des geltenden § 10 HPresseG von einer Ausnahme vom BDSG hin zu einer Ausnahme von der DSGVO und vom BDSG (neu). Minimales Erfordernis für den Schutz des status quo redaktioneller Pressefreiheit ist dabei, dass die Bereichsausnahme des § 10 HPresseG bei der Anpassung inhaltlich unverändert lassen, insbesondere unverändert höchstens Anforderungen an Datensicherheit und Datengeheimnis stellen und auch die Freiheit von der Aufsicht der

Datenschutzaufsichtsbehörden unangetastet bleibt. Beides wird durch § 10 HPresseG-Entwurf geleistet.

Das ist mit der DSGVO ebenso zulässig wie unter der noch geltenden Richtlinie, wie das mit dieser Stellungnahme übersandte Gutachten von Professor Dr. Matthias Cornils, Universität Mainz, ausführlich bestätigt. Art. 85 Abs. 1 DSGVO und Art. 85 Abs. 2 DSGVO ermöglichen es problemlos, die bestehenden Bereichsausnahmen zum Schutz der Pressefreiheit ohne Abstriche aufrecht zu erhalten.

1. Tatsächlich ist die *Verpflichtung* der Mitgliedsstaaten in Art. 85 Abs. 2 DSGVO zu Ausnahmen und Abweichung von den dort genannten Kapiteln sogar noch pressefreiheitsfreundlicher als der bis 2018 geltende Art. 9 der Datenschutzrichtlinie 95/46/EG (DSRiLi).

Und der erstmals zur Ausweitung und Festigung der Kompetenz der Mitgliedsstaaten eingeführte Art. 85 Abs. 1 DSGV, der ebenfalls ausdrücklich die journalistische Datenverarbeitung erfasst, *erlaubt* weitergehend sogar freiheitsangemessene Regelungen über den von Art. 85 Abs. 2 DSGVO *zwingend* erfassten Bereich hinaus.

2. Insbesondere müssen nach Art. 85 DSGVO ebenso wenig wie nach Art. 9 der noch geltenden EU-Datenschutzrichtlinie 95/46/EG – im Folgenden: DSRiLi – die Kapitel über „Allgemeine Bestimmungen“, „Rechtsbehelfe, Haftung und Sanktionen“, „Durchführungsmaßnahmen“ oder „Schlussbestimmungen“ für anwendbar erklärt werden.

a) Das ergibt sich schon dann, wenn nur die Verpflichtung zu Ausnahmen von bestimmten Kapiteln in Art. 85 Abs. 2 DSGVO in Betracht gezogen wird. Die hier fraglichen Kapitel, im Falle der Richtlinie die Kapitel I, III und VII, sind in Art. 9 DSRiLi, der Art. 85 Abs. 2 DSGVO entspricht, nicht erwähnt. Dennoch werden die auf diesen Kapiteln beruhenden Bestimmungen des BDSG (alt) zu Recht weder in Medienregelungen der Pressegesetze, noch im geltenden § 57 RfTmStV oder im § 41 BDSG für anwendbar erklärt. Genauso wenig müssen diese allgemeinen Normen, die im Falle der Datenschutzgrundverordnung in den Kapiteln I, VIII, X und XI stehen, nunmehr für anwendbar erklärt werden[2].

Im Falle des Kapitels VIII der DSGVO kommt hinzu, dass mit der aufgrund von Art. 85 Abs. 2 DSGVO explizit normierten Ausnahme vom Kapitel VI eine behördliche Aufsicht über die redaktionelle Datenverarbeitung entfällt und damit auch die eine solche behördliche Aufsicht voraussetzenden Bestimmungen des Kapitels VIII schon tatbestandlich leerlaufen und also nicht anwendbar sind.

b) Jedenfalls aber erlaubt Art. 85 Abs. 1 DSGVO Abweichungen auch von Kapiteln der Datenschutzgrundverordnung, die in Art. 85 Abs. 2 DSGVO nicht genannt sind. Art. 85

[2] Ausführlich dazu *Matthias Cornils* (Fn. 1), ferner die Stellungnahme von BDZV, dju, DJV, Presserat und VDZ zum Vorschlag vom 21.6.2017 für eine einheitliche Regelung zum Redaktionsdatenschutz in den Pressegesetzen der Länder unter B I. 1. a), S. 7 f.

Abs. 1 DSGVO erfasst ausdrücklich nicht nur die allgemeine Meinungsäußerung, sondern auch die journalistische Datenverarbeitung. Art. 85 Abs. 1 DSGVO ist sodann im Unterschied zu der tatbestandlich engeren Norm des Art. 85 Abs. 2 DSGVO bei seiner Gestattung mitgliedsstaatlicher Regelung nicht auf bestimmte Kapitel beschränkt. Und er erlaubt zwangsläufig Abweichungen von der DSGVO. Denn alle mitgliedsstaatlichen Rechtsvorschriften, die Meinungsfreiheit und Datenschutz – nach den unterschiedlichen verfassungsrechtlichen und kulturellen Wertsystemen – miteinander in Einklang bringen, ohne die DSGVO zu wiederholen, weichen zwangsläufig von eben dieser DSGVO ab.

Demnach erlaubt es jedenfalls Art. 85 Abs. 1 DSGVO, wie bisher die Anwendbarkeit insbesondere des VIII. Kapitels und damit die Anwendbarkeit des Art. 77 f. (Rechtsbehelf zu einer Datenschutzaufsichtsbehörde) auszuschließen[3]. Die datenschutzbehördliche Aufsicht muss auch unanwendbar bleiben, da die Abwesenheit einer Kontrolle der Redaktionsarbeit durch staatliche Datenschutzaufsichtsbehörden ein ganz wesentliches Element der Pressefreiheit ist.

3. Es ist nach alldem ohne weiteres möglich, mit § 10 HPresseG-Entwurf die Pressefreiheit ungeschmälert zu wahren und nur Datensicherheit und Datengeheimnis sowie eine entsprechende Haftungsregelung anzuwenden. Eine gegenteilige restriktive Interpretation, nach der den Mitgliedsstaaten nun weniger als unter der RiLi 95/46/EG möglich wäre und sie europarechtlich gezwungen wären, Datenschutzaufsichtsbehörde Kontrolle über die redaktionelle Arbeit von Zeitungen und Zeitschriften einzuräumen, ist mit der ratio der Norm, der Systematik und der Entstehungsgeschichte nur schwer vereinbar.

Wer dennoch Art. 85 Abs. 1 und Abs. 2 DSGVO in einem Sinne deuten wollte, der die Möglichkeiten der Mitgliedsstaaten zum Schutz der Presse gegenüber Art. 9 RiLi 95/46/EG verschlechtern und europarechtlich zwingend weitergehende Eingriffe des Datenschutzrechts verlangen würde, würde eine bewusste Entscheidung zur Schwächung der Pressefreiheit hinter einer fernliegenden Interpretation des EU-Rechts verstecken. Auch schon zum geltenden Recht gibt es Stimmen insbesondere aus dem Lager des Datenschutzrechtes, die eine weitergehende Beschneidung und Beseitigung der Pressefreiheit befürworten, zu Recht aber weder vom Gesetzgeber noch von den Gerichten gehört wurden[4].

4. Es sind keinerlei politische Gründe ersichtlich, die redaktionelle Pressefreiheit im Verhältnis zum Datenschutz weiter einzuschränken als in den geltenden Pressegesetzen.

---

[3] Ausführlich dazu *Matthias Cornils* (Fn. 1), ferner Stellungnahme von BDZV, dju, DJV, Presserat und VDZ zum Vorschlag vom 21.6.2017 für eine einheitliche Regelung zum Redaktionsdatenschutz in den Pressegesetzen der Länder unter B I. 1. b), S. 8 – 12.

[4] Vgl. dazu auch noch Stellungnahme von BDZV, dju, DJV, Presserat und VDZ zum Vorschlag vom 21.6.2017 für eine einheitliche Regelung zum Redaktionsdatenschutz in den Pressegesetzen der Länder unter B I. 1. b) ee), S. 11 f.

Insbesondere bedarf es nach wie vor keiner Einführung datenschutzbehördlicher Aufsicht über die Redaktionen.

Das gilt auch für die nach § 10 HPresseG wie nach § 10 HPresseG-Entwurf geltenden Verpflichtungen zu Datensicherheit und Datengeheimnis. Diese Vorgaben untersagen die Verarbeitung journalistischer Daten zu anderen als eben journalistischen Zwecken. Beide Verpflichtungen werden nach dem alten wie nach dem neuen hessischen Pressegesetz mit gerichtlich durchsetzbaren Ansprüchen auf Schadensersatz und Unterlassung sanktioniert (i. V. m. § 7 BDSG (alt) nach altem und in Verbindung mit § 83 BDSG (neu) und Art. 82 DSGVO nach neuem Recht bzw. i. V. m. §§ 823 II, 1004 BGB analog nach altem wie neuem Recht).

Unterlassungs- und Schadensersatzanspruch stellen – wie im inhaltsbezogenen Äußerungs- und Persönlichkeitsrecht – eine scharfe Sanktion dar, über die aber die Gerichte und nicht die Datenschutzaufsichtsbehörden entscheiden. Es handelt sich dabei um das gleiche Sanktionssystem, in dem über die Frage der Verletzung des Persönlichkeitsrechts durch Wahrnehmung der Pressefreiheit im Wege der Veröffentlichung personenbezogener Daten entschieden wird.

Es ist völlig ausgeschlossen, dass dieses sogar für den tatsächlich wie rechtlich sehr viel bedeutsameren **Streit um die rechtlichen Grenzen der Veröffentlichung** personenbezogener Daten hinreichende Instrumentarium und Sanktionssystem nicht in der Lage sein soll, den nach Häufigkeit wie Intensität vergleichsweise sehr viel weniger bedeutsamen, ja wohl bislang sogar wohl eher theoretischen **Streit um Datensicherheit und Datengeheimnis** angemessen zu bewältigen.

Während Pressefreiheit zu einem ganz wesentlichen Teil in der Freiheit der Verarbeitung personenbezogener Daten gegen den Willen und gegen die Interessen des Betroffenen besteht, also bei der Veröffentlichung wirklich ein Interessenkonflikt besteht, gibt es diesen strukturellen Konflikt zwischen Persönlichkeitsrecht und Pressefreiheit bei Datensicherheit und Datengeheimnis gerade nicht. Der Schutz der Redaktionsdaten gegen Zweckentfremdung ist ein ureigenes und überlebenswichtiges Interesse jeder Redaktion und läuft insoweit parallel zu den Interessen Betroffener, deren Daten im Redaktionsarchiv gespeichert sind. Das erklärt auch, wieso Fälle der Verletzung dieser Pflichten, soweit ersichtlich, praktisch keine relevante Rolle spielen.

Im Gegenteil: Die Einführung einer datenschutzbehördlichen Aufsicht über Redaktionen wegen dieser Verpflichtungen würde ganz offenbar problematisch erscheinen und mit den Prinzipien der Pressefreiheit nach wie vor nicht vereinbar sein. Es bedarf demnach nicht nur keiner Aufsicht durch die Datenschutzaufsichtsbehörden, sondern würde den ersten Schritt zu einer Erosion wesentlicher Bedingungen freier Presse in einem immer weiter vereinten Europa bedeuten. Gerade mit Blick auf die unterschiedliche Ausübung des Gestaltungsermessens in den europäischen Mitgliedsstaaten, ist es umso wichtiger, dass

Deutschland den fragilen status quo eines effektiven Schutzes der Pressefreiheit in keiner Weise schmälert.

C Keine Ergänzung der Pressegesetze um Auskunfts- oder Berichtigungsanspruch etc.

Zu Recht sieht § 10 HPresseG-Entwurf keine ergänzenden Auskunfts- oder Berichtigungsansprüche gegenüber Redaktionsdatenbeständen oder Regelungen zur Art und Weise der Aufbewahrung von Gegendarstellungen etc. vor.

Wie soeben vor B unter 4. beschrieben, zählt es zum Schutz der Pressefreiheit, aus dem Datenschutzrecht nur Datensicherheit und Datengeheimnis mit den Sanktionsmöglichkeiten des gerichtlich durchsetzbaren Unterlassungs- und Schadensersatzanspruchs vorzusehen. Es gibt keinerlei Verpflichtung und auch keinerlei Anlass, diesen status quo der Pressefreiheit an irgendeiner Stelle zu verschlechtern.

Das gilt auch für gesonderte pressegesetzliche Ansprüche auf Auskunft oder Berichtigung von Redaktionsdaten sowie für Ansprüche auf bestimmte Formen der Sicherstellung der Beachtung und Berücksichtigung von Gegendarstellungen, Unterlassungsverpflichtungen etc. im weiteren Verlauf der Redaktionsarbeit.

1. Soweit es um spezifische **gesetzliche Ansprüche auf Auskunft über nicht veröffentlichte Redaktionsdaten** (Archive, Manuskripte etc.) zur Person des Betroffenen geht, ist ein solcher Anspruch nach wie vor nicht sinnvoll. Im weiten Umfang des Quellenschutzes, des Schutzes gegen die Ausforschung von Recherchen oder gar von Artikelmanuskripten etc. sind derartige Ansprüche mit der Pressefreiheit nicht vereinbar. Soweit danach noch ein Anwendungsbereich verbleibt, würde ein solcher Anspruch im Falle praktischer Relevanz die Gefahr einer empfindlichen Behinderung der Redaktionen begründen, der kein nachvollziehbarer Mehrwert für die Betroffenen gegenüberstünde. Im Einzelnen:

> Wird eine Information veröffentlicht, bedarf der Betroffene keiner Auskunft mehr. Er kann mit den üblichen Rechtsbehelfen eine Berichtigung durchsetzen, die schon deshalb natürlich in das Redaktionsdatenarchiv übernommen wird, weil jede Wiederholung der Veröffentlichung empfindlich geahndet würde.
>
> Wird eine Information wie bspw. der durch einen Informanten erhobene Vorwurf eines Fehlverhaltens eines Politikers nicht veröffentlicht, etwa weil sich der Vorwurf (noch) nicht in einer für eine Verdachtsberichterstattung ausreichenden Weise erhärten lässt, greift in aller Regel einer der Ausnahmetatbestände eine solchen Anspruchs (keine Ausforschung der Recherche und Redaktionsarbeit oder Informantenschutz), die auch bei einer gesetzlichen Normierung geschaffen werden müssen.
>
> Es bleibt also kein großer Anwendungsbereich. Soweit aber ein Anwendungsbereich verbliebe, stünde der bürokratische Aufwand für die Einzelfallabwägung, die für jedes

Datum gesondert durchgeführt werden müsste, in keinem Verhältnis zu dem Nutzen für den Anspruchsteller. Es müssten zudem alle auf den jeweiligen Betroffenen bezogenen Daten herausgesucht, zusammengestellt und so isoliert werden, dass nicht personenbezogene Daten Dritter offenbart werden. Zunächst müsste auch die Identität des Anspruchsstellers verifiziert werden, denn gerade bei den von der Presse recherchierten Informationen kann es ein großes Interesse Unbefugter geben, sich Zugang zu verschaffen. Allein das ist schon problematisch.

2. Auch **gesonderte gesetzliche Berichtigungsansprüche gegenüber Redaktionsdaten** sind nach wie vor nicht angezeigt, sondern bei sorgfältiger Abwägung eher unangemessen.

Soweit es um etwaige Ansprüche auf Berichtigungen personenbezogener Angaben in **veröffentlichten Presseartikeln** geht, ist das Äußerungs-, Persönlichkeits- und Presserecht mit Unterlassungs-, Gegendarstellungs-, Widerrufs- und Berichtigungsansprüchen das richtige Rechtsregime, um die widerstreitenden Interessen Betroffener und der Pressefreiheit gegeneinander abzuwägen. Es bedarf keiner gesonderten datenschutzrechtlich begründeten Ansprüche in den Pressegesetzen.

Soweit es um Berichtigungsansprüche gegenüber nicht veröffentlichten personenbezogenen Redaktionsdaten geht, setzt ein gesonderter Berichtigungsanspruch einen gesonderten Auskunftsanspruch voraus, der nach wie vor nicht sinnvoll ist (siehe soeben unter 1.).

Hinzu kommt, dass auch der Berichtigungsanspruch bei genauer Betrachtung nicht sinnvoll erscheint. Ist bspw. eine Behauptung eines Informanten (noch) nicht weiter zu erhärten und wäre ihre Veröffentlichung damit (noch) nicht rechtmäßig, bleibt doch die Information im Redaktionsarchiv nicht nur für die weitere Redaktionsarbeit notwendig, sondern auch rechtmäßig. Aber selbst wenn die Information nach dem jeweiligen Stand der Recherche falsch sein sollte, ist für die Bewertung des Informanten ebenso wie für die weitere Recherche die Tatsache der falschen Aussage des betreffenden Informanten ebenso wie der (falsche) Inhalt dieser Aussage wichtig und darf nicht berichtigt werden, soll das Archiv seinen Zweck erfüllen können.

3. Auch für einen gesonderten gesetzlichen Anspruch auf Aufnahme von Gegendarstellungen, Verpflichtungserklärungen etc. in die Redaktionsdaten gibt es keine Notwendigkeit. Es zählt selbstverständlich zur journalistischen Sorgfaltspflicht, Unterlassungserklärungen, Gegendarstellungen, Unterlassungsurteile etc. bei weiterer Redaktionsarbeit zu den jeweiligen Tatsachen zu berücksichtigen.

Prof. Dr. Christoph Fiedler
VDZ
Markgrafenstraße 15

10969 Berlin
Tel.: 030 72 62 98 120
c.fiedler@vdz.de

dbb beamtenbund und tarifunion
Landesbund Hessen

dbb Hessen · Eschersheimer Landstr. 162 · 60322 Frankfurt a. M.

Hessischer Landtag
-Innenausschuss-
Herrn Vorsitzenden
Horst Klee, MdL
Schlossplatz 1-3
65183 Wiesbaden per Mail

Frankfurt a. M., 7.3.2018

Stellungnahme zum Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/ DIE GRÜNEN für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit
-Drucksache 19/5728-

Sehr geehrter Herr Vorsitzender Klee,
sehr geehrte Damen und Herren,

der dbb Hessen bedankt sich für die Gelegenheit, zum vorliegenden Gesetzentwurf Stellung nehmen zu können.

Vorbemerkungen

Im Interesse einer Rechtsklarheit durch die Umsetzung der EU-Datenschutzgrundverordnung (EU-DSGVO) in nationales bzw. hessisches Recht begrüßen wir, dass mit dem vorliegenden Entwurf die erforderlichen Gesetzesanpassungen vorgenommen werden sollen, die sich durch die EU-DSGVO ergeben.
Wenn die vorgesehenen Regelungen noch rechtzeitig in Kraft treten, werden wir also auch in Hessen die notwendige Rechtsklarheit haben.

Bedeutung des Datenschutzes wächst mit zunehmender Digitalisierung

Die Digitalisierung in der öffentlichen Verwaltung schreitet zunehmend voran, immer mehr Verwaltungsabläufe werden elektronisch abgewickelt, wobei wachsende Mengen an Daten von Bürgerinnen und Bürgern, Unternehmen und Beschäftigten erhoben und verarbeitet werden.

Der Schutz dieser Daten war und ist dabei eine zentrale Verantwortung der öffentlichen Stellen, die sie verwenden. Um diesen Schutz zu gewährleisten, ist einerseits ein wirksames und umfassendes Datenschutzrecht notwendig. Für den dbb hessen als gewerkschaftliche Interessenvertretung der Beschäftigten im öffentlichen Dienst steht dabei der Beschäftigtendatenschutz im Mittelpunkt, sodass der Fokus dieser Stellungnahme hierauf liegt.

Datenschutz braucht Recht und Ressourcen für die praktische Umsetzung

Datenschutz darf sich nicht lediglich auf die Schaffung gesetzlicher Regelungen beschränken, sondern die rechtlichen Vorgaben müssen in der Praxis auch umgesetzt werden können. Neben der rechtlichen Grundlage erfordert die Umsetzung des umfangreichen neuen Datenschutzrechts auf allen Ebenen der öffentlichen Verwaltung also auch zusätzliches und besonders qualifiziertes Personal. Die rechtlichen Bestimmungen bleiben wirkungslos, wenn sie durch die Verantwortlichen nicht umgesetzt werden können.

Daher sind vermehrt Planstellen, Qualifizierungsangebote sowie eine Sensibilisierung aller Beschäftigten des öffentlichen Dienstes notwendig. Die Aufgaben können nicht allein durch die behördlichen Datenschutzbeauftragten abgedeckt werden. Ohnehin ist die Wahrnehmung der Aufgaben des Datenschutzbeauftragten im Nebenamt in Behörden ab einer gewissen Größe nicht mehr zu vertreten.

Auch um die technischen Voraussetzungen für den Datenschutz zu schaffen und zu pflegen, entstehen erhöhte personelle Bedarfe, insbesondere im IT-Bereich. Um dabei im Wettbewerb mit der Privatwirtschaft bestehen zu können, ist es dringend erforderlich, die Einkommens- und Beschäftigungsbedingungen in diesem Bereich attraktiver zu gestalten.

Für die Anwendung des mit dem vorliegenden Entwurf geplanten, neuen hessischen Datenschutzrechts bedarf es also neben den konkreten Regelungen, um die Daten der Bürgerinnen und Bürger, Unternehmen und Beschäftigten zu schützen, auch der Bereitstellung der erforderlichen personellen und finanziellen Mittel für die praktische Umsetzung.

Zum Beschäftigtendatenschutz nach § 23 HDSIG-E

Datenschutz gilt auch für die Beschäftigten im öffentlichen Dienst

Mit dem Anstieg der Zahl der digitalen Verwaltungsverfahren auch im Zuge des Projekts „Digitale Modellbehörde“ und der flächendeckenden Einführung der elektronischen Akte in der Landesverwaltung wächst auch die Bedeutung des Datenschutzes in den einzelnen Behörden weiter. Dabei steht der Schutz der Daten von Bürgerinnen, Bürgern und Unternehmen meist im Fokus. Der Schutz der Daten der Beschäftigten, die bei der Personaladministration und der elektronischen Aufgabenerledigung entstehen, wird jedoch häufig vernachlässigt.

Personaladministration muss Datenschutz berücksichtigen

Der Datenschutz bei der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses ist dabei die eine Seite. Hierbei geht es um die Datenverarbeitung, die notwendig ist, um Beschäftigungsverhältnisse zu begründen, abzuwickeln und das Personal zu administrieren. Die diesbezüglich vorgesehenen Regelungen in § 23 HDSIG-E wurden im Vergleich zu § 34 HDSG teilweise konkretisiert, was wir sehr begrüßen.

Es fehlt aber eine konkrete rechtliche Grundlage für die elektronische Personalakte. Diese ist dringend erforderlich, da bereits verschiedene Projekte zur E-Personalakte durchgeführt werden und in naher Zukunft datenschutzkonform umgesetzt werden müssen.

Beschäftigtendatenschutz auch bei Fachanwendungen
Weiter fehlen auch Regelungen zur Verarbeitung von Beschäftigtendaten, die bei der digitalen Abwicklung von Fachaufgaben entstehen. Dies können z. B. Daten über An- und Abwesenheit, die Arbeitsleistung oder das Arbeitsverhalten der Beschäftigten sein. Auch dies sind schützenswerte personenbezogene Daten, die missbräuchlich zur Leistungs- und Verhaltenskontrolle herangezogen werden können.
Hier sollte deshalb dringend eine entsprechende ergänzende Regelung vorgesehen werden. Diese Problematik stellt sich auch in den vermehrt aufgesetzten Digitalisierungsprojekten in der Landesverwaltung sowie insgesamt bei der elektronischen Aktenführung.

So viele Daten wie nötig, so wenige wie möglich
Dabei geht es nicht darum, die Digitalisierung von Verwaltungsprozessen zu behindern, sondern diese datenschutzkonform umzusetzen und dabei die Persönlichkeitsrechte der Beschäftigten zu wahren. Bei der Beurteilung, welche persönlichen Daten der Beschäftigten in Fachanwendungen erfasst werden und welche Auswertungsmöglichkeiten bestehen sollen, muss eine Beschränkung auf das absolut notwendige Mindestmaß erfolgen.
Der allgemein zu beobachtenden Neigung, die technischen Möglichkeiten nach oben auszuschöpfen, muss dabei konsequent entgegengetreten werden.

Datenschutz muss technisch umgesetzt werden
Aber auch mit den technischen Systemen, die nach dem HDSG und HDSIG-E rechtmäßig zur Verarbeitung von Beschäftigtendaten genutzt werden, bestehen in der Praxis datenschutzrechtliche Probleme. So ist beispielsweise das Problem des Löschens von Daten in SAP/HR, dem zentralen Personalverwaltungsprogramm der hessischen Landesverwaltung, auf das der Hauptpersonalrat beim Hessischen Ministerium des Innern und für Sport und der Hessische Datenschutzbeauftragte seit Jahren hinweisen, immer noch nicht gelöst.
Sowohl beamtenrechtliche als auch datenschutzrechtliche Löschpflichten können derzeit technisch nicht umgesetzt werden. Hier darf sich der Datenschutz nicht an den technischen Gegebenheiten orientieren, sondern die Technik muss unverzüglich an das Datenschutzrecht angepasst werden.

Personalvertretungen müssen Einhaltung des Datenschutzes überwachen können
Die Anforderungen an den Beschäftigtendatenschutz dürfen also keinesfalls niedriger sein als beim übrigen Datenschutz und die Umsetzung in der Praxis muss gewährleistet werden. Bei der Überwachung, ob in den einzelnen Dienststellen auch datenschutzkonform mit den Beschäftigtendaten umgegangen wird, haben die Personalvertretungen neben den behördlichen Datenschutzbeauftragten eine zentrale Rolle.
Um diese Aufgabe wahrnehmen zu können, sollte das neue hessische Datenschutzrecht auch klare Rechte der Personalvertretungen festlegen. Dementgegen wurde beispielsweise die Regelung aus § 34 Abs. 5 HDSG, die die Dienststelle dazu verpflichtet, der Personalvertretung das Verfahrensverzeichnis im personalvertretungsrechtlichen Beteiligungsverfahren vorzulegen und die Möglichkeit, hierzu eine Stellungnahme des Hessischen Datenschutzbeauftragten anzufordern, nicht übernommen. Diese sollte dringend ergänzt werden, um die bisherigen Rechte der Personalvertretungen nicht zu beschneiden.
Auch bei der Sanktion von Verstößen gegen den Beschäftigungsdatenschutz ist der vorliegende Gesetzentwurf nicht ausreichend. Der oder die einzelne Beschäftigte hat zwar das Recht, auf Schadensersatz zu klagen, ein kollektives Recht für die Personalvertretung, um gegen Datenschutzverstöße vorzugehen, gibt es allerdings nicht ausdrücklich.

Hier sollte eine eindeutige und effektive Regelung getroffen werden, um den Datenschutz der Beschäftigten auch kollektiv durchsetzen zu können.
Häufig werden der Beschäftigtendatenschutz und die Personalvertretungen, die auf dessen Einhaltung hinwirken, als „lästige Übel“ und „Behinderer“ von Digitalisierungsprozessen empfunden. Einer solchen Haltung ist jedoch entschieden entgegenzutreten, denn es geht um den notwendigen Schutz verfassungsmäßiger Persönlichkeitsrechte. Daher sollten Führungskräfte mit Personalräten und Beschäftigten an einem Strang ziehen.

Zu den weiteren Regelungen des Gesetzentwurfs

Fundierte Datenschutz-Folgenabschätzung für alle Verfahren
Bisher war in § 7 Abs. 6 HDSG geregelt, dass vor jeder automatisierten Datenverarbeitung eine Vorabkontrolle stattfinden muss, in der geprüft wird, ob damit Gefahren für die Rechte und Interessen der betroffenen Personen, deren Daten verarbeitet werden, verbunden sind. Dies wird in § 62 Abs. S. 1 HDSIG-E abgeschwächt zu *„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen“*. Die Datenschutz-Folgenabschätzung dient aber doch gerade dazu, fundiert einzuschätzen, ob hier Gefahren bestehen. Um tatsächlich wirksam vorzubeugen, dass durch Verarbeitungsvorgänge Rechte verletzt werden, muss die Verpflichtung zu einer Datenschutz-Folgenabschätzung bei jedem Verfahren gegeben sein. Die bisherige Regelung aus dem HDSG sollte also beibehalten werden.

Anspruch auf Informationszugang muss administriert werden können
Durch den Anspruch auf Auskunft nach § 80 HDSIG-E kann zukünftig jede Bürgerin und jeder Bürger den Zugang zu Informationen öffentlicher Stellen beantragen. Dieses Antragsverfahren muss deshalb zukünftig von jeder öffentlichen Stelle zusätzlich zu den Fachaufgaben abgewickelt werden, was zu einem Personalmehraufwand führen wird.
Dieser Mehraufwand muss durch zusätzliche Personalressourcen ausgeglichen werden.

Datenübermittlung an nicht öffentliche Stellen als besonders sensibler Bereich
Insbesondere die in § 22 HDSIG-E vorgesehene Datenübermittlung an nicht öffentliche Stellen scheint uns –neben dem Beschäftigtendatenschutz- ein hochsensibler Bereich zu sein.
Gerade hier verfügt man über vergleichsweise wenig Erfahrungswerte, muss aber angesichts der Gesamtsituation alle zur Verfügung stehenden Kontrollmechanismen vorsehen.
Es ist hinlänglich bekannt, wie „wertvoll“ personenbezogene Daten für die Privatwirtschaft ganz allgemein, aber auch für unseriöse Unternehmen und Menschen mittlerweile geworden sind.
Vor diesem Hintergrund scheint uns die Gefahr, dass übermittelte Daten an nicht öffentliche Stellen danach „außer Kontrolle“ geraten könnten, besonders hoch.
Auf diesen Umstand möchten wir besonders nachdrücklich hinweisen.

Die vorstehenden Ausführungen wurden weitestgehend von der DVG Hessen für den dbb Hessen erarbeitet.

Nachfolgend möchten wir zu einigen, eher ressortspezifischen Regelungen gesondert Stellung nehmen.

Zu § 25 HDSIG-E – Datenüberarbeitung zu im öffentlichen Interesse stehenden Archivzwecken

Das Archivgesetz zählt zu den bereichsspezifischen Datenschutzgesetzen. Fragen, die den Datenschutz für das öffentliche Archivgut betreffen, wurden bisher im Hessischen Archivgesetz und nicht im HDSG behandelt. Mit § 25 des hier vorliegenden Entwurfs werden nun die Auskunfts- und weitere Rechte der Betroffenen und damit ein wesentlicher Teil der bisher im Archivgesetz geregelten Bestimmungen in das neue HDSIG-E übernommen.

Dies hat zur Folge, dass zur Klärung datenschutzrechtlicher Fragen in Bezug auf das öffentliche Archivgut neben der ebenfalls neuen EU-Datenschutzgrundverordnung und dem bisherigen Archivgesetz auch noch das HDISG-E herangezogen werden muss. Diese Zersplitterung dürfte für Betroffene, Nutzer von Archivgut sowie für Archivbeschäftigte ein erhebliches Erschwernis darstellen.

Wir regen daher an, die Bestimmungen des § 25 HDSIG-E eher in einem ergänzten Archivgesetz zu regeln. Diese Vorgehensweise wurde auch von anderen Bundesländern wie z. B. Thüringen favorisiert.

In diesem Zuge wären dann auch die bisherigen Regelungen in § 15 des jüngst verlängerten Hessischen Archivgesetzes (HArchivG) anzupassen.

Vorstehende Ausführungen gelten analog auch für andere bereichsspezifische Datenschutzgesetze.

Zu Art 18 - Änderung des Hess. Gesetzes über die öffentliche Sicherheit und Ordnung

Der Wegfall der Möglichkeit, Daten zur Gefahrenabwehr zu erheben, wenn *tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies im Interesse der Person liegt und sie in Kenntnis des Zwecks einwilligen würde,* bedeutet in der polizeilichen Praxis eine deutliche Einschränkung, und zwar eindeutig zum Nachteil der betroffenen Bürgerinnen und Bürger.

Dies muss vor dem Hintergrund der Tatsache, dass es sich ausdrücklich um Gefahrenabwehr *im Interesse der betroffenen Person handelt,* sehr kritisch gesehen werden.

Hier ist auch eine Kollision mit der Zielrichtung der in § 21 Abs. 1 Nr. 1 HDSIG-E getroffenen Regelung erkennbar, die die Weiterverarbeitung zulässt, wenn sie *im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde.*

In beiden Fallkonstellationen wurde/wird eine Prognose aus dem Blickwinkel und im Interesse des betroffenen Bürgers erwartet.

Und die Weiterverarbeitung von Daten soll unter diesen Umständen zulässig sein, die Erhebung zum Zwecke der Gefahrenabwehr hingegen nicht.

Das ist schwer nachvollziehbar und bedarf der Überarbeitung.

Zu Art. 29 – Änderung des Hessischen Vermessungs- und Geoinformationsgesetzes

Die vorgesehene Änderung stößt auf Bedenken, denn nach unserem Kenntnisstand werden im Grundbuch in Hessen seit geraumer Zeit keine Eigentümeradressen mehr geführt bzw. aktualisiert. Im Liegenschaftskataster hingegen werden Adressen geführt und anlassbezogen auch aktualisiert (bspw. zur Versendung von Ladungen zu Vermessungsterminen).

Der Hinweis, wonach die Einschränkung der Betroffenenrechte dann nicht gelten soll, wenn die betroffene Person geltend gemacht hat, dass die im Liegenschaftskataster nachrichtlich geführten Eigentumsangaben nicht mit der Originalquelle im Grundbuch übereinstimmen, könnte daher fehlgehen.

Im Übrigen bliebe auch die Frage offen, ob Bürger die Löschung der Daten im Liegenschaftskataster oder deren Rückführung auf die Daten des Grundbuchs verlangen können.

Für weitere Ausführungen stehen wir gerne im Rahmen der öffentlichen Anhörung am 15. März zur Verfügung.

Mit freundlichen Grüßen

Heini Schmitt
Landesvorsitzender

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Stellungnahme

zum

Hessischen Datenschutz- und Informationsfreiheitsgesetz

(Art. 1 des Gesetzentwurfs der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit, Stand: 05.12.2017)

I. Vorbemerkung

Mit dem Hessischen Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit soll zunächst das Hessische Datenschutzgesetz neu gefasst werden, um es an die Vorschriften der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DS-GVO) anzupassen. Zudem sollen im Rahmen dieser Neufassung des Hessischen Datenschutzgesetzes zugleich Regelungen zur Umsetzung der Richtlinie (EU) Nr. 2016/680 (Richtlinie zu Polizei und Justiz, RLPJ) aufgenommen werden. Außerdem sollen die Bürgerinnen und Bürger einen gesetzlichen Anspruch auf Zugang zu den bei öffentlichen Stellen des Landes vorhandenen amtlichen Informationen erhalten, der aufgrund des engen Zusammenhangs zwischen dem Informationszugangsrecht auf der einen Seite und dem Datenschutz auf der anderen Seite auch im Hessischen Datenschutzgesetz – das daher zukünftig Hessisches Datenschutz- und Informationsfreiheitgesetz (HDSIG) heißen soll – geregelt werden soll. Ferner sollen mit dem vorgenannten Gesetzentwurf auch einige datenschutzrechtliche Regelungen in den Hessischen Fachgesetzen an die Datenschutz-Grundverordnung angepasst werden bzw. zur Umsetzung der Richtlinie zu Polizei und Justiz geändert werden.

Dieses anspruchsvolle Gesetzesvorhaben führt dem Grunde nach zu einer Neufassung des Hessischen Datenschutzgesetzes, aber zusätzlich auch zu erheblichen Änderungen in den übrigen Hessischen Landesgesetzen.

Der erhebliche Umfang und die Komplexität des gesetzgeberischen Vorhabens erfordert die Beachtung einer Vielzahl von Gegebenheiten. Zunächst steht das Verhältnis des Landesdatenschutzrechtes zur Datenschutz-Grundverordnung im Vordergrund. Diese genießt Vorrang vor innerstaatlichem Recht, soweit sie reicht. Dementsprechend ist zu klären, ob und inwieweit der Landesgesetzgeber über Spielräume zur Regelung verfügt. Bei der Ausfüllung dieser Spielräume sind die Vorgaben der einschlägigen Öffnungsklauseln der Datenschutz-Grundverordnung zu beachten.

Hinzu treten die Fragen der Harmonisierung mit der Richtlinie zu Polizei und Justiz. Die beiden Rechtsakte unterscheiden sich nach ihren Anwendungsbereichen, verfügen aber über eine Reihe

von parallelen Regelungen. Der innerstaatliche Gesetzgeber kann demnach in Umsetzung der Richtlinie zu Polizei und Justiz Regelungen treffen, die allerdings die parallelen Regelungen der Datenschutz-Grundverordnung mit zu bedenken haben.

Aufgrund der erheblichen Komplexität des Gesetzgebungsvorhabens bedarf der Entwurf einer sorgfältigen und gründlichen Prüfung sowie Erörterung. Seitens des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) erfolgt allerdings keine umfassende Prüfung bzw. Erörterung des gesamten Gesetzentwurfs, vielmehr werden Schwerpunkte gesetzt und herausgehobene Problembereiche und Fragestellungen erörtert. Dabei liegt der Fokus primär auf dem informationsfreiheitsrechtlichen Teil des zukünftigen HDSIG (siehe III.). Dennoch werden zunächst im Folgenden Ausführungen zum datenschutzrechtlichen Teil – insbesondere zur Anpassung des Hessischen Datenschutzgesetzes an die Datenschutz-Grundverordnung – erfolgen (siehe II.). Im Rahmen dieser Stellungnahme unbeachtet bleiben die Änderungen in den übrigen Hessischen Landesgesetzen (Art. 2 bis 31 des Gesetzentwurfs).

II. Datenschutzrechtliche Bestimmungen des HDSIG (Erster bis dritter Teil des HDSIG)

1. Zu der Struktur des Gesetzentwurfs

Die Strukturierung des zukünftigen HDSIG in fünf Teile – mit dem Voranstellen eines ersten Teiles, der gemeinsame Bestimmungen für die folgenden Teile enthält – ist vor dem Hintergrund der Verständlichkeit des Gesetzes nachvollziehbar. Gerade die Schaffung eines ersten Teiles, der sowohl in Anpassung an die Datenschutz-Grundverordnung als auch in Umsetzung der Richtlinie zu Polizei und Justiz erfolgt, führt allerdings zu umfangreichen Wiederholungen (teils wortgleichen) des Textes der Datenschutz-Grundverordnung. Z.B. wiederholen die §§ 5 bis 7 HDSIG im Wesentlichen die Artikel 37 bis 39 der Datenschutz-Grundverordnung.

Wiederholungen des Verordnungstextes werden zwar teilweise unter Berufung auf Erwägungsgrund 8 der Datenschutz-Grundverordnung für zulässig erachtet. Allerdings lässt dieser Erwägungsgrund eine Aufnahme von Teilen der Verordnung durch die Mitgliedstaaten in nationales Recht nur zu, wenn „in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind“ und „soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.“

Das grundsätzlich bestehende Wiederholungsverbot bei europarechtlichen Verordnungen wird folglich nicht völlig außer Kraft gesetzt. Die Datenschutz-Grundverordnung erlaubt Wiederholungen nur in Einzelfällen, sofern ohnehin eine Öffnungsklausel für die Mitgliedstaaten in der Datenschutz-Grundverordnung zur Vornahme von Präzisierungen oder Einschränkungen vorgesehen ist.

Dies bedeutet nach Auffassung des LfDI, dass Wiederholungen grundsätzlich unzulässig sind. Dies betrifft nicht lediglich wortlautgleiche Wiederholungen, sondern auch alternative Formulierungen, die letztlich den Vorschriften der Datenschutz-Grundverordnung entsprechen. Daraus folgt, dass im Grundsatz alle nationalen datenschutzrechtlichen Regelungen, die vom Anwendungsbereich der Datenschutz-Grundverordnung erfasst sind – unabhängig davon, ob diese den Regelungen der Datenschutz-Grundverordnung entsprechen oder widersprechen – zu streichen sind, so-

weit keine Öffnungsklausel vorhanden ist. Ansonsten werden die grundsätzlich unmittelbare Geltung und der Anspruch auf Gesamtverbindlichkeit der Datenschutz-Grundverordnung kompromittiert.

Darüber hinaus ist fraglich, ob die Struktur des Gesetzes tatsächlich zu mehr Rechtsklarheit bei den betroffenen Personen führt, wie es Ziel des Erwägungsgrundes 8 ist. Das Zurechtfinden in fünf unterschiedlichen Teilen, von denen vereinzelte dann auch noch nachrangig bzw. ergänzend zur Datenschutz-Grundverordnung gelten, erfordert ein hohes Maß an Orientierungsleistung und Verständnis für das Verhältnis der Gesetze zueinander.

2. Zu den Regelungen zum Hessischen Datenschutzbeauftragten (§§ 8 bis 18 HDSIG)

Die Gewährleistung der vollständigen Unabhängigkeit des Hessischen Datenschutzbeauftragten – insbesondere durch die Regelung des § 8 Abs. 2 HDSIG – ist zu begrüßen. Gleiches gilt für die Regelung zur Personal- und Sachausstattung in § 18 HDSIG.

Ob die Regelungen des § 11 Abs. 2 S. 4 bis 6 HDSIG dagegen mit der Datenschutz-Grundverordnung vereinbar sind, erscheint zumindest zweifelhaft. Die Datenschutz-Grundverordnung regelt in Art. 53 Abs. 4, dass ein Mitglied seines Amtes nur enthoben wird, wenn es eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt. Die Regelung der Datenschutz-Grundverordnung ist insoweit zwingend und grundsätzlich abschließend. Lediglich hinsichtlich des Verfahrens und der Konkretisierung der unbestimmten Rechtsbegriffe bestehen noch Regelungsspielräume für die Mitgliedstaaten.

§ 11 Abs. 2 S. 4 HDSIG nennt Gründe, die eine Absprache des Amtes bzw. der Rechte aus dem Amt durch Urteil des Staatsgerichtshof rechtfertigen können. Diese Gründe sind aber nicht allesamt solche, die die in Art. 53 Abs. 4 DS-GVO genannten Begriffe konkretisieren, vielmehr sollen dadurch wohl weitere Gründe für eine Amtsenthebung auf landesrechtlicher Ebene eingeführt werden, was nicht zulässig sein dürfte und die Unabhängigkeit des Hessischen Datenschutzbeauftragten beeinträchtigen könnte.

Die ausführliche Regelung der Aufgaben (§ 13 HDSIG) und Befugnisse (§ 14 HDSIG) des Hessischen Datenschutzbeauftragten, die vorwiegend der Umsetzung der Richtlinie zu Polizei und Justiz dient, ist dem Grunde nach in diesem Zusammenhang zu begrüßen. Auf die in Bezug zu diesen Vorschriften bestehende Problematik der Normenwiederholung wird verwiesen.

In § 14 HDSIG Abs. 2 HDSIG wird für den Anwendungsbereich der Richtlinie zu Polizei und Justiz das Instrument der Beanstandung aufrechterhalten. Diese Regelung ist im Rahmen des Umsetzungsspielraums, den die Richtlinie zu Polizei und Justiz dem Landesgesetzgeber eröffnet, möglich. Richtigerweise werden zusätzlich in § 14 Abs. 3 HDSIG wirksame Abhilfebefugnisse des Hessischen Datenschutzbeauftragten geregelt, wie sie Art. 47 Abs. 2 der RLPJ vorsieht. Diese Befugnisse müssen so ausgestaltet werden, dass dem Hessischen Datenschutzbeauftragten eine effektive Abhilfe von Datenschutzverletzungen möglich ist. Die Abhilfebefugnisse entfalten ihre Effektivität nur dann, wenn sie ohne eine mögliche Rangfolge oder Nachschaltung neben dem Instrument der Beanstandung unmittelbar ausgeübt werden können. Sollte die Formulierung in § 14 Abs. 3 S.

1 HDSIG „darüber hinaus“ eine Rangfolge der Ergreifung der Befugnisse nach der Ausübung der Beanstandung implizieren, wäre dies nicht richtlinienkonform. Nach richtlinienkonformer Auslegung besteht vielmehr ein gleichrangiges Verhältnis zwischen den Befugnissen des Hessischen Datenschutzbeauftragten nach § 14 Abs. 2 und Abs. 3 HDSIG.

3. Zu § 20 HDSIG (Verarbeitung besonderer Kategorien personenbezogener Daten)

Die Regelung des § 20 HDSIG ist inhaltlich unzureichend. Der Hessische Landesgesetzgeber macht nicht von der in Art. 9 Abs. 4 DS-GVO enthaltenen Möglichkeit Gebrauch, genetische, biometrische und Gesundheitsdaten vor den vielfältigen Risiken einer unspezifischen Verarbeitung durch die von dem Gesetz erfassten Stellen nachhaltig und umfänglich zu schützen. Dies ist aber angesichts des erhöhten Schutzbedarfs dieser Informationen geboten. Der Gesetzentwurf wird damit nicht dem verfassungsrechtlichen Auftrag gerecht, das informationelle Selbstbestimmungsrecht gerade bei der Verarbeitung besonders schutzbedürftiger personenbezogener Daten durch geeignete Gewährleistungen sicherzustellen, insbesondere bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DS-GVO.

Darüber hinaus berücksichtigt § 20 HDSIG nicht das im Verhältnis zwischen Bürger und Verwaltung bestehende Ungleichgewicht und die daraus resultierenden generellen Zweifel an der datenschutzrechtlichen Tragfähigkeit einer im Einzelfall vom Bürger gegenüber der Verwaltung abgegebenen Einwilligung in die Verarbeitung derart schutzbedürftiger Daten (vgl. Erwägungsgrund 43). Dementsprechend sollte die grundsätzlich nach Art. 9 Abs. 2 lit. a DS-GVO bestehende Möglichkeit, auch besondere Kategorien personenbezogener Daten auf der Basis einer Einwilligung zu verarbeiten, gesetzgeberisch eingeschränkt und nur dann zugelassen werden, wenn diese bereichsspezifisch ausdrücklich erlaubt sind. Art. 9 Abs. 2 lit. a DS-GVO lässt dem Landesgesetzgeber den dazu erforderlichen Regelungsspielraum. Zudem sollte eine Regelung dahingehend erfolgen, dass die zulässige Einwilligung in die Verarbeitung genetischer, biometrischer oder Gesundheitsdaten der Schriftform bedarf und dass die Übermittlung derartiger Daten auf der Grundlage einer Einwilligung nur wirksam ist, wenn die empfangende Stelle Kenntnis von Inhalt und Reichweite der Erklärung hat.

Zudem wird in dem Regelungsentwurf der besondere Schutzbedarf genetischer, biometrischer oder Gesundheitsdaten bei der Verarbeitung sowohl durch den Verantwortlichen selbst als auch durch einen von diesem hinzugezogenen Auftragsverarbeiter nicht angemessen berücksichtigt. Angesichts der zunehmend zu beobachtenden Praxis, im Bereich der Verarbeitung derart schutzbedürftiger Daten externe Dienstleister einzubinden, entspricht der Entwurf insoweit nicht den datenschutzrechtlichen Anforderungen an einen effektiven Grundrechtsschutz.

III. Informationsfreiheitsrechtliche Bestimmungen des HDSIG-E (Vierter Teil des HDSIG-E)

1. Allgemeine Einschätzung

Das Fundament einer demokratischen Gesellschaft sind mündige und gut informierte Bürgerinnen und Bürger. Hier haben Staat und Politik eine Bringschuld: Sie müssen sich erklären, ihre Vorhaben und Entscheidungsgrundlagen nachvollziehbar machen, veröffentlichen, Barrieren abbauen und sich öffnen. Sie müssen transparenter werden, auch und gerade mit Hilfe der neuen Medien, wobei es bei dieser Öffnung auch Grenzen gibt. Diese ergeben sich etwa aus dem Schutz personenbezogener Daten, von Betriebs- oder Geschäftsgeheimnissen oder auch staatlichen (Sicherheits-)Interessen. Zunächst aber ist es wichtig, ein Recht der Bürgerinnen und Bürger auf umfassende Information zu normieren. Dieses Ziel verfolgt der vorgelegte Entwurf im Vierten Teil des HDSIG-E.
Die Intention des Gesetzes ist es, das Recht auf Zugang zu amtlichen Informationen umfassend, das heißt ohne Darlegung eines Interesses und außerhalb eines laufenden Verwaltungsverfahrens, zu gewähren und dabei gleichzeitig die berechtigten öffentlichen Interessen und die Interessen privater Dritter zu schützen. Damit beabsichtigt das Gesetz eine Vergrößerung der Transparenz und die Verbesserung der Kontrolle der Verwaltung. Dies ist begrüßenswert.
Die Erfahrungen der Informationsfreiheitsbeauftragten des Bundes und der Länder haben gezeigt, dass sich die Befürchtungen, die vor und im Rahmen der Einführung von Informationsfreiheitsgesetzen häufig artikuliert werden – wie etwa ein „Lahmlegen“ der Verwaltung durch eine nicht zu bewältigende Flut von Anfragen oder die Begünstigung querulatorischer Tendenzen – nicht bewahrheiten. Vielmehr treten in der Realität der Informationsfreiheit – das zeigt insbesondere die rheinland-pfälzische Erfahrung aus der Anwendungspraxis des Landestransparenzgesetzes (LTranspG) – die positiven Aspekte hervor. Hervorzuheben ist insbesondere eine deutlich höhere Akzeptanz politischer Entscheidungen, die durch ein höheres Maß an Information, die frühzeitige Einbindung zivilgesellschaftlicher Akteure und interessierter Bürgerinnen und Bürger und durch die so erreichte Nachvollziehbarkeit von Verwaltungshandeln erzielt wird.
Die beiden deutschen Transparenzgesetze – das Hamburgische Transparenzgesetz und das Landestransparenzgesetz Rheinland-Pfalz –, die neben dem Informationszugang auf Anfrage für einen gesetzlich normierten Katalog an Informationen eine proaktive Veröffentlichungspflicht statuieren, bewähren sich in der Praxis. Den beiden Gesetzen ist gemein, dass sie die Digitalisierung auch für das Informationsverhältnis zwischen Staat und Bürger realisieren, indem das Internet für einen digitalen Dialog zwischen Staat und Gesellschaft genutzt wird. Aber nicht nur die neueren Informationsfreiheitsregelungen in Deutschland sondern auch neue oder novellierte Informationsfreiheitsgesetze in Europa (z.B. in Albanien und Kroatien) sehen proaktive Veröffentlichungspflichten vor. Diesen Standard erreicht der vorgelegte Entwurf nicht.
Der Entwurf des Hessischen Gesetzgebers ist in seiner Grundintention sehr zu begrüßen. Viele der gewählten Regelungen zeichnen sich durch ein großes Maß an Bürgerfreundlichkeit aus. Manche Einzelregelungen sind jedoch bedenklich oder von zu begrenzter Tragweite.
Als besonders problematisch erachtet wird, dass der Hessische Landesgesetzgeber im Vierten Teil des HDSIG-E keinen voraussetzungslosen Anspruch auf Zugang zu Informationen bei den öffentlichen Stellen der Gemeinden und Gemeindeverbänden normiert. Dass zudem keine landesweit einheitliche Kostenregelung für den Informationszugang getroffen wird, sondern die jeweilige Kommune nicht nur per Satzung bestimmt, ob die Vorschriften des Vierten Teils des HDSIG-E anwendbar sein sollen, sondern darüber hinaus, ob und wenn ja in welcher Höhe Kosten für den

Informationszugang erhoben werden, erscheint nachbesserungsbedürftig. Das Ziel, einen landesweit einheitlichen Standard zu gewährleisten wird auf diese Weise nicht erreicht. Dies widerspricht dem demokratischen und auch dem gesellschaftspolitischen Charakter eines Informationsfreiheitsgesetzes.
Zu den einzelnen Bestimmungen wird im Folgenden Stellung genommen.

2. Zu § 2 Abs. 2 und 3 (öffentliche Stellen)

Die in § 2 Abs. 2 vorgenommene Modifikation des Begriffs der „öffentlichen Stellen“ bedeutet hinsichtlich des Zugangs zu amtlichen Informationen eine Bereichsausnahme für alle privatrechtlich organisierten kommunalen und staatlichen Unternehmen – etwa solche der Daseinsvorsorge –, soweit diese am Wettbewerb teilnehmen. Die Gesetzesbegründung zu § 80 Abs. 2 bestätigt diese Lesart, denn es wird hierzu ausgeführt:

> „Der Auskunftsanspruch unterliegt weiterhin den allgemeinen Einschränkungen des § 2 Abs. 3 S. 2 HDSIG-E, so dass das Auskunftsrecht etwa nicht gegenüber öffentlichen Stellen gilt, soweit diese als Unternehmen am Wettbewerb teilnehmen.“

Eine solche Bereichsausnahme erscheint nicht erforderlich, da der Schutz von Betriebs- oder Geschäftsgeheimnissen privatrechtlich organisierter staatlicher Unternehmen ohnehin über § 82 Nr. 4 gewährleistet wird.
Die in Absatz 3 getroffene Regelung, dass wiederum Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und mehrheitlich in der Hand einer oder mehrerer öffentlicher Stellen sind, als öffentliche Stellen gelten, steht hinsichtlich des Informationszugangs in einem Widerspruch zu der Wertung des Absatzes 2. Vor dem Hintergrund des Ziels der Informationsfreiheit, einen möglichst einheitlichen, umfassenden und voraussetzungslosen Zugang zu amtlichen Informationen zu ermöglichen, erscheint die Privilegierung in Absatz 2 als nicht zielführend, sondern verwirrend. Die Möglichkeit, Informationen eines staatlichen oder kommunalen Unternehmens der Daseinsvorsorge zu erhalten, wird dann zum einen davon abhängen, ob dieses Unternehmen Monopolist ist oder mit anderen Unternehmen am Markt konkurriert und zum anderen von der gewählten Organisationsform. Es wird aber kein allgemeiner Zugang zu amtlichen Informationen aller öffentlichen Unternehmen gewährt, der lediglich hinsichtlich der Beachtung schützenswerter Belange einzuschränken ist.
Der Kreis der informationspflichtigen Stellen könnte klarer und bürgerfreundlicher definiert werden. Als Beispiel könnte hier die Begriffsbestimmung in § 3 Abs. 1 (ohne Hs. 2) und Abs. 2 S. 1 und 2 LTranspG dienen. Diese lautet:

> (1) Dieses Gesetz gilt für die Behörden des Landes, der Gemeinden und der Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, soweit sie in öffentlich-rechtlicher oder privatrechtlicher Form Verwaltungstätigkeit ausüben.
> (2) Behörde ist jede Stelle im Sinne des § 2 des Landesverwaltungsverfahrensgesetzes. Für den Zugang zu amtlichen Informationen ist Behörde im Sinne dieses Gesetzes auch eine natürliche oder juristische Person des Privatrechts, soweit eine Behörde sich dieser Person zur Erfüllung ihrer öffentlichen Aufgaben bedient oder dieser Person die Erfüllung öffentlicher Aufgaben übertragen wurde.

3. § 80 Abs. 1 und 2 (Anspruch auf Informationszugang/ besondere Vorschriften)

Zu Absatz 1:
Die im HDSIG-E verwendete Terminologie ist insofern uneinheitlich, als in §§ 80 und 82 die Begrifflichkeit des „Anspruchs auf Auskunft“ gewählt wird, in § 81 Abs. 1 hingegen der „Zugang zu Informationen“. Auch die Gesetzesbegründung schafft keine Klarheit, da sie zu § 80 (Anspruch auf Auskunft) ausführt: „§ 80 Abs. 1 HDSIG-E gewährt jedermann einen Anspruch auf Zugang zu den bei öffentlichen Stellen vorhandenen amtlichen Informationen.“
Die Differenzierung zwischen dem Anspruch auf Auskunft und dem Zugang zu Informationen kennzeichnet u.a. den unterschiedlichen Umfang der Ansprüche nach dem Landespresserecht und nach den Informationsfreiheitsgesetzen. Das OVG Berlin-Brandenburg hat diesen Unterschied in einem Leitsatz formuliert: „Presserechtliche Auskunftsansprüche beziehen sich grundsätzlich nur auf die Beantwortung konkreter Fragen, nicht aber auf Aktennutzung durch Einsichtnahme in oder Kopie von Behördenakten“ (OVG 6 S 48.13). Aus diesem Grunde sollte die im HDSIG-E verwendete Begrifflichkeit vereinheitlicht werden.

Zu Absatz 2:
Die Gesetzesbegründung zu Absatz 2 führt aus, dass der Zugangsanspruch nach Absatz 1 gegenüber Regelungen anderer Rechtsvorschriften über Auskunftsbegehren keine Anwendung findet. Für problematisch erachtet wird – aus Gründen des oben beschriebenen Unterschieds zwischen dem Recht auf Auskunft und dem Recht auf Zugang zu amtlichen Informationen –, dass hier explizit das Hessische Presserechtsgesetz genannt wird. Zum einen ist der Anspruch auf Auskunft kein aliud zu einem Anspruch auf Zugang zu Originaldokumenten, zum anderen wird verkannt, dass ein Pressevertreter auch in seiner Eigenschaft als natürliche Person einen Anspruch auf Informationszugang haben muss und hiervon nicht ausgenommen werden kann.
Die in der derzeitigen Ausformulierung von § 80 Abs. 2 getroffene Regelung bewirkt eine Schlechterstellung von Pressevertretern im Vergleich zu Bürgerinnen und Bürgern. Hiervon sollte Abstand genommen werden. Vielmehr sollte unterschieden werden, zwischen einem voraussetzungsgebundenem Auskunftsrecht und dem voraussetzungslosen Informationszugangsrecht.

4. § 81 (Anwendungsbereich und Bereichsausnahmen)

Zu Absatz 1:

a. Abs. 1 Nr. 2: Hessischer Rechnungshof

Die Regelung der Quasi-Bereichsaufnahme für den Hessischen Rechnungshof könnte klarer formuliert werden. Insbesondere der Begriff der „Aufgabenstellung“ ist nicht hinreichend konkret. Klarer wäre es, zwischen der Prüftätigkeit und der sonstigen Verwaltungstätigkeit der Behörde zu differenzieren. Als Beispiel könnte die entsprechende Regelung des § 3 Abs. 5 Satz 1-3 LTranspG dienen. Diese lautet:

> (5) Dieses Gesetz gilt für den Landesrechnungshof nur, soweit antragstellenden Personen durch Auskunft, Akteneinsicht oder in sonstiger Weise Zugang zu dem Prüfungsergebnis gewährt wird, wenn dieses abschließend festgestellt wurde. Zum Schutz des Prüfungs- und Beratungsverfahrens wird Zugang zu den zur Prüfungs- und Beratungstätigkeit geführten Akten nicht gewährt. Dies gilt auch für die entsprechenden Akten bei den geprüften Stellen.

b. Abs. 1 Nr. 2:

Nicht ersichtlich sind die Gründe für eine Bereichsausnahme für den Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Dessen Interessen werden durch die Schutzbestimmungen gewahrt. Unsere Erfahrung hinsichtlich der praktischen Geltung des LTranspG RLP zeigt, dass die Glaubwürdigkeit des Informationsfreiheitsbeauftragten gestärkt wird, wenn auch er auskunftspflichtige Stelle im Sinne des Informationsfreiheitsgesetzes ist. Deshalb wird hier angeregt, eine grundsätzliche Informationspflicht zu normieren, die ggf. hinsichtlich der Kontrolltätigkeit eingeschränkt werden könnte.

c. Abs. 1 Nr. 5:

Die explizite Normierung, dass Schulen und Hochschulen im Bereich der Wahrnehmung von Verwaltungsaufgaben auskunftspflichtige Stellen im Sinne des HDSIG-E sind, wird als sinnvoll erachtet.

d. Abs. 1 Nr. 6 und § 88 Abs. 2:

Kernproblem des Gesetzentwurfs

Die in Absatz 1 Nr. 6 getroffene Bestimmung, dass die Behörden und sonstigen öffentlichen Stellen der Gemeinden und Landkreise sowie deren Vereinigungen durch einen eigenen Rechtsakt, (dem Erlass einer Satzung) die Anwendbarkeit der §§ 80 bis 89 bestimmen können, stellt den größten Kritikpunkt am vorliegenden Gesetzentwurf dar.

Zur leichteren Realisierbarkeit: Mustersatzungen für Kommunen anbieten

Die Gesetzesbegründung führt zutreffen aus, dass die Erfahrungen der anderen Bundesländer belegen, dass das größte Interesse der Bürgerinnen und Bürger den Informationen gilt, über die die Kommunen verfügen. Dies erstaunt nicht, denn die tägliche Lebensführung jeder und jedes Einzelnen wird zumeist mehr durch die Rahmenbedingungen im unmittelbaren Lebensumfeld beeinflusst, als durch bundes- oder landespolitische Entscheidungen und Vorgaben. Daraus den Schluss zu ziehen, es zur Wahrung des kommunalen Selbstverwaltungsrechts den Kommunen anheim zu stellen, ob diese die Anwendung des HDSIG-E ausdrücklich durch Satzung bestimmen möchten, erscheint verfehlt.

Sollte dieser Weg gewählt werden, sollte den Kommunen seitens des Landes zumindest eine Mustersatzung zur Verfügung gestellt werden, um die Hürde für die Anwendbarkeit des vierten Teils des HDSIG-E zu senken.

Eigene Festlegung des Kostenrahmens durch Satzungen der Kommunen

Dass die Kommunen für den Informationszugang Kosten nach Maßgabe ihrer Satzung erheben, ist problematisch. Um eine landesweite Einfachheit und Einheitlichkeit zu gewährleisten, sollte der Kostenrahmen des Landes einheitlich für den Informationszugang bei allen auskunftspflichtigen Stellen des Landes Hessen gelten. Die geplante Lösung hingegen führt zu einer erheblichen Ungewissheit für den Antragsteller auf kommunaler Ebene, zu landesweit uneinheitlichen Kosten des Informationszugangs und damit zu einer Rechtszersplitterung, die für Bürgerinnen und Bürger nicht verständlich sein wird. Dies könnte auch die Akzeptanz des Gesetzes beeinträchtigen.

Zu Absatz 2 Nr. 1:
Die Erfahrungen mit dem LTranspG haben gezeigt, dass eine Bereichsausnahme für die Polizei und den Verfassungsschutz entbehrlich ist, und dass es zum Schutz der Tätigkeit dieser Behörden ausreichend ist, den Zugang zu schutzbedürftigen Informationen im Rahmen der Normierung der dem Informationszugang entgegenstehenden Belange zu regeln (vgl. § 14 LTranspG RLP). Entsprechend könnten statt des § 81 Abs. 2 Nr. 1 schützenswerte Belange in § 82 aufgenommen werden. Sie sind in Teilen bereits in § 82 Nr. 2b normiert.

Zu Absatz 3: „wenn sie sich in Dateien oder Akten anderer öffentlicher Stellen befinden“
Problematisch erscheint die Realisierbarkeit wegen des hohen Abstimmungsbedarfs zwischen den öffentlichen Stellen; die erforderliche Abstimmung wird zu einer Verzögerung des Informationszugangs führen; auch kann diese Regelung dazu führen, dass der Informationszugang im Zweifel unterbleibt, wenn nicht sichergestellt werden kann, dass man alle betroffenen Behörden einbezogen hat. Die Abstimmung kann als mehrstufiger Verwaltungsablauf gestaltet werden, sodass sich der Anspruchsinhaber nur an einen Anspruchs- bzw. Klagegegner wenden muss. Die ergänzende Regelung könnte wie folgt lauten: „Befinden sich Datei- oder Aktenbestandteile von Stellen nach Absatz 1 oder Absatz 2 (Ausgangsstellen) in Dateien oder Akten anderer öffentlicher Stellen, so entscheidet die Ausgangsstelle im Einvernehmen mit der anderen öffentlichen Stelle über den Antrag auf Informationszugang.“

5. § 82 Schutz besonderer öffentlicher und privater Belange

a. Nr. 4 (Schutz personenbezogener Daten)

Die erste Fallgruppe „zum persönlichen Lebensbereich gehörenden Geheimnisse“ könnte ersatzlos gestrichen werden. Ein zum persönlichen Lebensbereich gehörendes Geheimnis ist ein personenbezogenes Datum. Der Informationszugang zu einem solchen Datum würde sich dann nach § 83 i.V.m. § 22 richten. Dies hätte zur Folge, dass die Verarbeitung personenbezogener Daten nach einheitlichen Maßstäben beurteilt würde.

b. Nr. 5 (kein Anspruch bei einem rein wirtschaftlichen Interesse an der Information)

§ 82 Nr. 5 normiert den Ausschluss des Informationszugangs in den Fällen, in denen ein rein wirtschaftliches Interesse an der Information besteht. Aus praktischen Erwägungen stellt sich die Frage, wie ein solcher Nachweis geführt werden soll. Davon abgesehen kollidiert diese Regelung mit der Grundidee moderner Informationsfreiheitsgesetze, dass neben den positiven Effekten für die Demokratie und die Beteiligung und neben der Bekämpfung von Korruption auch ein Mehrwert aus den zugänglich gemachten Informationen der Verwaltung generiert werden soll.
Die EU bringt diese Ideen u.a. in der PSI-Richtlinie (2003/98/EG) über die Weiterverwendung von Informationen des öffentlichen Sektors und in der Richtlinie 2013/37/EU zur Änderung der PSI-Richtlinie zum Ausdruck. Der Erwägungsgrund (3) zur Richtlinie 2013/37/EU lautet:

> „Eine Politik der Förderung offener Daten, die eine breite Verfügbarkeit und Weiterverwendung von Daten des öffentlichen Sektors zu privaten oder gewerblichen Zwecken mit minimalen oder keinen rechtlichen, technischen oder finanziellen Beschränkungen unterstützt und die Verbreitung von Informationen nicht nur für Wirtschaftsakteure, sondern auch für die Öffentlichkeit fördert, kann eine wichtige Rolle spielen, wenn es darum geht, die Entwicklung neuer

> Dienstleistungen anzustoßen, die solche Informationen auf neuartige Weise kombinieren und nutzen sowie Wirtschaftswachstum und soziales Engagement fördern."

Zwar steht die in § 82 Nr. 5 getroffene Regelung nicht in Widerspruch zu § 2a EWG, da nicht die Weiterverwendung der Information beschränkt, sondern bereits kein Informationszugang gewährt wird, doch läuft die getroffene Regelung eindeutig der Intention der PSI-Richtlinie zuwider.

6. § 84 Abs. 3 (Protokolle vertraulicher Beratungen)

Weder § 84 Abs. 3 selbst noch die Gesetzesbegründung legen fest, welche Beratungen vertraulich sind. Damit wird ein übermäßig weiter Anwendungsbereich der Regelung eröffnet. Der Norm und dem Zweck des vierten Teils drohen dadurch eine weitgehende Aushöhlung. Es sollte nicht in das Ermessen von Besprechungsteilnehmern oder Gremien gestellt werden, die Regelungen über den Informationszugang durch Individualvereinbarung auszuschließen. Das liefe dem Gesetzeszweck – der offenen und transparenten Gestaltung von Verwaltungshandeln (LT-Drs. 19/5728, vgl. S. 116) – zuwider.
Es stellt sich außerdem die Frage, ob bei vertraulichen Beratungen dem Transparenzgedanken nicht dadurch Rechnung getragen werden könnte, dass – vorbehaltlich entgegenstehender Belange – zumindest die Entscheidungsgrundlagen und -ergebnisse veröffentlicht werden. Hier bietet die Verwaltungsvorschrift zum LTranspG eine ausgewogene und differenzierte Lösung:

> „Der Begriff der Beratung bezieht sich nur auf den Beratungsvorgang. Ausgenommen vom Schutzbereich der Vorschrift sind das Beratungsergebnis und der Beratungsgegenstand. Der Begriff der Beratung erfasst die Vorgänge interner behördlicher Meinungsäußerung und Willensbildung, die sich inhaltlich auf die Entscheidungsfindung beziehen. Der Schutz gilt vor allem dem Beratungsprozess als solchem, also der Besprechung, Beratschlagung und Abwägung, d. h. dem eigentlichen Vorgang des Überlegens. Zum nicht geschützten Beratungsgegenstand können insbesondere Sachinformationen oder gutachterliche Stellungnahmen im Vorfeld gehören, also die Tatsachengrundlagen und Grundlagen der Willensbildung. Die amtlichen Informationen sind daher nur dann geschützt, wenn sie den Vorgang der behördlichen Willensbildung und Abwägung abbilden oder jedenfalls gesicherte Rückschlüsse auf die Meinungsbildung zulassen."

Es wird zudem angeregt, die Norm um eine Präzisierung des Begriffs der „vertraulichen Beratung" zu ergänzen.

7. § 85 Antrag

a. Abs. 2 Satz 2 (Informationen, die aus einer Vielzahl von Aktenvorgängen zusammengetragen werden müssen)

Die Erfahrungen der Informationsfreiheitsbeauftragten in Bund und Ländern zeigen, dass die Anfragen der Bürgerinnen und Bürgern an öffentliche Stellen zumeist auf Lebenssachverhalte gerichtet sind, z.B. den Umbau einer Schule. Auf der Seite der Verwaltung sind häufig mehrere Zuständigkeitsbereiche einer Behörde in die Realisierung eines solchen Projekts eingebunden. Die in § 85 Abs. 2 S. 2 getroffene Regelung läuft dieser Erkenntnis ebenso zuwider wie dem Sinn und Zweck der Gewährung eines voraussetzungslosen Informationszugangsanspruchs. Den Informati-

onsanspruch dann auszuschließen, wenn er auf „allgemeines Behördenhandeln“ gerichtet ist – also etwa die Frage nach Entscheidungsmaßstäben oder Vergabe- oder Auswahlkriterien –, und auch dann, wenn sich die Anfrage auf Informationen bezieht, die „aus einer Vielzahl von Aktenvorgängen und Informationsträgern zusammengetragen werden müssen“, bleibt hinter dem anerkannten informationsfreiheitsrechtlichen Status quo zurück.
Das IFG des Bundes und fast alle Informationsfreiheitsgesetze der Länder stellen auf das Vorhandensein der Information ab. Entsprechend besteht – von Ausnahmen abgesehen – also keine Informationsbeschaffungspflicht einer öffentlichen Stelle.
Die Regelung des § 85 Abs. 2 S. 2 zielt auf den für ein Informationsbegehren zumutbaren Verwaltungsaufwand ab. Hier hat der Hessische Verwaltungsgerichtshof (VGH Hessen, 02.03.2010 - 6 A 1684/08) am Beispiel der BaFin in einem Leitsatz eine Formel entwickelt, die der Orientierung dienen kann:

> „Die auf § 7 Abs. 2 Satz 1 IFG gestützte vollständige Ablehnung eines hinreichend konkret und präzise gefassten Zugangsantrags wegen eines hierdurch verursachten unverhältnismäßigen Verwaltungsaufwands ist nur unter Anlegung strenger Maßstäbe möglich. Die Grenze zur Unverhältnismäßigkeit des Verwaltungsaufwands ist in diesen Fällen grundsätzlich erst dann überschritten, wenn durch die Art des Informationszugangsbegehrens oder seinen Umfang ein Verwaltungsaufwand notwendig ist, der den bei üblichen Gesuchen an die Behörde verursachten Aufwand in solch deutlichem Maße übersteigt, dass die Behörde das Gesuch letztlich nur unter nicht nur vorübergehender Zurückstellung ihrer sonstigen Aufgaben bewältigen kann.“

Die Verwaltungsvorschrift zum rheinland-pfälzischen LTranspG führt zu dem Kriterium des Vorhandenseins einer Information folgendes aus:

> „Vorhandene Informationen sind alle Informationen, die durch Heraussuchen aus Akten, Vorgängen oder Dateien zusammengetragen werden können. Unschädlich ist dabei, dass ggf. Teile der Unterlagen unkenntlich zu machen sind. Nicht zu den vorhandenen Informationen gehören Informationen, die erst durch eine weitere Aufbereitung oder Bearbeitung herausuchbarer Informationen gewonnen werden können (z. B. Nachfrage nach einer Bewertung von Zahlenmaterial, die bislang nicht vorgenommen wurde). Es besteht somit die Pflicht, die begehrten Informationen ggf. aus vielen Dokumenten herauszusuchen, aber kein Anspruch darauf, dass die Informationen gesondert zusammengestellt, aufbereitet oder bewertet werden. Die Behörde ist jedoch nicht gehindert, Informationen auch gesondert zusammenzustellen, insbesondere, wenn dies für sie weniger Aufwand verursacht. Der Europäische Gerichtshof hat in seiner Entscheidung vom 11. Januar 2017, Az. C-491/15 P, zu der Verordnung Nr. 1049/2001 zu der Frage, wann ein Dokument als vorliegend anzusehen ist, entschieden, dass als vorliegendes Dokument alle Informationen einzustufen sind, die aus einer elektronischen Datenbank im Rahmen ihrer üblichen Nutzung mit Hilfe vorprogrammierter Suchfunktionen extrahiert werden können, auch wenn diese Informationen noch nicht in dieser Form angezeigt wurden oder von den Bediensteten der Organe nie gesucht worden sind.“

Diese Auffassung erscheint zum einen praktikabel und hat sich bereits in der rheinland-pfälzischen Anwendungspraxis bewährt. Zum anderen beschreiben die Entscheidung des Hessischen VGH und die Verwaltungsvorschrift zum rheinland-pfälzischen LTranspG den derzeitig herrschenden

informationsfreiheitsrechtlichen Standard in Deutschland, der mit der in § 85 Abs. 2 Satz 2 gewählten Regelung deutlich unterschritten würde.

Sachgerecht ist die Regelung in § 85 Abs. 2 Satz 3, welche die Behörde zur Beratung des Antragstellers verpflichtet.

b. Abs. 3

Eine Begründung ist nicht erforderlich, da die §§ 82 f. keine Ermessensentscheidung vorsehen.

c. Abs. 4

Satz 2 könnte durch die Einschränkung „(…) soweit der angerufenen Stelle die zuständige Stelle bekannt ist“ ergänzt werden. Damit würde erreicht, dass die angerufene Stelle nicht selbst nach der informationshaltenden Stelle recherchieren muss und so schonend mit den personellen Ressourcen der Verwaltung umgegangen wird.

8. § 87 Abs. 3 (Frist)

Die in § 87 Abs. 1 Halbsatz 1 getroffene Regelung sollte wie folgt geändert werden:„Die informationspflichtige Stelle macht die begehrten Informationen in der Regel unverzüglich, (…)“.
Gelungen ist, dass neben der Regelfrist von einem Monat auch eine absolute Höchstfrist von drei Monaten normiert wird, innerhalb derer der Informationszug erfolgen muss.

9. § 88 Abs. 1 (Kosten)

Nach § 88 Abs. 1 richtet sich die Höhe der Kosten – in Anlehnung an § 11 HUIG – nach der Maßgabe des Hessischen Verwaltungskostengesetzes in Verbindung mit der dazu ergangenen Allgemeinen Verwaltungskostenordnung. Diese Regelung führt zu einer möglichst einfachen und landesweit einheitlichen Kostenregelung hinsichtlich des Zugangs zu amtlichen Informationen bei Behörden des Landes.

10. § 89 Abs. 3 (Die oder der Hessische Informationsfreiheitsbeauftragte)

Nicht eindeutig aus der Norm geht hervor, wer „ihre oder seine Beauftragten“ i.S. d. § 89 Abs. 3 Satz 1 sind.
Die Befugnisse der oder des Informationsfreiheitsbeauftragten sollten in § 89 genannt werden. Dies kann durch eine entsprechende Übernahme der Befugnisse aus § 14 geschehen. Zudem sollte die Aufgabe der oder des Informationsfreiheitsbeauftragten normiert werden. Möglich wäre eine § 16 Abs. 2 LTranspG entsprechende Regelung.

11. Zusätzliche Anregungen

a. Legaldefinition des Begriffs der amtlichen Information

Die Regelungen des Vierten Teils des HDSIG-E beziehen sich offensichtlich auf den Zugang zu amtlichen Informationen auf Antrag. Nicht berührt werden die Regelungen zum Zugang zu Umweltinformationen bei öffentlichen Stellen des Landes Hessen im HUIG. Aus diesem Grunde und auch aus Gründen der Rechtssicherheit und zur besseren Anwendbarkeit der getroffenen Regelungen

wird angeregt, den Begriff der amtlichen Informationen z.B. in § 80 zu definieren. Als Beispiel sei hier auf § 5 Abs. 2 LTranspG verwiesen. Er lautet:

> (2) Amtliche Informationen sind alle dienstlichen Zwecken dienenden Aufzeichnungen; dies gilt für Entwürfe und Notizen nur, wenn sie Bestandteil eines Vorgangs werden sollen.

Diese Regelung könnte im Halbsatz 1 wie folgt ergänzt werden: „Amtliche Informationen sind alle dienstlichen Zwecken dienenden Aufzeichnungen, unabhängig von der Art ihrer Speicherung."

b. Erweiterung der Zuständigkeit des Hessischen Informationsfreiheitsbeauftragten auf den Zugang zu Umweltinformationen nach dem HUIG

Die Konferenz der Informationsfreiheitsbeauftragten der Länder und des Bundes hat im Rahmen ihrer Sitzung vom 14. November 2017 eine Stellungnahme verabschiedet, mit der sie sich in den derzeit laufenden Prozess der Evaluation des Umweltinformationsgesetzes des Bundes einbringt. Die zentrale Empfehlung der Konferenz lautete, die Zuständigkeit der Informationsfreiheitsbeauftragten deutschlandweit auf die Beratung und Unterstützung von Behörden und Bürgerinnen und Bürgern in Fragen des Zugangs zu Umweltinformationen auszuweiten, da die Informationsfreiheitsbeauftragten in Deutschland ihren Auftrag der Unterstützung der Bürgerinnen und Bürger bei ihrem Bemühen um Zugang zu Informationen nicht umfassend erfüllen können, weil ihnen hierfür wesentliche gesetzliche Kompetenzen fehlen:

> „Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland empfiehlt dringend, im Rahmen der laufenden Evaluation des Umweltinformationsgesetzes darauf hinzuwirken, dass der Bundesgesetzgeber der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Kontrollkompetenz für das Umweltinformationsgesetz einräumt. Ebenso sollte dort, wo dies noch nicht geschehen ist auf Landesebene so verfahren werden. Diese Kompetenz besteht bereits in Schleswig-Holstein und Rheinland-Pfalz. Sie sollte auf Landesebene insgesamt eingeführt werden." (Volltext der Stellungnahme unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Konferenzdokumente/Informationsfreiheit/Stellungnahme_UIG_IFK_20171114.pdf)

Insofern könnte mit der Übertragung der Zuständigkeit für die Umweltinformationen auf den künftigen Hessischen Informationsfreiheitsbeauftragten eine zeitgemäße und bürgerfreundliche Regelung geschaffen werden.

c. Rechtswegregelung

In den Entwurf des HDSIG-E könnte zur Stärkung der Bürgerorientierung und zur Klarstellung, dass bei Streitigkeiten hinsichtlich des Informationszugangs der Verwaltungsrechtsweg gegeben ist, eine Rechtswegregelung aufgenommen werden. Der § 19 ist zwar mit „Gerichtlicher Rechtsschutz" überschrieben, trifft aber keine Aussage über den Rechtsschutz bei Streitigkeiten, die den Informationszugang betreffen. Es wird angeregt, eine Regelung aufzunehmen, die der des § 9 HUIG (Rechtsschutz) entspricht.

d. Evaluierungsklausel

Da mit dem vorliegenden Entwurf erstmals im Land Hessen der allgemeine und voraussetzungslose Zugang zu amtlichen Informationen gesetzlich geregelt wird, empfiehlt es sich, eine Evaluierungsklausel in das Gesetz aufzunehmen. Idealer Weise sollte eine wissenschaftliche Evaluierung erfolgen. Die existierenden Evaluationen zu dem IFG des Bundes aus dem Jahre 2012, zu dem LIFG Rheinland-Pfalz (ebenfalls aus 2012) und der Abschlussbericht zur Evaluation des Hamburgischen Transparenzgesetzes vom 02.08.2017 zeigen, dass eine wissenschaftliche Beurteilung der gesetzlichen Regelungen hilfreich ist, um einen Überblick über die landesweite Anwendungspraxis des Gesetzes zu erhalten und um eventuelle Schwachstellen im Rahmen einer Novellierung beheben zu können.

Gez.
Prof. Dr. Dieter Kugelmann

***die*Datenschützer** Rhein Main

Stellungnahme zum Gesetzesentwurf der Fraktionen CDU und BÜNDNIS 90/DIE GRÜNEN

für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit vom 5.12.2017 (Drucks. 19/5728)

E-Mail: kontakt@ddrm.de Internet: https://ddrm.de/

Stellungnahme zum Gesetzesentwurf Artikel 1

Erster und zweiter Teil – Hessisches Datenschutzgesetz, allgemeine Bestimmungen und Umsetzung der EU Datenschutz-Grundverordnung

1 (Maßlose) Videoüberwachung öffentlich zugänglicher Räume

Im vorliegenden Entwurf werden in § 4 HDSIG-E konkrete Regelungen zur Videoüberwachung durch öffentliche Stellen getroffen. Das ist grundsätzlich begrüßenswert. Jedoch ist die Norm viel zu weit gefasst und in Abs. 1 Punkt 3 insoweit nicht normenklar, als die konkret festgelegten Zwecke nicht weiter eingeschränkt oder beschrieben werden. An dieser Stelle sehen ***die*Datenschützer** Rhein Main deutlichen Nachbesserungsbedarf.

Weiterhin soll in § 4 Abs. 3 HDSIG-E eine Zweckänderung selbst bei nicht geringfügigen Ordnungswidrigkeiten erlaubt werden. Nach der Definition sind das Ordnungswidrigkeiten, die mit einem Bußgeld höher als 55,-- Euro belegt werden können. So werden Bagatellen Gegenstand exzessiver öffentlicher Überwachung.

In Summe sehen wir die Norm im Konflikt mit der Rechtsprechung des BVerfG und halten sie in dieser Form für verfassungswidrig.

2 (Eingeschränkte) Befugnisse der oder des Hessischen Datenschutzbeauftragten

Gegenüber den Regelungen aus der EU DS-GVO fallen die Befugnisse der oder des Hessischen Datenschutzbeauftragten in Fällen, in denen diese nicht einschlägig ist, ungewöhnlich gering aus. Nach § 14 Abs. 3 HDSIG-E bestehen insbesondere keine Möglichkeiten, eine Verarbeitung zeitweise oder gänzlich zu unterbinden oder zu beschränken oder eine Übermittlung in ein Drittland auszusetzen.

Weiterhin erlaubt § 14 Abs. 5 HDSIG-E einer obersten Landesbehörde die ohnehin schwachen Befugnisse aus Abs. 3 der Norm lediglich durch die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten ausüben zu lassen. Angesichts der umfänglichen Aufgaben dieser Person sehen ***die*Datenschützer** Rhein Main darin nicht nur eine gefährliche Regelung in Bezug

auf die unmittelbare Ausübung des Befugnisse, sondern auch ein unberechtigtes Misstrauen gegenüber den Beschäftigten.

Soweit in diesen Fällen sogar der oder dem Hessischen Datenschutzbeauftragten Zugriff auf personenbezogenen Daten verweigert werden kann, sehen wir einen grundsätzlichen Widerspruch zu Art. 38 (2) EU DS-GVO.

3 Benachteiligungsverbot

Ausdrücklich begrüßen möchten wir die Regelungen des § 17 HDSIG-E.

4 Verarbeitung zu anderen Zwecken

§ 21 HDSIG-E regelt, unter welchen Voraussetzungen die Weiterverarbeitung personenbezogener Daten zu einem anderen als dem Erhebungszweck möglich sein soll. Die Norm ist insofern bedeutsam, als in der Folge sich einige weitere Normen auf sie direkt oder indirekt beziehen insbesondere §§ 22 und 27 HDSIG-E.

Für sich genommen erscheint der Regelungsgehalt mit Ausnahme von Abs. 6, soweit er die Verarbeitung zu Ausbildungs- und Prüfzwecken zulässt, angemessen. ***die*Datenschützer** Rhein Main befürchten dennoch, dass durch die Summe der Ausnahmetatbestände die Grundsätze der direkten Erhebung und der Zweckbindung insbesondere im Zusammenhang mit § 22 HDSIG-E unzulässig aufgeweicht werden.

5 (Nahezu ungebremste) Datenübermittlung durch öffentliche Stellen

Unter der Maßgabe des eben genannten § 21 HDSIG-E eröffnet § 22 HDSIG-E Abs. 1 die Übermittlung personenbezogener Daten an andere öffentliche Stellen. Zwar erfolgt diese Übermittlung in Satz 2 unter der Bedingung, dass die aus der Übermittlung resultierende Zweckbindung eingehalten wird, aber schon Satz 3 hebt diese Verfügung in sofern wieder auf, als dass sie unter Maßgabe von wiederum § 21 HDSIG-E eine erneute Zweckänderung zulässt.

Diese Regelung findet sich sogar in § 21 Abs. 2 bei der Datenübermittlung an nichtöffentliche Stellen.

Unter diesem Licht erhält § 21 HDSIG-E eine besondere Schärfe, zumal die Normen keine Regelung über eine Unterrichtungspflicht an die Betroffenen nach Art. 14 EU-DSGVO vorsehen. Die ergänzenden Regelungen aus den §§ 31 und 32 HDSIG-E werden wir weiter unten beleuchten. In keinem Fall jedoch werden sie der kaskadenartigen Weitergabe von personenbezogenen Daten gerecht.

6 (Kaum) Rechte der betroffenen Person bei Geheimhaltungspflichten

§ 26 Abs. 1 möchte weitere Ausnahmetatbestände zur Informationspflicht nach Art. 14 Abs. 1 bis 4 EU-DSGVO verankern, wenn diese Informationen dem Wesen nach der Geheimhaltung zugeschrieben werden. Insbesondere wird sich explizit nicht, was naheliegend gewesen wäre, auf Art. 14 Abs. 5 c) und d) DSGVO bezogen. Daher ist zu unterstellen, dass ein weiterer Tatbestand hinzugefügt werden soll. Dabei verkennen die einbringenden Fraktionen nach Ansicht von ***die*Datenschützer** Rhein Main, dass Art. 14 EU-DSGVO keine Öffnungsklausel enthält und insofern der Ausnahmekatalog abschließend und eine nationale gesetzgeberische Kompetenz nicht gegeben ist. Selbiges gilt für die Art. 13, 15 und 34 EU-DSGVO, die in den Abs. 2, 3 und 4 des § 26 adressiert werden.

Insbesondere § 26 Abs. 4 ist einer besonderen Betrachtung wert. Dieser regelt vordergründig die Einschränkung zur Pflicht der Information der Betroffenen im Falle einer Datenübermittlung im Rahmen des Mandatsverhältnisses an einen Berufsgeheimnisträger. Bezug genommen wird jedoch auf Art. 13 Abs. 3 DSGVO. Dieser regelt jedoch keine Weitergabe, sondern eine Zweckänderung. Es ist fraglich, ob hier nicht Art. 14 Abs. 3 EU-DSGVO insbesondere Punkt c) gemeint gewesen sein könnte.

7 (Weitere) Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften

§ 27 HDSIG-E erlaubt unter der Maßgabe des § 22 HDSIG-E und somit auch erneut § 21 HDSIG-E die Weitergabe personenbezogener Daten an öffentlich-rechtliche Religionsgemeinschaften, also bei (verkürzt dargestellt):

- offensichtlich im Interesse der Betroffenen liegenden Gründe
- Überprüfung von Unrichtigkeiten
- Abwehr erheblicher Nachteile für das Gemeinwohl
- Verfolgung von Straftaten oder Ordnungswidrigkeiten
- Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person oder
- Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder Durchführung von Organisationsuntersuchungen

Hier wäre eine weitaus restriktivere Handhabung denkbar und nach unserer Meinung erforderlich gewesen.

8 (Unzulässig eingeschränkte) Informationspflichten bei der Erhebung

Wie bereits erwähnt, sollen nach § 31 HDSIG-E die Informationspflichten nach Art. 13 Abs. 3 DSGVO eingeschränkt werden, also die Unterrichtung bei geplanter zweckfremder Weiterverarbeitung und erneut soll der Ausnahmekatalog in Abs. 4 unzulässig erweitert werden. Stattdessen sollen die Anforderungen aus Art 13 Abs. 1 und 2 EU DS-GVO durch Bereitstellung für die Öffentlichkeit erfüllt werden. Aber auch hiervon gibt es wieder Ausnahmen, wenn

1. eine Weiterverarbeitung analog gespeicherter Daten betrifft, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem Erhebungszweck nach der EU DS-GVO vereinbar ist, die Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere mit Blick auf den Zusammenhang, indem die Daten erhoben wurden, als gering anzusehen ist,
2.
    a) die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 Buchst. a bis e der EU DS-GVO gefährden,
    b) die öffentliche Sicherheit oder Ordnung gefährden,
    c) die Rechte oder Freiheiten Dritter gefährden,
    d) die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen oder
    e) sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde und das Interesse des Verantwortlichen an der Nichterteilung der Information das Informationsinteresse der betroffenen Person überwiegt.
3. eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.

Die Entscheidung trifft jeweils die Behördenleitung.

Nach Ansicht von ***die*Datenschützer** Rhein Main ist diese Regelung unverhältnismäßig und verstößt zudem gegen Europarecht aus der EU DS-GVO

9 (Unzulässig eingeschränkte) Informationspflichten bei indirekter Erhebung

Auch § 32 HDSIG-E verstößt nach unserer Ansicht gegen Europarecht, wenn der Gesetzgeber sich anmaßt die Ausnahmetatbestände nach Art 14 Abs. 5 EU DS-GVO

„ergänzen“ zu dürfen, also nicht explizit auf Abs. 5 c) und d) zurück zu greifen.

Die Ausnahmen umfassen:

1. die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 Buchst. a bis e der EU DS-GVO gefährden,
2. die öffentliche Sicherheit oder Ordnung gefährden,
3. die Rechte oder Freiheiten Dritter gefährden oder
4. sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten

Die Entscheidung trifft erneut die Behördenleitung und die Regelung aus § 31 HDSIG-E, dass die Information lediglich für die Öffentlichkeit bereit gestellt werden muss, findet erneut Anwendung.

Abs. 3 der Norm fügt dann noch eine Ausnahme für die Bereitstellung ein, nämlich den Vorbehalt der Zustimmung bei Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung.

Insbesondere bemerkenswert ist nach Ansicht von ***die*Datenschützer** Rhein Main, dass für Erstgenannte nicht einmal ein Sicherheitsinteresse vorherrschen oder dargelegt muss.

10 (Unzulässig eingeschränkte) Auskunftsrechte

Die Auskunftsrechte aus Art. 15 EU-DSGVO werden in § 33 HDSIG-E zum Einen weiter eingeschränkt durch die Ausnahmen in den §§ 24 (wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken), 25 (im öffentlichen Interesse liegenden Archivzwecken) und 26 (siehe oben), zum Anderen werden weitere Ausnahmen hinzugefügt, wenn

1. die betroffene Person nach § 32 Abs. 1 oder 3 nicht zu informieren ist, oder

2. die Daten

a) nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder

b) ausschließlich Zwecken der Datensicherung, der Datenschutzkontrolle oder der Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen.

Im Wesentlichen handelt es sich um eine Kopie des § 34 BDSG-neu, dessen Rechtmäßigkeit durchaus umstritten ist.

Wenn gleich ***die*Datenschützer** Rhein Main zumindest die Regelung 2 b) positiv beurteilen, steht ihr die abschließende Behandlung des Art. 15 EU DS-GVO entgegen.

Hinzugefügt wurde in § 33 Abs. 3 eine Regelung, dass Betroffene sich an den HDSB wenden können. Grundsätzlich ist diese zu begrüßen. Jedoch darf dieser dann lediglich Mitteilung machen, dass er geprüft habe und keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen.

11 (Unzulässig eingeschränktes) Recht auf Löschung

Art. 17 EU DS-GVO soll durch § 34 HDSIG-E dahingehend erweitert werden, dass bei einer nicht-automatisierten Datenverarbeitung die Löschung unterbleiben kann, wenn sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und das Interesse der betroffenen Person an der Löschung als gering anzusehen ist.

Auch hier ist zu konstatieren, dass Art. 17 EU DS-GVO keinerlei Öffnungsklausel enthält und somit dem nationalen Gesetzgeber keine Regelungskompetenz zufällt. Die Norm ist daher nach unserer Einschätzung ebenfalls europarechtswidrig.

12 Sanktionen

Wie nicht anders zu erwarten, wird in § 26 HDSIG-E die Öffnungsklausel aus Art. 83 (7) dahingehend genutzt, dass gegen Behörden und sonstige öffentliche Stellen keine Bußgelder verhängt werden können. Über den Sinn und Unsinn einer diesbezüglichen Regelung lässt sich trefflich streiten, insgesamt ist die Norm jedoch nicht zu beanstanden.

Abs. 3 der selben Norm fügt eine Regelung hinzu, dass eine Meldung nach Art. 33 EU DS-GVO oder eine Benachrichtigung nach Art. 34 Abs. 1 EU DS-GVO in einem Ordnungswidrigkeitsverfahren gegen die meldepflichtige oder benachrichtigende Person nur mit ihrer Zustimmung verwendet werden.

Der Hintergrund dieser Regelung erschließt sich uns nicht.

Stellungnahme zum Gesetzesentwurf Artikel 1

Vierter Teil: Anspruch auf Informationszugang

13 Vorbemerkungen

Die Regierungsfraktionen des Hessischen Landtages haben einen Entwurf für ein Informationsfreiheits-Gesetz vorgelegt. Anders als in den anderen Bundesländern und im Bund ist es versteckt am Ende des Entwurfes für ein neues Hessisches Datenschutzgesetz in den §§ 80 – 89 GE zu finden.

14 Transparenzgesetz, statt nur Informationsfreiheitsgesetz, Hessisches Grundrecht auf Transparenz

Initiative Transparenz durch die öffentliche Verwaltung geht einem Informationszugang auf dem individuellen Antragsweg vor.

Ein wichtiger Aspekt für ein Transparenzgesetz ist der Grundsatz der Gleichbehandlung aus Art. 3 Grundgesetz (GG). Nur wenn interne Richtlinien, Dienstanweisungen und standardisierte Vorgänge allen bekannt sind, ist gewährleistet, dass auch alle Bürger unter gleichen Voraussetzungen gleich behandelt werden. Die Verwaltung der Finanzämter in Hessen und anderswo handhaben das bereits seit mehr als 50 Jahren so.

Dies geht aber nur, wenn - wie z.B. weitgehend derzeit bei der Finanzverwaltung - die Behörden ein Maximum an Informationen von sich aus veröffentlichen, statt den Informationszugang einem aufwendigen Antragsverfahren zu unterziehen. Veröffentlichungen in Broschüren und in elektronische Form auf der Homepage der jeweiligen Behörde stellen ein hohes Maß an Transparenz her und sind gleichzeitig die kostengünstigste Form des Informationszugangs für Bürger. Ein weit überwiegender Teil der durch diesen Entwurf vorgegebenen Antragsverfahren würden alleine hierdurch gespart – an Aufwand nicht nur für die Behörde sondern auch für die Bürger.

Gerade vor diesem Hintergrund und eingedenk der Tatsache, dass die Hessische Verfassung derzeit im hessischen Landtag einer Überarbeitung unterliegt, fordern ***die*Datenschützer** Rhein Main ein hessisches Grundrecht auf Transparenz und Informationszugang gegenüber allen hessischen Landes- und kommunalen Behörden.

Transparenz ist in einem demokratischen Gemeinwesen Teil der Daseinsvorsorge und kein Luxus.

15 Fehlende Differenzierung zum Informationszugang und zu Zugang zu Richtlinien

Der vorgelegte Entwurf macht keinen Unterschied zwischen dem Informationszugang zu internen Richtlinien, Dienstanweisungen und weiteren standardisierten Vorgängen einerseits und zu dem Zugang zu seltenen und eher spezifischen und oft aufwendigen Verfahren andererseits. Erstere können uneingeschränkt veröffentlicht werden und aus dem kosten-/ gebührenpflichtigen Bereich ganz herausgenommen werden. Nur bei letzteren mag es sinnvoll sein, über Aufwand und Kosten nachzudenken und gegebenenfalls Regelungen zu unterwerfen.

Statt über zahlreiche Ausnahmen, sei es dadurch, dass bestimmte Behördenzweige aus der Informationspflicht herausgenommen werden, sei es, dass durch Bedingungen mir unbestimmten Rechtsbegriffen Ausnahmen formuliert werden, könnten und sollten Ausnahmen eher seltenen, präzise formuliert und vergleichsweise komplexeren Informationsanfragen vorbehalten bleiben.

In dieser perfiden Struktur des vorgelegten Entwurfs wird der Informationszugang an einer Stelle verteuert und gleichzeitig an anderen Stellen mit dem Kostenargument durch Ausnahmeregelungen eingeschränkt. Diese Strukturfalle lehnen ***die*Datenschützer** Rhein-Main ab.

16 Keine Ausnahmen

***die*Datenschützer** Rhein Main wenden sich entschieden gegen den langen und weitestgehend sachfremd begründeten Katalog von Ausnahmen im § 81 des G-Entwurfs.

16.1 Polizei

***die*Datenschützer** Rhein Main haben durch eine einfache Regelung, nämlich dem Einsichtsrecht in das öffentliche Verfahrensverzeichnis des *Frankfurter Polizeipräsidiums* Frankfurt am Main offen gelegt, dass dieses, gegen hessisches Datenschutzrecht verstoßend, Videodaten an Stellen außerhalb der EU übermittelt. Dies war nur möglich mithilfe der Regelungen zum öffentlichen Verfahrensverzeichnis (nach altem Recht im HSOG geregelt). Mit dem öffentlichen Verfahrensverzeichnis entfällt auch das Einsichtsrecht hierzu. Diese Streichung kann nicht damit begründet werden, dass ein Informationsfreiheitsgesetz geschaffen wird, wenn die hessische Polizei uneingeschränkt von diesem Informationszugang ausgenommen wird. Das ist

nicht ein Beitrag zur öffentlichen Sicherheit, sondern zu - auch rechtswidriger - Willkür durch die Polizeibehörden.

16.2 Gemeinden, Landkreise & deren Vereinigungen

Auch die Ausnahme für Gemeinden, Landkreise und Gemeindeverbände ist nicht nachvollziehbar. Vorgeschoben wird hier das Argument der kommunalen Selbstverwaltung. Tatsächlich mag aber eine Gemeinde, die sich durch Satzung eine Regelung zu mehr Transparenz gibt, mit dem Kostenargument von der Landeskommunalaufsicht gerügt oder mit Auflagen besehen werden, an anderer Stelle Einsparungen vorzunehmen, um sich den angeblichen „Luxus“ der Informationsfreiheit erst zu verdienen. Gemeinden, Landkreise und Gemeindeverbände werden durch diese vorgetäuschte Entscheidungsfreiheit erpressbar und gerade in ihrer kommunalen Selbstbestimmung eingeschränkt.

16.3 Forschung & Lehre mit öffentlichen Geldern, sowie Leistungsbeurteilungen & Prüfungen

Das Grundrecht der Freiheit von Forschung und Lehre richtet sich nicht gegen den Bürger sondern gegen den Staat. Diese Ausnahme entbehrt daher jeder Grundlage. Berechtigter Informationszugang gegenüber Hochschulen, Berufsschulung und allgemeinbildenden Schulen schränken der Freiheit von Forschung und Lehre nicht ein. Im Gegenteil in Prüfungsverfahren und die der Verwendung von Forschungsgeldern sind Massen von Bürgern betroffen, so dass der Informationszugang über interne Richtlinien, Dienstanweisungen und andere standardisierte Vorgänge besonders leicht auszumachen sind und auf Initiative der Behörden hin einfach zugänglich gemacht werden können.

16.4 "wirtschaftliches Interesse"

Auch die Ausnahme, dass das Informationsinteresse einen wirtschaftlichen Hintergrund hat, ist abzulehnen.

Dem gesamten Bereich von Medien, Rundfunk und Presse würde so der Informationszugang verwehrt. Dieser Bereich verfolgt im öffentlichen und demokratischen Interesse, wenn auch auf einer wirtschaftlichen Basis, Ziele die unzertrennlicher Bestandteil unseres demokratischen Gemeinwesens sind. Sie aus einem Demokratiefeld, wie behördliche Transparenz herauszunehmen, ist systemwidrig und zutiefst undemokratisch. Der Schaden wäre unabsehbar.

16.5 Behörden mit direktem Kontakt zu Bürgern

Alle Behörden, die einen direkten Kontakt zu Bürgern haben, sollen dieser Transparenz unterliegen. Hierzu zählen auch der Hessische Datenschutzbeauftragte, die IHK und deren Arbeitsgemeinschaften, Handwerkskammern und Notare. Soweit sie einer besonderen Unabhängigkeit unterliegen, wie der Hessische Datenschutzbeauftragte, wird diese durch ein transparentes Behördenhandeln nicht geschmälert. Sie dienen sowohl in ihrem Behördenauftrag als auch in einer

transparenten Vorgehensweise dem Bürger gleichermaßen.

16.6 Datei-, Aktenbestandteile in anderen Behörden

Transparenz über Datei- und Aktenbestandteilen, die in anderen Behörden liegen, offenbaren, wie Behörden zusammen arbeiten. Nur so wird deutlich, ob es sich um eine zulässige, erforderliche und gesetzeskonforme Zusammenarbeit handelt. Die Bestandteile aus der Informationspflicht herauszunehmen ist daher sachfremd.

16.7 "nachteilige Auswirkungen" § 82 (2) E

Die aufgelisteten Bereiche, bei denen „nachteiligen Auswirkungen“ auftreten können, sind zu unbestimmt. Hier gehört eine Definition, ab wann eine Auswirkung nachteilig ist und welche Auswirkungen hinzunehmen sind. Ein Positivkatalog genau beschriebener unerwünschter Auswirkungen würde dem Recht auf Transparenz mehr Geltung verschaffen.

16.8 Betriebs- und Geschäftsgeheimnisse

Ausnahmen zugunsten von Betriebs- und Geschäftsgeheimnissen gehören beschränkt auf *berechtigte* Betriebs- oder Geschäftsgeheimnisse. Die Festlegung, was einem solchen Geheimnis unterliegt, trifft das Unternehmen. Auch diese Entscheidung kann gegen eine Rechtspflicht verstoßen. Zu schützen sind daher nur *berechtigte* Geheimnisse.

17 Statt Ausnahmen, Erweiterung auf Unternehmen im Besitz der öffentlichen Hand

Statt zahlreicher Ausnahmen fordern ***dieDatenschützer*** Rhein Main die Einbeziehung der Transparenzpflicht bzw. des Informationszugangs bei Unternehmen, Vereinen und anderen nichtöffentlichen Stellen, wenn sie

- ganz oder im überwiegenden Eigentum des Landes oder einer Gemeinde, eines Kreises oder eines Gemeindeverbands liegen oder
- dieser nichtöffentlichen Stelle hoheitliche Aufgaben des Landes, einer Gemeinde, eines Kreises oder eines Gemeindeverbands übertragen wurden.

Immerhin darf durch eine „Flucht ins Private“ Rechtspflichten öffentlicher Stellen nicht unterlaufen werden. So wäre ein Betriebs- und Geschäftsgeheimnis dieser Unternehmen unbeachtlich, wenn das entsprechende behördliche Handeln selbst keiner Geheimhaltungspflicht unterliegen würde.

18 Verfahren der niedrigsten Hürde

Es soll das Prinzip gelten, dass Bürger ein Verfahren einhalten müssen, das die niedrigste Hürde - am besten ganz ohne Hürde - für den Zugang zur gewünschten Information darstellt. Der vorgelegte Gesetzesentwurf macht sich derzeit dieses Prinzip noch nicht zu eigen - daher muss er wie folgt nachgebessert werden.

18.1 Antrag bei jedem Bürgeramt möglich, dieses leitet ggf. weiter

Der Gesetzesentwurf legt zwar der Behörde, die sich für nicht zuständig erklärt, die Pflicht auf, den Bürger über die zuständige Behörde zu informieren, vgl. § 85 (4) GE. Niedriger wäre aber die Hürde, wenn der Bürger nicht erneut seinen Antrag stellen muss, sondern die Behörde in der Pflicht ist, den Antrag entgegen zu nehmen und ihn an die zuständige andere Behörde weiterzugeben. Fristen würden dann zugunsten der Bürger bereits zu laufen beginnen und der Aufwand für einen weiteren Antrag wäre nicht erforderlich. Insbesondere sollte bei jedem Bürgeramt der Antrag auf Informationszugang eingereicht werden können; das ist gelebte Bürgernähe.

Der Entwurf sollte überdies mit den folgenden Punkten nachgebessert werden:

18.2 Dateiübermittlung nicht genannt

Die Variante, die Information digital an den Bürger zu übergeben, wenn dieser das wünscht, ist im Gesetzesentwurf nicht vorgesehen. Dabei wäre das die kostengünstigste Form der Bereitstellung, insbesondere bei großen Datenmengen oder Dateien. Möglich ist das als Dateianhang einer E-Mail. Auch das Brennen einer CD-ROM oder einer DVD durch die Behörde vor deren Versendung käme als Variante infrage.

18.3 Elektronische Datenübermittlung geht vor Einsichtsrecht

Die Übermittlung der gewünschten Information in elektronischer Form sollte dem Einsichtsrecht vorgehen. Bei Letzterem muss der Bürger die Behörde aufsuchen, bei Ersterem kann er sich diesen Aufwand sparen. Das Wahlrecht verbleibt beim Bürger.

18.4 Weitestgehende Veröffentlichungen sollen Antragsverfahren unnötig machen

Die Veröffentlichung von Informationen, insbesondere Richtlinien, Dienstanweisungen und anderer standardisierter Vorgänge, erspart aufwendige Antragsverfahren. Gespart werden hierbei Aufwände sowohl der Behörde und als auch der Bürger.

Die Veröffentlichung kann durch Broschüren auf Papier oder in elektronischer Form auf der jeweiligen Homepage des Behördenauftritts im Internet erfolgen.

Die Pflicht zur Veröffentlichung von Informationen kehrt die Holschuld der Bürger in eine Bringschuld der Behörde um. So wird aus einer Informationsfreiheit eine allgemeine Transparenz von Behördentätigkeit, vergleiche oben Ziffer 14.

18.5 Formloser Antrag

Um niedrige Hürden für die Bürger zu erreichen, sollte jeder Antrag formlos gestellt werden können. Ungenauigkeiten, wie z.B. durch eine unpräzise Beschreibung der gewünschten Information, können durch eine Beratungspflicht der Behörde ausgeglichen werden. Es ist eben nicht der Bürger, der sich in Behördenstrukturen auskennen muss, sondern die Behördenmitarbeiter haben hier größere Einsichten, die sie so in den Dienst der Bürger stellen können.

18.6 Beratungspflicht der angefragten Behörde

Die erwähnte Beratungspflicht der Behörde umfasst

- eine Hinweispflicht über bereits bestehende und einschlägige Veröffentlichung,
- den Inhalt des Antrags, der am nächsten zu dem Informationswunsch des Bürgers liegt,
- die geeignete Form, sofern hier tatsächlich bei grundsätzlicher Formfreiheit Anforderungen zu erfüllen sind und
- die zu erwartenden Kosten zu jedem Zeitpunkt der Bearbeitung des Antragsverfahrens.

Die Verletzung dieser Pflichten sollte öffentlich rechtliche Schadenersatzansprüche auslösen. Verzögerung, die hier entstanden sind und ursächlich zu Verzögerungen in anderen behördlichen Verfahren des Bürgers geführt haben, sollen in diesen Verfahren Fristverletzungen heilen.

Kosten, über die der Bürger nicht informiert war, dürfen nicht berechnet werden. Der Nachweis liegt bei der Behörde.

18.7 Anonymer Antrag

Bei einer Internet-Verfügbarkeit von Informationen kennt die Behörde den Interessenten an der Information nicht. Im individuellen Antragsverfahren könnte korrespondierend ein anonymer Antrag zulässig sein. Die Erhebung von personenbezogenen Bürgerdaten ist dann nicht erforderlich, wenn den Zugang zur Information ohnehin *jedermann* zugänglich sein soll. Für den Antragssteller würde auch das die Hürde, von seinem Recht auf Informationszugang Gebrauch zu machen, deutlich senken.

18.8 Schnelle Beauskunftung, 14 Tage, 1 Monat

Ist die beantragte Information nicht oder noch nicht öffentlich zugänglich, ist ein Antragsverfahren unumgänglich. Hier soll es Fristen geben, die die Behörden – die einzigen, die über die erforderlichen Ressourcen verfügen, einhalten müssen.

Bei allen Regelfällen ist eine Frist von 14 Tagen einzuhalten.

Nur wenn die Information in seltenen Fällen in einem komplexen Verfahren, z.B. bei

mehreren Behörden zusammen getragen werden muss oder z.B. ein aufwendiger Vorgang über einen Einzelfall erst noch geeignet anonymisiert werden muss, soll die Behörde 1 Monat Zeit bekommen. Sie wird dann die entstandene Verzögerung nachvollziehbar begründen müssen.

Aufwendige Verfahren organisiert die Antragsbehörde, nicht der Betroffene.

Wichtig dabei ist, dass Behörden mit ausreichend Ressourcen auszustatten sind. Sie dienen Bürgern, die diese Informationen in anderen Zusammenhängen benötigen und dabei ihrerseits Fristen einzuhalten haben.

18.9 Vollständigkeit geht vor Kostengünstigkeit

Da im Zentrum einer Regelung zur Transparenz die Information liegt, die an den Bürger geht, soll der Grundsatz gelten, dass eine kostengünstigere Variante, die auf einen Teil der zur Verfügung zustellenden Information verzichtet, nachrangig gehandhabt wird zu der Variante, die Vollständigkeit dieser Information gewährt. Der Bürger, der laufend über die Kostenentwicklung informiert wird, kann dann selbst eingreifen und mit dieser Wahlfreiheit gegebenenfalls auf einen Teilaspekt seines Informationbegehrens verzichten. Für die Behörde soll gelten, dass die Vollständigkeit die höhere Priorität besitzt.

18.10 Ehe ein Dokument in Gänze zurückgehalten wird, soll mit Schwärzungen gearbeitet werden

Bei diesem Ansatz wird das gleiche Ziel verfolgt. Es ist die Variante zu wählen, bei der überhaupt noch Informationen bereit gestellt werden, wenn es gute Ausnahmegründe gibt, einen Teil der Unterlagen nicht zur Verfügung zu stellen.

19 Kostenfreiheit

Der Kernpunkt der „niedrigsten Hürde“ sind Regelungen, die beim Verfahren zum Informationszugang den Antragssteller von einer Kostenbelastung ganz oder weitestgehend frei stellt. Daher sollte der Grundsatz gelten, dass der Zugang zu Informationen kostenfrei zur Verfügung zu stellen ist. Begründete, genau umrissene und möglichst seltene Ausnahmen können diesen Grundsatz begleiten.

Der Entwurf selbst regelt in § 88 (1) GE: „*Die Gebühren sind […] so zu bemessen, dass die antragstellenden Personen dadurch nicht von der Geltendmachung ihres Informationsan-spruchs […] abgehalten werden.“*

Allerdings legt er nahe, dass die antragstellende Person ihre finanzielle Situation offen legen muss, um diesen Punkt zu prüfen. Ausgehend davon, dass es sich bei Transparenz nicht um einen Luxus, sondern um einen Vorgang der Daseinsvorsorge handelt, darf die Prüfung über den Informationszugang nicht an eine Bedürftigkeitsprüfung der antragstellenden Person geknüpft werden. Vielmehr ist er

bedingungslos zu gewähren. Ganz abgesehen davon, dass diese Prüfung der Bedürftigkeit wiederum –perfider Weise – höchst kostenaufwendig wäre.

19.1 Notwendige Kosten

Der G-Entwurf regelt in § 88 (1): „Die Erteilung mündlicher und einfacher schriftlicher Auskünfte sowie die Einsichtnahme in Dateien und Akten vor Ort […] sind kostenfrei."

Dennoch verweist der G-Entwurf auf eine Gebührenordnung, vgl. § 88 (1) GE, nach der Kosten von bis zu 600,-- € in nur 1 Antragsverfahren anfallen können. Das ist der Weg der maximalen Hürde, statt der der niedrigsten.

Ein Gebührenkonzept könnte wie folgt aussehen:

- die ersten 25,-- Euro sind frei und daher vom Gesamtaufwand abzuziehen,
- eine Kopie auf Papier kostet höchsten 6 Euro-Cent – der § 88 (1) des G-Entwurfs legt 10 Euro-Cent nahe; hier ist gerade nicht eine kaufmännische Vollkostenrechnung zugrunde zu legen, sondern nur die tatsächlich entstandenen Materialkosten,
- die Gesamtkosten für die beantragende Person dürfen 50,-- Euro nicht übersteigen; auch für juristische Personen sollte diese Grenze nicht wesentlich höher liegen und
- die elektronische Überlassung ist immer kostenfrei.

Zu jedem Zeitpunkt des Verfahrens müssen die zu erwartenden Kosten der antragstellenenden Person transparent sein. Dies bedeutet auch, dass je geringer die durch das abschließende Gesetz geregelten Gesamtkosten werden können, umso geringer ist auch der Aufwand der Behörde, diese Transparenz zu gewährleisten.

19.2 Die Kostenentscheidung

Kommt es zu Kosten für die antragsstellende Person, ist diese Kostenentscheidung gesondert zu begründen. Außerdem soll sie zugänglich sein für eigene Rechtsbehelfe, die den Informationszugang selbst und dessen Verfahren unberührt lassen.

20 Gesetzeseinführung muss begleitet werden von einer Aufklärungskampagne über die Rechte der BürgerInnen

Nach den bisherigen Erfahrungen gab es immer wieder einmal eine kommunale Informationsfreiheitssatzung und vergleichbare Regelungen. Sie wurden wieder abgeschafft mit dem Argument, dass Nachfragen zum Informationszugang praktisch kaum vorkamen. Dieser Umsetzungsdefizit war aber in jedem Fall der Tatsache geschuldet, die die berechtigten Bürger ihre Rechte nicht kannten. Überall dort

wurden auf Aufklärungskampagnen verzichtet und auch sonst kein Versuch gestartet, öffentlich über diese neuen Rechte aufzuklären.

Der vorgelegte Entwurf sieht eine Pflicht zur Aufklärung der Bürger beim neuen Hessischen Informationsfreiheitsbeauftragten, geregelt in § 89 GE, nicht vor. Der Aufgabenkatalog sollte insofern erweitert werden.

21 Resümee Informationsfreiheit & Transparenz

Der vorgelegte Entwurf ist ein Beispiel dafür, dass Bündnispartner aus Fraktionsdisziplin ein Informationsfreiheitsgesetz formulieren und vorlegen, ohne Informationsfreiheit oder Transparenz tatsächlich anzustreben. Es wäre nach dem aktuellen Ranking das schlechteste Informationsfreiheitsgesetz in Deutschland.

Es ist müßig zu diskutieren, welcher Schaden größer wäre: entweder das Gesetz in diesem Abschnitt zu verabschieden, damit es überhaupt einen Recht auf Informationszugang gibt, oder diesen Abschnitt herauszustreichen, umweiter auf ein besseres Gesetz zu warten. Tatsache ist, dass dieser Entwurf die Vereinbarung aus dem Koalitionsvertrag der Hessischen Landesregierung nach einem Informationsfreiheitsgesetz gerade nicht erfüllt.

Mit dem vorgelegten Entwurf wird für Hessen die historische Chance verpasst, ein Transparenzgesetz vorzulegen, dass ein Schritt weg vom Obrigkeitsstaat hin zu einem demokratischen Gemeinwesen führt, in dem Bürger in Behörden, die über andere Bürger hoheitlich entscheiden, und dies in maximaler Offenheit geschieht. Diese Offenheit nähme den Behörden nicht ihre Entscheidungsbefugnis, sondern würde sie darin unterstützen, weil die betroffenen Bürger sich sehr viel sorgfältiger auf berechtigte Erwartungen der Behörden vorbereiten könnten.

MEHR DEMOKRATIE

Mehr Demokratie e.V.
Landesverband Hessen
c/o Matthias Klarebach
Wintergasse 15
35321 Laubach

07.03.2018

Stellungnahme

zur öffentlichen mündlichen Anhörung des Innenausschusses und des Unterausschusses Datenschutz betreffend den Gesetzesentwurf der Fraktionen der CDU und BÜNDNIS90/DIE GRÜNEN für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit

- Drucksache 19/5728 -

Autor:
Felix Hoffmann, Mitarbeiter
0152-327 095 38
Felix.Hoffmann@mehr-demokratie.de

1. Einleitung

Für die Möglichkeit der Stellungnahme zum vorliegenden Gesetzentwurf möchten wir uns herzlich bedanken. Die nachfolgenden Ausführungen beziehen sich auf den Vierten Teil des Gesetzes und damit auf die vorgesehenen Regelungen zur Informationsfreiheit.

Im Bereich der Informationsfreiheit und Transparenz ist Deutschland seit je her Nachzügler. Blicken andere – insbesondere die skandinavischen – Länder schon seit vielen Jahrzehnten auf eine gesetzlich verbriefte Informationsfreiheit zurück, so sind derartige Rechte der Bürgerinnen und Bürger in der Bundesrepublik eine vergleichsweise junge Erscheinung. Mit Brandenburg führte 1998 das erste Bundesland einen gesetzlich geregelten Zugang zu Verwaltungsinformationen ein (im Bereich des Umweltinformationsrechts bestehen Bundes- und Landesgesetze schon länger aufgrund EU-rechtlicher Verpflichtung). Bis heute erkannten elf weitere Bundesländer den Nutzen einer transparenten Verwaltungsführung. Drei Bundesländer entwickelten bestehende Informationszugangsgesetze weiter hin zu Transparenzgesetzen, die eine proaktive Veröffentlichung von Informationen vorsehen. Darunter verabschiedete mit Rheinland-Pfalz 2016 auch erstmals ein Flächenland ein solches Gesetz.

Dagegen verzichten vier Bundesländer noch immer auf ein Informationsfreiheits- oder Transparenzgesetz. Neben Bayern, Niedersachsen und Sachsen hinkt Hessen hinsichtlich einer solchen Regelung hinterher (vgl. Transparenzranking 2017, Mehr Demokratie e.V.). Der vorliegende Gesetzentwurf versucht, hier Abhilfe zu schaffen. Als im Datenschutzgesetz enthaltenes Informationsfreiheitsgesetz bleibt der Entwurf jedoch weit hinter dem im Koalitionsvertrag festgeschriebenen Anspruch, Verwaltungshandeln offen und transparent zu gestalten, zurück. Auch mit Blick auf die bislang in den politischen Prozess eingebrachten Gesetzentwürfe[1] mutet der vorliegende Entwurf mehr als bescheiden an. Und das, obwohl Informationsfreiheit zahlreiche und wertvolle Vorteile für das Gemeinwesen mit sich bringt.

Demokratie lebt davon, dass sich informierte Menschen in Debatten einmischen und fundierte Entscheidungen bei Wahlen und Abstimmungen treffen. Einzelne Zugangsrechte wie nach dem Hessischen Umweltinformationsgesetz (HUIG) oder nach dem Verbraucherinformationsgesetz (VIG) können genauso wenig ein Ersatz für ein allgemeines Informationszugangsrecht sein, wie eine partiell freiwillige Veröffentlichung von Informationen. Bürgerinnen und Bürger sind keine lästigen Bittsteller oder sollten es nicht sein, sie sind der Kern der Demokratie. Transparentes staatliches Handeln ist dabei die Voraussetzung für eine aktive politische Teilhabe der Staatsbürgerinnen und -bürger: Nur wer von

[1] Drs. 18/7200: Gesetzentwurf der SPD-Fraktion für ein Hessisches Transparenzgesetz (HessTG); Drs. 19/2341: Gesetzentwurf der SPD-Fraktion für ein Hessisches Transparenzgesetz (HessTG).

einem Vorgang weiß, kann sich aktiv in politische Prozesse einbringen und aus dem Instrumentarium politischer Partizipationsmöglichkeiten schöpfen. Informationsfreiheit stellt folglich einerseits die *Grundlage politischer Teilhabe*, andererseits das *Fundament einer demokratischen Meinungsbildung* dar. Ferner wird durch die Nachvollziehbarkeit politischer Entscheidungen Akzeptanz und Vertrauen geschaffen, die in Zeiten von Fake News, Postfaktismus und schwindendem Vertrauen in staatliche Institutionen unabdingbare Voraussetzungen für die Stärkung der Demokratie darstellen. Andererseits steckt in Transparenz und Open Data ein enormes wirtschaftliches Potential, wie jüngere Studien[2] konstatieren.

Als Treibstoff der Demokratie bietet Informationsfreiheit die Möglichkeit, die Beziehung zwischen Bürgern und Verwaltung neu zu justieren und mit dem Kulturwandel der Verwaltung, weg vom Amtsgeheimnis hin zum Grundsatz der Transparenz, den Herausforderungen der Digitalisierung zu begegnen und Chancen zur Demokratisierung wahrzunehmen.

2. Zum Gesetz im Einzelnen

Zu § 80 - Anspruch auf Informationszugang

In ***Absatz 1*** wird ein allgemeines Auskunftsrecht formuliert. Wie der Zugang zu Informationen de facto aussehen kann, wird dabei jedoch nicht weiter konkretisiert. Zwar führt § 88 die Einsichtnahme in Dateien und Akten vor Ort auf und kann damit als Argument für ein Recht auf Akteneinsicht dienen, dennoch besteht eine Rechtsunsicherheit, die durch klare und umfassende Gesetzesvorschriften vermieden werden könnte. Eine einfache Auskunft ist nicht mit einer direkten Akteneinsicht oder dem Recht auf Kopien der Akten zu vergleichen, der Informationsgehalt variiert erheblich. Ferner ist aus Gründen der Bürgerfreundlichkeit eine konkrete Benennung der Möglichkeiten des Informationszugangs angebracht, wie sie sich auch in den Gesetzen anderer Bundesländer finden lässt (Vgl. bspw. § 5 Abs. 1 Satz 1 IZGH S-H; § 12 Abs. 1 Satz 1 LTranspG RLP).

Zu § 81 - Anwendungsbereich

Eine große Lücke wird durch die Beschränkung der auskunftspflichtigen Bereiche aufgerissen. Vom Anspruch auf Informationszugang sind öffentliche Stellen der Gemeinden und Landkreise nach ***Absatz 1, Ziffer 6*** nur erfasst, sofern diese entsprechende Regelungen in eigenständigen Informationsfreiheits-

[2] Konrad Adenauer Stiftung 2016: „Open Data. The Benefits. Das volkswirtschaftliche Potential für Deutschland". http://www.kas.de/wf/doc/kas_44906-544-1-30.pdf?160418125028.

oder Transparenzsatzungen bestimmen. Zum einen bestehen schon gravierende rechtliche Bedenken dagegen, die Informationsfreiheit bei Gemeinden und Kreisen in ihrer Funktion als mittelbare Landesverwaltung von einer entsprechenden Satzungsregelung abhängig zu machen und damit eine uneinheitliche Umsetzung von Bundes- und Landesgesetzen zuzulassen. Zum anderen bleibt der vorliegende Entwurf weit hinter dem im Koalitionsvertrag formulierten Anspruch zurück, Verwaltungshandeln offen und transparent zu gestalten.[3] Informationsbegehren treten vor allem auf der kommunalen Ebene auf, wie die in der jüngsten Gesetzesfolgenabschätzung des Niedersächsischen Informationszugangsgesetz (NIZG) vorgenommene empirische Analyse bestehender Informationsfreiheitsgesetze anderer Flächenländer bestätigt und auch schon in der ersten Lesung des vorliegenden Gesetzentwurfs von den Regierungsfraktionen angemerkt wurde.[4] Überträgt man die vorgenommene Gesetzesfolgenabschätzung auf Hessen, ergeben sich daraus die nachfolgenden Zahlen und die Erkenntnis, dass nicht von einer übermäßigen Belastung der Kommunen auszugehen ist.

Abbildung 1: Schätzung auf Grundlage der Angaben der aufgeführten Länder

Land	**Anträge im Jahr (ggf. Durchschnitt)**	**Bevölkerung 2015**	**Auf Hessen übertragen (Bevölkerung 2015 6 140 000[5])**
Brandenburg	186	2 484 800	459
Schleswig-Holstein	1050	2 858 700	2 255
Nordrhein-Westfalen	1789	17 865 500	615
Mecklenburg-Vorpommern	179	1 612 400	682
Thüringen	209	2 170 700	591
Sachsen-Anhalt	97	2 245 500	265
Rheinland-Pfalz	553	4 052 800	838
Durchschnitt			815

[3] CDU Hessen/BÜNDIS90/DIEGRÜNEN Hessen: Verlässlich gestalten – Perspektiven eröffnen, 2013, S.104.
[4] Vgl. Entwurf des Gesetzes über den Zugang zu Informationen in Niedersachsen, S. 18-19 (Drs. 17/8004).
[5] Die Bevölkerungszahl basiert auf Angaben des Statistischen Landesamts Hessen und wurde auf eine Zahl gerundet, die zwischen der Bevölkerungszahl vom 01.01.2015 (6 093 888) und vom 31.01.2015 (6 176 172) liegt (Quelle: https://statistik.hessen.de/sites/statistik.hessen.de/files/AI2_AII_AIII_AV_15_2hj.pdf, S. 45).

Aufgrund der angegebenen Bearbeitungsdauer von Informationsanfragen in anderen Ländern kann von durchschnittlich vier Stunden pro Antrag ausgegangen werden. Mit der in *Abbildung 1* dargestellten Schätzung würde ein Bearbeitungsaufwand von rund 3 300 Arbeitsstunden anfallen. Da Informationen vor allem auf kommunaler Ebene begehrt werden, wird sich bei einem kommunalen Anteil von 80% der Arbeitsaufwand in Kommunen auf ca. 2 800 Stunden beziffern. Diese verteilen sich auf 21 Landkreise, 191 Städte sowie 232 Gemeinden und verursachen damit einen eher geringfügigen Aufwand, der keinen zusätzlichen Personalbedarf nötig macht – wie die langjährigen Erfahrungen anderer Bundesländer zeigen. Die Annahme, dass durch ein umfassendes Informationsfreiheitsgesetz kommunale Behörden übermäßig belastet werden, findet keinerlei Stütze in der Wirklichkeit.

In ***Ziffer 1 bis 5*** sind weitere Bereichsausnahmen bestimmt, die in Teilen berechtigt sind. Diffuse Formulierungen wie „der Bereich der Abgeordneten- und Fraktionsangelegenheiten“ könnten durch prägnante Konkretisierungen abgelöst werden. ***Ziffer 5*** ist kritisch zu bewerten, ist doch gerade bei der Drittmittelforschung Transparenz angebracht, die der Freiheit wissenschaftlicher Forschung zugutekommt. Zu diesem Ergebnis kommt auch das Grundsatzpapier der Informationsfreiheitsbeauftragten der Länder, die auf Basis der bisherigen Erfahrungen Empfehlungen abgegeben haben.[6] Eine Orientierung an diesen Empfehlungen ist aus Sicht von Mehr Demokratie sinnvoll und für ein gut ausgestaltetes Informationsfreiheitsgesetz grundlegend.

In ***Absatz 2*** werden pauschale Bereichsausnahmen aufgeführt, die jegliche Informationen der genannten Behörden vom Informationsanspruch prinzipiell ausschließen. Die öffentliche Kontrolle dieser Institutionen muss jedoch gewährleistet sein. So sind beispielsweise die Polizeibehörden in allen Bundesländern, die über ein Informationsfreiheitsgesetz verfügen, vom Informationszugang erfasst. Warum Hessen gerade hier eine Bereichsausnahme vornehmen möchte, erschließt sich uns nicht. Gleiches gilt auch für den Verfassungsschutz, wie auch vom Grundlagenpapier der Informationsfreiheitsbeauftragten hervorgehoben wird. Vielmehr sollten Bereichsausnahmen von der Sensitivität einer Information abhängig gemacht werden und nicht von der Behörde, bei der die Unterlagen vorzufinden sind. Selbstverständlich können Informationen, die speziellen Schutzerfordernissen unterliegen, vom Informationszugangsanspruch ausgenommen werden, was jedoch bereits durch die Regelungen zum Schutz besonderer öffentlicher und privater Belange in ***§ 82*** erfolgt ist.

[6] https://www.datenschutz.rlp.de/fileadmin/lfdi/Konferenzdokumente/Informationsfreiheit/Grundsatzpositionen_IF_20170929.pdf

Zu § 82 - Schutz besonderer öffentlicher und privater Belange

Die in ***Ziffern 1 bis 3*** genannten Ausnahmen sind auch nach unserer Auffassung berechtigt.

In ***Ziffer 4*** sollten Betriebs- oder Geschäftsgeheimnissen um eine Klausel zur Abwägung des öffentlichen Interesses an einer Information ergänzt und damit nicht unter einen absoluten Schutz gestellt werden. Ohne einen solchen Abwägungsvorbehalt legt der Gesetzgeber die Reichweite des Informationszugangs in die Hände betroffener Unternehmen, sodass eine willentliche Gefahr der Behinderung des Informationszugangs durch Private offenkundig ist (vgl. Kloepfer 2011[7], S. 75). Entsprechende Abwägungsvorbehalte wirken dem entgegen und gelten mittlerweile als internationale Standards. Jene lassen sich auch in den Ländern der Bundesrepublik (Berlin; Brandenburg; Bremen; Hamburg; Nordrhein-Westfalen; Rheinland-Pfalz und Schleswig-Holstein) wie auch im Hessischen Umweltinformationsgesetz (§ 8 Abs. 1 HUIG) finden. Es besteht kein Anlass, hinter die bisher gut gewählten Vorkehrungen bei Umweltinformationen in einem breiter angelegten Informationsfreiheitsgesetz zurückzufallen. Eine Minimierung der grundrechtlich zugesicherten Betriebs- und Geschäftsgeheimnisse ist dabei ohnehin nicht zu erwarten, wie sich in der bisherigen Praxis bestätigt. Überdies empfiehlt auch der Evaluationsbericht des Bundes-IFG, eine entsprechende Abwägungsklausel bei einer Novellierung einzuführen und diesen Missstand zu beseitigen.

Ziffer 5 benennt ein rein wirtschaftliches Interesse an einer Information als Ausnahmetatbestand. Eine solche Regelung findet sich in keinem anderen Informationsfreiheits- oder Transparenzgesetz der Bundesrepublik. Der Gesetzgeber sollte vielmehr das Potential von „Open Data“ erkennen und deren Nutzung für wirtschaftliche Innovationen ermöglichen, statt diese durch diesen Ausnahmetatbestand zu blockieren. Zudem ist fraglich, wie die ökonomische Intention eines Informationsgesuchs erkannt werden soll und wer aufgrund welcher Maßstäbe die Behauptung eines nicht-wirtschaftlichen Beweggrundes (z.B. bei journalistischen Anfragen) ablehnen will. Diese Regelung sollte, weil unnötig und unpraktikabel, aus dem vorliegenden Gesetzentwurf gestrichen werden.

Zu § 83 - Schutz personenbezogener Daten

Die Regelungen zum personenbezogenen Datenschutz sollten – wie auch im Falle der Betriebs- und Geschäftsgeheimnisse – um einen allgemeinen Abwägungstatbestand ergänzt werden. Informationen

[7] Informationsfreiheitsgesetz und Schutz von Betriebs- und Geschäftsgeheimnissen. Rechtsgutachten im Auftrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, erstattet von Prof. Dr. iur. Michael Kloeper:
http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/GutachtenIFGKloepfer.pdf%3F__blob%3DpublicationFile.

sollten trotz personenbezogener Daten zugänglich gemacht werden können, wenn das öffentliche Interesse gegenüber dem Geheimhaltungsinteresse des Dritten erheblich überwiegt.

Zu §84 - Schutz behördlicher Entscheidungsprozesse

Auch das Landesparlament sollte Verwaltungshandeln offen und transparent gestalten, sofern und solange nicht direkt der behördliche Entscheidungsprozess betroffen ist. Dies wird durch ***Absatz 1*** erfüllt. Eine Ergänzung um einen Abwägungsvorbehalt, wie ihn etwa das rheinland-pfälzische Gesetz kennt (§ 15 Abs. 1 Ziffer 1 LTranspG RLP), wäre wünschenswert.

Zu § 85 - Antrag

Absatz 1 regelt die Formerfordernisse des Antrags in umfassender Weise. Begrüßenswert ist, dass ein Antrag auch in elektronischer Form gestellt werden kann. Positiv ist auch die in ***Absatz 2*** festgeschriebene Beratung der informationspflichtigen Stelle, welche die Kommunikationsbeziehung zwischen Verwaltung und Bürger/-innen fair ausgestaltet. So auch ***Absatz 4***. Lediglich die Bekanntgabe der Ablehnung eines Antrags könnte für den Fall einer elektronischen Antragsstellung auf demselben Wege erfolgen, sofern vom Antragsstellenden nichts anderes gewünscht ist.

Zu § 86 - Verfahren bei Beteiligung einer betroffenen Person

Für die Gelegenheit zur Stellungnahme in ***Absatz 1*** sollte eine Frist von zwei Wochen ausreichen. Darüber hinaus sollten Dritte, besonders bei Betriebs- und Geschäftsgeheimnissen, grundsätzlich um die Kennzeichnung von schutzwürdigen Daten gebeten werden. Dies könnte als gesetzliche Pflicht für Private aufgenommen werden und die doppelte Aktenführung deutlich vereinfachen.

Zu § 87 - Entscheidung

Die Fristsetzung zur Entscheidung über den Zugang zur begehrten Information ist wichtig, übt sie doch als Stellschraube einen zentralen Einfluss auf den Verfahrensablauf des Informationszugangs aus. ***Absatz 1*** legt die informationspflichtige Stelle auf eine Frist von einem Monat fest. Diese Regelung bewegt sich in gemäßigten Bahnen und könnte zwar kürzer – und insofern bürgerfreundlicher – gewählt sein, orientiert sich jedoch am Durchschnitt der in den Ländern der Bundesrepublik geltenden Fristen. Die in ***Absatz 2*** festgelegte Frist von drei Monaten bei Beteiligung Dritter könnte kürzer ausfallen. Positiv hervorzuheben ist die schriftliche Bekanntmachung einer Fristverlängerung gegenüber der antragsstellenden Person, wie in ***Absatz 3*** geregelt.

Zu § 88 - Kosten

Mehr Demokratie spricht sich für möglichst niedrige Gebühren und damit für ein auf Bürgerfreundlichkeit bauendes Verfahren aus und fordert dahingehend die Einführung eines Kostendeckels in das Informationszugangsverfahren.

Gebühren wirken sich in der Praxis häufig restriktiv als erfolgreiche Abschreckung aus. Der Informationszugang darf nicht vom Geldbeutel abhängig sein und Bürger/-innen dürfen nicht durch Gebühren von der Inanspruchnahme des Informationszugangs abgehalten werden. Zwar spricht sich der Gesetzentwurf dafür aus, die Gebühren so zu bemessen, „dass die antragsstellenden Personen dadurch nicht von der Geltendmachung ihres Informationsanspruchs nach § 80, Abs. 1 abgehalten werden“ (***Absatz 1 Satz 4***), zieht jedoch nicht den Mechanismus eines Kostendeckels in Erwägung, der diesem Anliegen wohl am ehesten gerecht werden und den Antragsstellenden eine gewisse Sicherheit geben würde. Nach der Anlage zu § 13 Abs. 9 HDSG (Verwaltungskostenverzeichnis) können sich Gebühren in Höhe von 10 bis 15.000 Euro ergeben. Ein Kostendeckel von maximal 500 Euro wäre hier angebracht, um Antragssteller nicht bereits im Vorfeld von einer Anfrage abzuhalten. Zwar wird ein „Ausfertigungs-, Abschrift- und Kopiekostendeckel“ von 0,10 Euro je Seite festgeschrieben, damit wird jedoch nur ein Minimum an Bürgerfreundlichkeit gewährleistet. Einen übergreifenden Kostendeckel haben die Länder Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt und Schleswig-Holstein sowie das bundesgesetzliche Informationsfreiheitsgesetz gewählt. Die Mehrheit davon regelt einen Kostendeckel von 500 Euro.

Die vorgesehene Missbrauchsgebühr nach ***§ 13 Abs. 10*** sollte in dem vorliegenden Gesetzentwurf gestrichen werden. Ein empirisch begründetes Bedürfnis für eine solche, über die ohnehin mögliche Kostenlast hinausgehende Gebühr ist nicht zu erkennen; eine entsprechende Begründung – etwa mit Erfahrungen im Umweltinformationsrecht oder in anderen Bundesländern – wird im Gesetzentwurf auch nicht gegeben. Die Erhöhung des Gebührenrisikos mit einem diffusen Missbrauchsbegriff trägt dazu bei, Bürgerinnen und Bürger von einem Informationsgesuch abzuhalten.

Zu § 89 - Die oder der Hessische Informationsfreiheitsbeauftragte

Die Wirksamkeit von Informationsfreiheitsgesetzen hängt wesentlich von den Rechten der Informationsfreiheitsbeauftragten und der Ausstattung einer solchen Aufsichtsbehörde ab. Es ist wichtig, diese mit einem allgemeinen Zugangsrecht zu Diensträumen und einem Akteneinsichtsrecht zu versehen. Dies erfolgt in ***Absatz 3 Ziffern 1 und 2.*** Zu vermissen ist jedoch die Möglichkeit von Sanktionen, die der oder die Informationsfreiheitsbeauftrage bei einem Verstoß gegen das geltende Gesetz gegenüber den auskunftspflichtigen Stellen verhängen kann. Eine solche Regelung würde der

Ernsthaftigkeit einer transparenten Verwaltungsführung Ausdruck verleihen und die Kompetenz des Amtes erweitern. Im Gegensatz dazu sieht der vorliegende Gesetzentwurf die Erhebung einer Missbrauchsgebühr in § 13 Abs. 10 gegenüber Bürgerinnen und Bürger vor, die die eigentlichen Adressaten des Gesetzes sind. Hier sollte das Vorzeichen umgekehrt werden und eine Missachtungsgebühr gegenüber informationspflichtigen Behörden eingeführt werden.

Darüber hinaus ist zu bemängeln, dass der oder die Informationsfreiheitsbeauftragte nicht übergreifend für dieses Gesetz und zugleich für den Vollzug des Umweltinformationsgesetzes zuständig sein soll. Es fehlt jede Begründung im vorliegenden Gesetzentwurf, warum der/die Beauftragte in ihrer Ombudsfunktion nicht auch für Anfragen nach dem HUIG verantwortlich ist. Dieses Defizit teilen die Beauftragten in den Ländern (vgl. Grundsatzpositionen der Informationsfreiheitsbeauftragten).

3. Abschlussbemerkungen

Der vorliegende Gesetzentwurf würde zwar den Missstand beseitigen, dass Hessen seinen Bürgerinnen und Bürgern bislang überhaupt kein allgemeines Recht auf Informationszugang gibt. Insgesamt bleibt der Gesetzentwurf jedoch weiter hinter einem bürgerfreundlichen Transparenzanspruch zurück. Er stellt die Hürde eines Antrags, der zeitaufwändigen Bearbeitung und möglicher Gebühren zwischen die Bürger/-innen und die von ihnen begehrten Informationen. Diese Barrieren sollten durch eine zeitgemäße proaktive Veröffentlichung von Informationen aufgelöst werden. Mit dem vorliegenden Gesetzentwurf würde Hessen das deutschlandweit schlechteste Gesetz zu diesem Thema bekommen, wie die Einordnung des Entwurfs im Transparenzranking der Länder aufzeigt.[8]

Es bleibt zu hoffen, dass die bevorstehende Anhörung und das weitere Gesetzgebungsverfahren genutzt werden, um den Informationszugang nach dem Vierten Teil des Gesetzes deutlich zu erweitern und die in der Koalitionsvereinbarung versprochene transparente Gestaltung des Verwaltungshandelns zu verwirklichen.

[8] https://transparenzranking.de/laender/hessen/.

Bundeskriminalamt

Der Datenschutzbeauftragte

POSTANSCHRIFT Bundeskriminalamt • 65173 Wiesbaden

HAUSANSCHRIFT Thaerstraße 11, 65193 Wiesbaden

TEL +49 (0)611 55-0
FAX +49 (0)611 55-45641
BEARBEITET VON Dr. Mentzel, Thomas
E-MAIL DS-Recht@bka.bund.de
AZ ohne
DATUM **06.03.2018**

Herrn
Horst Klee, MdL
Hessischer Landtag
Vorsitzender des Innenausschusses
Schlossplatz 3
65183 Wiesbaden

Per Email an:
u.lindemann@ltg.hessen.de

Öffentliche Anhörung im Hessischen Landtag zum Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit - Drucksache 19/5728

Sehr geehrter Herr Vorsitzender Klee,
sehr geehrte Damen und Herren,

ich bedanke mich für die Möglichkeit, zu dem Gesetzentwurf Stellung zu nehmen!

A) **Einleitung**

Der Entwurf des HDSIG ist auf den Datenschutz bezogen im Wesentlichen dem neuen Bundesdatenschutzgesetz, das am 25. Mai 2018 in Kraft tritt, nachgebildet. Hierfür liegen mir somit noch keine Erfahrungen aus meiner Praxis als behördlicher Datenschutzbeauftragter vor. Ich habe mich in meiner Stellungnahme daher darauf beschränkt, auf einige Einzelaspekte hinzuweisen, die mir im Vergleich des Entwurfs des HDSIG mit dem BDSG-neu aufgefallen sind.

Soweit der Entwurf des HDSIG mit seinem Vierten Teil den Anspruch auf Informationszugang regelt, kann ich auf meine Erfahrungen mit dem Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz-IFG) zurückgreifen. Nach dem Geschäftsverteilungsplan des BKA obliegt mir neben dem Datenschutz auch die Bearbeitung von Anträgen nach dem IFG.

B) Die Reglungen zum Datenschutz

1. Rechtsstellung des behördlichen Datenschutzbeauftragten

Um einen effektiven behördlichen Datenschutz zu gewährleisten, ist es erforderlich, die Stellung des behördlichen Datenschutzbeauftragten gesetzlich so auszugestalten, dass dieser fachlich unabhängig und ohne Sorge der persönlichen Benachteiligung seine Tätigkeit ausüben kann.
Der Regelung des § 6 Abs. 3 S. 2 HDSIG kommt hier zentrale Bedeutung zu. Besonderes begrüßenswert ist, dass danach die oder der Datenschutzbeauftragte der höchsten Leitungsebene nicht nur unmittelbar berichtet, sondern ihr auch unmittelbar untersteht. In der gegenwärtigen Praxis in Bund- und Ländern finden sich immer wieder organisatorische Lösungen, die keine unmittelbare Unterstellung unter die höchste Leitungsebene beinhalten und die Stellung des Datenschutzbeauftragten damit schwächen.

Kritsch hingegen ist die Regelung des § 6 Abs. 3, S. 2 HDSIG zu bewerten, wonach die oder der Datenschutzbeauftragte wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen werden darf. Dies bedeutet im Umkehrschluss, dass sie oder er aus allen anderen Gründen abberufen werden kann, z.B. aus „Personalentwicklungsgründen" oder „aufgrund einer erforderlichen Umorganisation". Dies eröffnet die Möglichkeit, den Datenschutzbeauftragten eben doch wegen seiner Aufgabenerfüllung abzuberufen, indem man andere Gründe dafür anführt. Die Rechtstellung der oder des behördlichen Datenschutzbeauftragten ist damit nach dieser Regelung deutlich schwächer als nach dem aktuellen und dem neuen Bundesdatenschutzgesetz. Gem. § 6 Abs. 4 BDSG-neu ist die Abberufung der oder des Datenschutzbeauftragten nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuches zulässig (Fristlose Kündigung aus wichtigem Grund). Dies bedeutet, solange der Datenschutzbeauftragte sich nicht i.S. des § 626 BGB fehlverhält oder seine Tätigkeit nicht mehr ausüben kann, kann er gegen seinen Willen nicht abberufen werden. Das Hamburgische Datenschutzgesetz beispielsweise geht mit § 10a Abs. 3 sogar noch einen Schritt weiter. Dieser verweist ebenfalls auf den § 626 BGB aber erfordert zudem noch, dass vor der Entscheidung über den Widerruf die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit zu hören ist.

Positiv hingegen ist zu erwähnen, dass § 5 Abs. 1 HDSIG eine oder einen Vertreter des Datenschutzbeauftragten vorsieht. Zwar wäre es auch ohne die gesetzliche Regelung möglich einen Stellvertreter zu benennen, aber nach wohl überwiegender Auffassung in der datenschutzrechtlichen Literatur ermöglicht nur die ausdrückliche gesetzliche Regelung die Vertretung im vollen rechtlichen Umfang.

2. **Rechtsgrundlage für die einwilligungsbasierte Datenverarbeitung**
§ 46 HDSIG ist dem § 51 BDSG-neu nachgebildet und verweist wie dieser auf die Datenverarbeitung auf Einwilligungsbasis nach einer Rechtsvorschrift. Da es dem BDSG-neu wie dem HDSIG – im Gegensatz zu dem noch geltenden BDSG - aber an einer eigenen Rechtsgrundlage für die einwilligungsbasierte Datenverarbeitung fehlt, bedeutet dies, dass alle Gesetze daraufhin überprüft werden müssen, ob diese auch tatsächlich die einwilligungsbasierte Datenverarbeitung vorsehen. Da das gegenwärtige BDSG wie das gegenwärtige Hessische Datenschutzgesetz hierfür eine eigene Rechtsgrundlage besitzen, war es bisher nicht erforderlich, einwilligungsbasierte Datenverarbeitungen in jedem Einzelgesetz zu regeln. Auch wenn die gewählte Regelung aus Sicht einer gesetzlichen Klarstellung und der wirklichen Umsetzung in sich abgeschlossener Spezialgesetze zu begrüßen ist, so birgt sie doch auch die Gefahr der Schaffung ungewollter Lücken.

3. **§ 73 HDSIG Datenübermittlung an Drittländer und an internationale Organisationen**
Soweit Polizeibehörden Dienstverkehr mit anderen Staaten führen, gilt hierfür § 3 Bundeskriminalamtgesetz, wonach dies dem BKA obliegt. Dies sollte zur Klarstellung in Abs. 1 oder zumindest in die Gesetzesbegründung aufgenommen werden.

C) Vierter Teil - Anspruch auf Informationszugang

1. **Bereichsausnahme Polizei**
Mit der Bereichsausnahme für die Polizeibehörden gem. § 80 Abs. 2 Nr. 1 geht der Gesetzentwurf einen anderen Weg als das IFG des Bundes. Aus polizeifachlicher Sicht dürfte dies begrüßt werden. Die Erfahrungen mit dem IFG beim BKA zeigen, dass es häufig ein Spannungsverhältnis zwischen dem Interesse an Informationszugang auf der einen und dem Schutz operativer und polizeitaktischer Informationen auf der anderen Seite gibt. So wurde z.B. nach den Medienberichten über die Beschaffung einer neuen Software für die Quellen-TKÜ („Bundestrojaner") ein IFG-Antrag gestellt, der auf den Zugang zu der sog. Leistungsbeschreibung einer solchen Software gerichtet war. Die ungefilterte Herausgabe und Veröffentlichung hätte jedoch Informationen preisgegeben, die die Einsatzmöglichkeiten deutlich eingeschränkt hätten. So hätten z.B. kommerzielle Anbieter von Virenschutzprogrammen diese Informationen nutzen können, um ihre Produkte darauf einzustellen. Nachdem der Informationszugang versagt wurde, hat sich der Antragsteller an die BfDI gewandt, die die Anforderung stellte, dass in solchen Fällen jeder einzelne Satz des Dokuments daraufhin zu prüfen sei, ob er Informationen enthalte, deren Herausgabe die öffentliche Sicherheit i.S. des § 3 Abs. 1 Nr. 2 IFG gefährden könne.

Andererseits entzieht die Bereichsausnahme für die Polizei diese vollständig dem Transparenzansatz der hinter der Gesetzgebung zur Informationsfreiheit steht. Letztlich ist eine Bereichsausnahme aber eine politische Entscheidung, die durch mich nicht zu bewerten ist.

Die folgenden Aspekte beruhen zwar auf den Erfahrungen eines IFG ohne Bereichsaus-

ausnahme für die Polizei, dürften aber auch auf andere Behörden übertragbar sein.

2. Kosten

Nach der Gebührenverordnung zum IFG des Bundes können Gebühren für Anfragen nach dem IFG bis zu einer Maximalhöhe von 500,- € erhoben werden. Der tatsächliche Verwaltungsaufwand übersteigt dies in vielen Fällen in erheblichem Umfang. Wenn in einer größeren Behörde mehr als eine Fachabteilung betroffen ist, erfordern allein die internen Koordinierungs-, Beteiligungs- und Entscheidungsprozesse die Einbindung einer Vielzahl von Beschäftigten. Bei inhaltlich sensiblen Themen kommt die Einbindung des zuständigen Fachministeriums, in Streitfällen die der BfDI hinzu. Wenn man in betriebswirtschaftlicher Sicht den Personalaufwand einrechnet, kann der Verwaltungsaufwand der betroffenen Behörden durchaus mehrere tausend Euro betragen. Allerdings ist nach der Kommentierung zum IFG des Bundes eine Kostendeckung gerade nicht vorgesehen.

Die Regelung des vorliegenden Gesetzentwurfes, die für die Kosten auf das hessische Verwaltungskostengesetz verweist, ist m.E. deutlich besser geeignet, den durch einen Antrag auf Informationszugang tatsächlich entstehenden Verwaltungsauswand gem. der allgemeinen Kostenregelungen auszugleichen, sollte dies beabsichtigt sein.
Allerdings legt § 88 Abs. 1 S. 1 fest, dass die Erteilung einfacher schriftlicher Auskünfte kostenfrei ist. Diese Regelung stellt, wie die vergleichbare Regelung des IFG, auf das Ergebnis eines Antrages ab, nicht auf den für hierfür erforderlichen Verwaltungsaufwand. Die Herausgabe eines bestimmten z.B. einhundertseitigen Dokuments, wäre nach dieser Regelung ebenso eine einfache schriftliche Auskunft, wie die Versagung der Herausgabe dieses Dokuments. Der Verwaltungsaufwand hierfür könnte gleichwohl ein sehr erheblicher gewesen sein, wenn beispielsweise folgendes erforderlich war:

- Detaillierte Prüfung des gesamten Dokuments auf Versagungsgründe durch den zuständigen Fachbereich;
- Einbeziehung dritter Behörden, die fachlich zugeliefert haben;
- Prüfung des Ergebnisses durch die Behördenhierarchie;
- Befassung der Behördenleitung;
- Überprüfung durch das Justitiariat der Behörde;
- Erneute Vorlage bei der Behördenleitung
- Einbeziehung des zuständigen Fachministeriums;

Die Regelung des § 88 Abs. 1 S. 3 HDSIG, Verbot der prohibitiven Wirkung von Gebühren, entspricht vergleichbaren Regelung im Bund und in anderen Ländern, unterläuft aber den Verweis auf das hessische Verwaltungskostengesetz und insbesondere die dortigen Billigkeitsregelungen. Konkret bedeutet diese Regelung, dass gegen eine Person in schlechten wirtschaftlichen Verhältnissen auch dann nur eine geringe Gebühr festgesetzt werden kann, wenn der tatsächliche Verwaltungsaufwand bei ihrem Antrag mehrere tausend Euro beträgt.
In diesem Zusammenhang ist zu bedenken, dass nach § 80 Abs. 1, S.1 HDSIG, vergleichbar allen anderen deutschen Informationsfreiheitsgesetzen, der Kreis der Antragsberechtigten unbegrenzt ist („Jeder hat (...) Anspruch auf Zugang zu amtlichen Informationen").

Für die entsprechende Regelung des IFG ist anerkannt, dass es damit keine Begrenzung auf deutsche oder EU-Bürger oder z.B. Personen mit Aufenthalt in Deutschland gibt.

In der Gesamtbetrachtung kann dies durchaus zu Haushaltsrisiken und zu einen nicht absehbaren Personalbelastung führen.

3. **Datenschutz und Informationszugang**

Mit § 5 Abs. 4 enthält das IFG eine ausdrückliche Regelung, wonach Namen, Beruf- und Funktionsbezeichnungen, Erreichbarkeiten etc. von Sachbearbeitern nicht geschützt, sondern herauszugeben sind. Dies ist aus datenschutzrechtlicher Sicht insbesondere dann bedenklich, wenn der Sachbearbeitername zu Erfüllung des Informationsanspruchs gar nicht erforderlich ist. Handelt es sich um Unterlagen zu öffentlich kontrovers diskutierten Themen, kann dies dazu führen, dass der Sachbearbeiter für die Unterlagen und darin enthaltenen Entscheidungen quasi persönlich verantwortlich gemacht wird. Im Zeitalter von Internet und sozialen Netzwerken kann dies dazu führen, dass der Sachbearbeiter öffentlich verunglimpft oder sogar persönlich bedroht werden kann. Diese Gefahr besteht insbesondere, wenn auf Informationsfreiheit spezialisierte Internetportale erteilte Auskünfte und Unterlagen veröffentlichen.

Das Recht auf informationelle Selbstbestimmung gilt auch für Behördenbeschäftigte und hat Grundrechtscharakter. Das Recht auf Informationszugang hingegen ist ein einfachgesetzliches Recht, d.h. von niedrigerem Rang. Ein Gesetz, das den Zugang zu amtlichen Informationen gewährt, sollte daher einen ausreichenden Persönlichkeitsschutz für die Beschäftigten der öffentlichen Verwaltung vorsehen.

Der Entwurf des HDSIG enthält anders als das IFG hierzu keine ausdrückliche Regelung, sondern legt mit § 83 lediglich fest, dass der Zugang zu personenbezogenen Daten nur dann zu gewähren ist, wenn eine Übermittlung an eine nicht-öffentliche Stelle zulässig ist. Ob dies so zu interpretieren ist, dass Sachbearbeiternamen geschützt sind, war dem Gesetzentwurf nicht zu entnehmen und sollte (ggf. über die Begründung) präzisiert werden.

An der mündlichen Anhörung am 15.03.2018 werde ich sehr gerne teilnehmen und stehe dort für Ihre Fragen zur Verfügung.

Mit freundlichen Grüßen

Dr. Thomas Mentzel,
Leitender Kriminaldirektor

HESSISCHER STÄDTETAG

Hessischer Städtetag · Frankfurter Straße 2 · 65189 Wiesbaden
Der Vorsitzende des Innenausschusses
Herrn
Horst Klee MdL
c/o Hessischer Landtag
Postfach 32 40
65022 Wiesbaden

Gesetzesentwurf für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie(EU) Nr. 2016/680 und zur Informationsfreiheit

Ihre Nachricht vom:
21.12.2017

Ihr Zeichen:
I A 2.1

Unser Zeichen:
TA 042.5 Pf/Zi

Durchwahl:
0611/1702-32

E-Mail:
pflug@hess-staedtetag.de

Datum:
08.03.2018

Stellungnahme-Nr.:
029-2018

Sehr geehrte Damen und Herren,

zunächst möchten wir uns für die Gelegenheit zur Stellungnahme bedanken.
Im Wesentlichen stimmen wir dem Gesetzentwurf zu.
Insbesondere befürworten wir den neuen § 36 Abs. 2 HDSIG, mit dem von der Öffnungsklausel des Art. 83 Abs. 7 EU-DSGVO Gebrauch gemacht und die Verfolgung und Ahndung von Ordnungswidrigkeiten gegen Behörden und andere öffentliche Stellen i.S.d. § 2 Abs. 1 S.1HDSIG ausgeschlossen wird.
Kritisch sehen wir allerdings den neu eingefügten Anspruch auf Informationszugang im vierten Teil des HDSIG.
Dies insbesondere im Hinblick auf den enormen zusätzlichen sachlichen und personellen Aufwand, der bei den Städten durch einen solchen allgemeinen Anspruch auf Informationszugang hervorgerufen würde. Dennoch wird die in diesem Zusammenhang immerhin eingeräumte Entscheidungsmöglichkeit in § 81 Abs. 1 Nr. 6, wonach die entsprechenden

Verband der kreisfreien und kreisangehörigen Städte im Lande Hessen

Frankfurter Straße 2
65189 Wiesbaden
Telefon: 0611/1702-0
Telefax: 0611/1702-17

posteingang@hess-staedtetag.de
www.hess-staedtetag.de

Nassauische Sparkasse Wiesbaden
BIC: NASSDE55
IBAN: DE79 5105 0015 0100 0727 77

Vorschriften nur anwendbar sind, soweit durch Satzung ausdrücklich bestimmt, begrüßt. Es darf jedoch nicht übersehen werden, dass allein die gesetzlich verankerte Möglichkeit zu einer gewissen Erwartungshaltung und in einem weiteren Schritt zu einer Ausübung von Druck aus der Bürgerschaft den Städten gegenüber führen kann. Dies lässt befürchten, dass damit letztlich ein faktischer Zwang entsteht, die Vorschriften über den Anspruch auf Informationszugang durch Satzung für anwendbar zu erklären. Um dies zu vermeiden, sollten aus unserer Sicht die Behörden und sonstige öffentliche Stellen der Gemeinden sowie deren Vereinigungen nicht in den Anwendungsbereich des vierten Teils des HDSIG fallen. § 81 Abs. 1 Nr. 6 HDSIG sollte daher u. E. gestrichen werden.

Mit freundlichen Grüßen

Stephan Gieseler
Geschäftsführender Direktor

Deutsche Gesellschaft für Informationsfreiheit

Deutsche Gesellschaft für Informationsfreiheit e.V.
Ludwig-Richter-Str.19 | 16547 Birkenwerder

Birkenwerder, den 7. März 2017

Stellungnahme

zum Gesetzentwurf der Fraktion der CDU und BÜNDNIS 90/ DIE GRÜNEN für ein Hessisches Datenschutz und Informationsfreiheitsgesetz (HDSIG)

Die Deutsche Gesellschaft für Informationsfreiheit hat sich bereits in der 16. Wahlperiode (Gesetzentwurf der Fraktion Bündnis 90/Die Grünen, Lt-Drs. 16/5913) und in der 18. Wahlperiode an Beratungen zu einem Landesinformationsfreiheitsgesetz gutachterlich beteiligt. Die anliegende Stellungnahme nimmt im wesentlichen Grundgedanken zu Informationsfreiheit und Transparenz auf, die in den bereits erfolgten Anhörungen vorgetragen wurden.

Zum Vierten Teil des Hessischen Datenschutz und Informationsfreiheitsgesetzes (HDSIG) nehme ich für die Deutsche Gesellschaft für Informationsfreiheit wie folgt Stellung:

1. Allgemeines

Der vorliegende Gesetzentwurf der Fraktion der CDU und BÜNDNIS 90/ DIE GRÜNEN für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit enthält in Artikel 1 den Entwurf eines Hessischen Datenschutz und Informationsfreiheitsgesetzes (HDSIG), der wiederum als „Vierter Teil" Regelungen zur Informationsfreiheit enthält.

Den Gesetzentwurf zeichnet aus, dass die Regelungen zum Informationszugang sich im Ergebnis auf eine partiell eng begrenzte Ergänzung des Landesdatenschutzge-

Dr. Sven Berger
Vorsitzender
Ludwig-Richter-Straße 19
16547 Birkenwerder

Telefon: 030/227-53921
Fax: 03221/1326 795
E-Mail: berger@dgif.de
Internet: www.dgif.de

Bankverbindung
Berliner Volksbank
Kto-Nr 7415182001
BLZ 10090000

Durch Freistellungsbescheid des Finanzamtes Oranienburg vom 15.08.2017 (053/142/01754) als gemeinnützig im Sinne der §§ 51 ff AO anerkannt.

setzes beschränken.

Bedauerlich ist, dass an einer getrennten Kodifikation des allgemeinen Informationszugangsrechts auf Landesebene festgehalten wird und damit die Unübersichtlichkeit auf dem Gebiet der Informationszugangsregelungen noch verstärkt wird. Mit dem Hessischen Umweltinformationsgesetz (HUIG), dem Verbraucherinformationsgesetz (VIG), dem Agrar- und Fischereifonds-Informationen-Gesetz (AFIG) und mit dem Hessischen Vermessungs- und Geoinformationsgesetzes (HVGG) wird es dann vier spezialgesetzliche Informationszugangsregelungen für die hessischen Landesbehörden geben. Hier nun ein fünftes Gesetz anzufügen erscheint nicht sinnvoll. Der Landesgesetzgeber sollte der Regelungsvielfalt entgegentreten indem er die Beschränkung des bewährten hessischen Umweltinformationsgesetzes auf Umweltinformationen aufhebt und es damit zu einem modernen und einheitlichen Informationszugangsgesetz unter Einschluss der Umweltinformationen macht.

Es wird auch offensichtlich die Chance nicht genutzt, ein modernes Transparenzgesetz zu schaffen, dass durch die Statuierung von Veröffentlichungspflichten einen zeitgemäßen, barrierefreien, bürokratiearmen und kostengünstigen Zugang zu ausgewählten amtlichen Informationen eröffnet.

Der Gesetzentwurf ist offenkundig ein schwer errungener Kompromiss zwischen den Regierungsfraktionen, die auf diesem Politikfeld zu weit auseinander sind, um sich auf einen kohärenten und zukunftsweisenden Gesetzentwurf einigen zu können. So lässt sich auch erklären, dass hier die Einbringung des Gesetzentwurfs durch die Landtagsfraktionen gewählt wurde, obwohl der komplexe Gesamtgesetzentwurf mit Sicherheit vom Landesinnenministerium erarbeitet und im Ressortkreis ausführlich, und im Ergebnis auch sicher sehr streitig, abgestimmt wurde.

Der Gesetzentwurf ist auch nicht hinreichend begründet. Die Vielzahl unbestimmter Rechtsbegriffe bedürften dringend einer ausführlicheren konkretisierenden Erläuterung in der Gesetzesbegründung.

Im Ergebnis handelt es sich um eine handwerklich nicht immer gelungenen Gesetzentwurf, mit dem die Chance vergeben wird, die hessische Verwaltung auf allen Ebenen transparenter, moderner und im Ergebnis auch bürgerfreundlicher zu machen.

2. Zu den Regelungen

2.1 Zum Anwendungsbereich (§ 81 HDSIG)

Die Vorschrift scheint den üblichen Regelungen zum Kreis der Anspruchsberechtigten zu den verpflichteten Stellen und verweist auf „öffentliche Stellen" als auskunftsverpflichtet nach dem Gesetz. Ausweislich der Gesetzesbegründung soll sich der Begriff der öffentlichen Stelle nach § 2 Abs. 1-3 HDSIG richten.

Im Ergebnis entzieht § 2 Abs. 2 HDSIG öffentliche Stellen des Landes, der Gemeinden und Landkreise dem Anwendungsbereich des Gesetzes und damit auch den Informationszugangsregelungen, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Diese Regelung zeichnet sich nicht durch Normenklarheit aus.

Der Anwendungsbereich der Informationszugangsvorschriften wird auch nicht auf Private erstreckt, derer sich die Behörden zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedienen (so z.B. § 1 Abs. 3 IFG-Bund und § 2 Abs. 1 Nr. UIG-Bund). Damit wird die Flucht ins Privatrecht eröffnet.

2.2 Anwendungsbereich (§ 81 HDSIG)

Die Vorschrift enthält in Absatz 2 eine erstaunliche Vielzahl von Bereichsausnahmen. Augenscheinlich ist es den so privilegierten Behörden im Abstimmungsprozess des Gesetzentwurfs gelungen, sich komplett aus dem ungeliebten Gesetzgebungsvorhaben herauszunehmen. So sollen vom Anwendungsbereich des Gesetzes über die übliche Bereichsausnahme für die Nachrichtendienste hinaus ausgenommen sein die Polizeibehörden, die Landeskartellbehörde, die Regulierungskammer, die Industrie- und Handelskammern und die Handwerkskammern. Ausweislich der Gesetzesbegründung wird dies damit begründet, dass diese Stellen „regelmäßig Daten mit spezifischem Schutzerfordernissen" verarbeiten (so für die Polizei und den Verfassungsschutz), oder „in erheblichem Umfang Betriebs- und Geschäftsgeheimnisse verarbeiten" (für die Landeskartellbehörde und die Regulierungskammer). Es wird zwar auf die besonderen Schutzvorschriften z.B. für Betriebs- und Geschäftsgeheimnisse verwiesen (Lt-Drs. 19/5728, S. 150), warum diese keinen hinreichenden Schutz gewähren, bleibt unerfindlich.

Im Ergebnis weist der Gesetzentwurf damit den wohl engsten Anwendungsbereich der Informationsfreiheitsgesetze des Bundes und der Länder auf. Mit § 81 Abs. 3 HDSIG

werden die Bereichsausnahmen auf bei anderen Behörden liegende amtliche Informationen erstreckt, ohne dass es auf eine konkrete Schutzbedürftigkeit der Unterlagen ankommt.

Warum hier die auch eher restriktiven Informationszugangsregelungen des IFG-Bund mit seinen vielen Schutz und Ausnahmeregelungen nicht konsensfähig war, ist nicht nachvollziehbar.

2.3 Schutz besonderer öffentlicher und privater Belange (§ 82 HDSIG)

Nr. 1 nimmt Verschlusssachen nach dem Hessischen Sicherheitsüberprüfungsgesetz vom Informationszugang aus. Ob hier auf die formelle Einstufung abzustellen ist oder ob darüber hinaus auf das Vorliegen der materiellen Einstufungsvoraussetzungen abzustellen ist (so BVerwG zu § 3 Nr. 4 IFG-Bund, Urteil vom 29.10.2009, Az. 7C22.08, Rdnr. 51) bleibt auch in der Gesetzesbegründung offen.

Nr. 4 soll Geheimnisse schützen, die zum persönlichen Lebensbereich gehören. Um welche Informationen es hier gehen kann und warum die folgende Vorschrift zum Schutz personenbezogener Informationen nicht ausreicht, bleibt unerfindlich. Die Gesetzesbegründung verschweigt sich hier.

Besonders besorgniserregend ist die Ausnahmevorschrift des Nr. 5, der einen Informationszugang ausschließt, soweit „rein wirtschaftliche Interessen an den Informationen bestehen". Welchem Schutzbedürfnis diese Vorschrift dient, bleibt unerfindlich. Im Ergebnis wird damit die gesamte Presse vom Informationszugang nach dem Gesetz ausgeschlossen und auf die presserechtlichen Ansprüche zurückgeworfen, die nur einen Auskunfts- und gerade keinen Akteneinsichtsanspruch gewähren.

2.3 Schutz personenbezogener Informationen (§ 83 HDSIG)

Die Norm nimmt alle personenbezogenen Informationen im Ergebnis aus dem Anwendungsbereich der Informationszugangsregelungen heraus. Eine Abstufung nach der Schutzbedürftigkeit oder eine Rechtsgüterabwägung sieht das Gesetz nicht vor.

2.4 Schutz behördlicher Entscheidungsprozesse (§ 84 HDSIG)

Die Norm entspricht im Wesentlichen § 4 IFG-Bund. Überraschend ist die Schutzvorschrift des Absatzes 3 in Bezug auf „Protokolle vertraulicher Beratungen". Augenscheinlich muss es sich hier um Protokolle handeln die „vertraulich" sind, aber nicht

als Verschlusssache eingestuft sind, da sie ja dann bereits unter die Schutzvorschrift des § 82 Nr. 1 HDSIG fielen. Die Gesetzesbegründung verschweigt sich hier leider wieder. Augenscheinlich sollen hier die Behörden die Möglichkeit erhalten, Beratungsprotokolle nach eigenem Gutdünken dem Informationszugang zu entziehen.

2.5 Verfahren bei Beteiligung Dritter und Entscheidungen (§86 und 87 HDSIG)

Die Vorschriften entsprechen im Wesentlichen den Vorschriften des IFG-Bund (dort § 7 und 8) und zeichnen auch die Fristenregeln nach.

2.6 Kosten (§ 88 HDSIG)

Wie auch § 10 IFG-Bund stellt § 88 HDSIG auf Amtshandlungen nach dem Gesetz ab und würde daher auch die Gebührenerhebung bei Antragsablehnung erfassen. Seit 2001 stellt dahingegen das UIG auf die Übermittlung von Informationen nach diesem Gesetz ab und schließt damit bereits Gebührenerhebungen bei Antragsablehnung aus (§ 12 Abs. 1 UIG). Das in der Anlage enthalte Kostenverzeichnis nach § 13 Abs. 9 HDSIG enthält erfreulicherweise keinen Kostentatbestand für eine Antragsablehnung. Dies hätte bereits im Gesetz geregelt sein sollen.

2.7 Informationsfreiheitsbeauftragter (§ 89 HDSIG)

Die Einsetzung eines oder einer Informationsfreiheitsbeauftragten ist sehr zu begrüßen.

2.8 Archivalien

Der Gesetzentwurf enthält keine Regelungen zur Anwendung der Informationszugangsregelungen auf Archivalien nach dem hessischen Archivgesetz, womit die Unterlagen mit Archivierung dem Informationszugang nach diesem Gesetz wieder entzogen und nur noch archivrechtlichen Vorschriften mit ihren Schutzfristen unterfallen. Eine überraschende Regelung.

Dr. Sven Berger

Bund der
Strafvollzugsbediensteten Deutschlands
Landesverband Hessen
Fachgewerkschaft im
dbb beamtenbund und tarifunion

Birgit Kannegießer, Notisweg 59, 64342 Seeheim-Jugenheim

Birgit Kannegießer
Landesvorsitzende

Telefon dienstlich: 069/1367-1000
Telefon privat: 06257/9440680
E-Mail: Vorsitzende@bsbd-hessen.de
Datum: 07.03.2018

Hessischer Landtag
Postfach 3240

65022 Wiesbaden

Mündliche Anhörung im Hessischen Landtag zum Gesetzentwurf der Fraktionen der CDU und Bündnis 90/Die Grünen für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit

Schreiben vom 21.12.2017 (I A 2.1)

Sehr geehrter Herr Abgeordneter Klee,
sehr geehrte Frau Dr. Lindemann,

im Namen des Bunds der Strafvollzugsbediensteten Hessen (BSBD) bedanke ich mich ausdrücklich für die Gelegenheit, zu dem uns zugeleiteten Gesetzentwurf der Fraktionen von CDU und Bündnis 90/Die Grünen Stellung nehmen zu können.

Als Fachgewerkschaft Justizvollzug erlauben wir uns allerdings, uns auf die Neuregelungen in den Vollzugsgesetzen zu beschränken (Artikel 2 – 6), wobei sich die Ausführungen zunächst auf Artikel 3, die beabsichtigte Änderung des Strafvollzugsgesetzes bezieht, die Inhalte jedoch in alle Vollzugsgesetze übernommen werden sollen. Auf eine Wiederholung wird zweckmäßigerweise verzichtet.

Die Umsetzung der in Rede stehenden EU-Richtlinie war durch die Vollzugspraktikerinnen und Vollzugspraktiker quasi schon mit Schaudern erwartet worden. Welche zusätzlichen und zukünftig zu erfüllenden Anforderungen an die Dokumentation des dienstlichen Handelns und jeder Entscheidung ergeben sich aus der Einführung des „unbedingten Erfordernisses“. Beim Lesen waren wir versucht, mal durchzuzählen, wie viele Male das „unbedingt erforderlich“ nun im Gesetz ausgebracht wurde. Wir haben vom tatsächlichen Zählen abgesehen.

In der vollzuglichen Praxis sehen wir allerdings konkrete Umsetzungsschwierigkeiten:

- Wie soll ein Besuchsbeamter zukünftig reagieren, wenn die anwesenden Besuchsteilnehmer (Gefangener und externer Besucher) plötzlich über Dinge reden, die in § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes reden – also über die Herkunft, die politische Meinung, die religiösen und weltanschaulichen Überzeugungen? Soll er gar den Besuch abbrechen, weil nun die Überwachung unter dem Aspekt der „unbedingten Erforderlichkeit“ steht?
  (§ 34 Abs. 4)
- Bei optischer Überwachung ist zukünftig zu bewerten, ob diese zum Erreichen des verfolgten Zwecks „unbedingt erforderlich“ ist. (§ 34 Abs. 5)
- Auf die Postkontrolle, soweit sie „unbedingt erforderlich“ ist, sollen die Gefangenen zukünftig bei ihrer Aufnahme in die Anstalt hingewiesen werden (§ 35 Abs. 2)
- Die optische Überwachung von Kameras außerhalb der Hafträume war durch den ehemaligen Justizminister Jürgen Banzer ausdrücklich gefordert worden. Wir liefen als BSBD Hessen damals Sturm gegen diese Regelung, da Kameras keine zusätzliche Sicherheit bieten und verlangten Überwachung durch Präsenz von Beamtinnen und Beamten. Damals kamen die Kameras – nicht das Personal. Nun werden die damals eingeführten Kameras dem neuen Kriterium der „unbedingten Erforderlichkeit“ unterworfen (§ 45 Abs. 2 Satz 2). Heißt das nun: Reduzierung der Kameras ohne Personalverstärkung???

- Sogar die Unterbringung in einer so genannten Kamerazelle unterliegt nun dem „unbedingten Erfordernis“ (§ 50). Ja warum denn sonst? Gefangene werden dort doch nicht zum Spaß untergebracht!
- Begrüßt wird die Legitimierung des Auslesens von illegal eingebrachten Handys. Diese Geräte gefährden die Sicherheit im Justizvollzug markant. Das über die Möglichkeit des Auslesens jedoch zukünftig bei Aufnahme in die JVA belehrt werden sollt, bringt uns Vollzugspraktikerinnen und Vollzugspraktiker dann doch mal zum Schmunzeln.

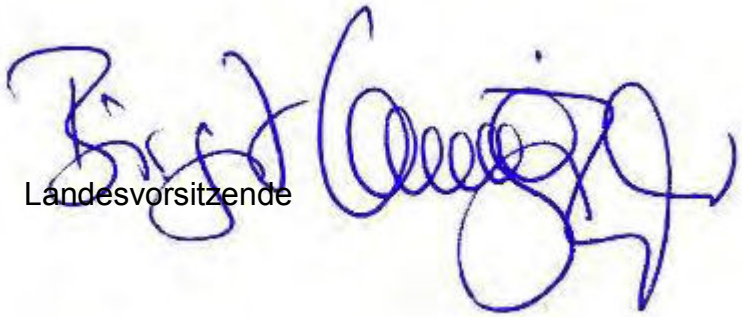
Richtig schlimm finden wir allerdings die in § 58 Abs. 6 beabsichtigte Regelung, bei Überwachung der Außenbereiche der Anstalt mit technischen Hilfsmitteln – insbesondere der Videoüberwachung – neben dem Hinweisschild bzgl. Kameraüberwachung gar **Name und Kontaktdaten der Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt kenntlich zu machen.**

Hier, sehr geehrte Abgeordnete des Hessischen Landtags, greift ganz entschieden das Schutzbedürfnis der verantwortlichen Bediensteten des Hessischen Justizvollzugs. Es kann nicht sein, dass Name und Kontaktdaten für diese Maßnahmen öffentlich bekannt zu geben sind! Die Bediensteten des Justizvollzugs haben jeden Tag Umgang mit schwieriger, immer wieder unberechenbarer, vernetzter Klientel. **Hier nun das Informationsbedürfnis Externer höher zu bewerten als dasjenige der Mitarbeiterinnen und Mitarbeiter des Vollzugs, ist nicht nachzuvollziehen. Auch Mitarbeiterinnen und Mitarbeiter des Justizvollzugs haben schützenswerte Rechte.** Hier wird das Risiko aus dem täglichen Umgang mit gefährlichen Menschen völlig unterschätzt bzw. außer Acht gelassen! Jegliche Bekanntgabe, die über das übliche Kamerasymbol hinaus geht, ist ungeeignet, die namentliche Benennung von Bediensteten des Justizvollzugs ist mithin unzumutbar.

Für Ihre Einladung zur öffentlichen Anhörung im Innenausschuss am 15.032018 bedanken wir uns, der BSBD Hessen wird durch Unterzeichnerin vertreten sein. Allerdings bleibt mir nur, bereits heute darauf hinzuweisen, dass ich der Anhörung nur bis gegen 12 Uhr folgen kann, da am gleichen Tag der bisherige Leiter der JVA Frankfurt I durch Frau Staatsministerin Kühne-Hörmann verabschiedet und der neue Leiter dieser Anstalt in sein Amt eingeführt wird.

Mit freundlichen Grüßen

Birgit Kannegießer



Landesvorsitzende

Prof. Dr. Anne Riechert
Frankfurt University of Applied Sciences
Nibelungenplatz 1
60318 Frankfurt

Hessischer Landtag
Schlossplatz 1-3
65183 Wiesbaden

Frankfurt, den 08.03.2018

Betr.: Mündliche Anhörung im Hessischen Landtag

Sehr geehrte Damen und Herren,

für die Übersendung des Gesetzentwurfs bedanke ich mich.

Nachfolgend erhalten Sie bitte meine Stellungnahme zu ausgewählten Regelungen des Artikel 1 (Hessisches Datenschutz- und Informationsfreiheitsgesetz) sowie Artikel 18 (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung) des Gesetzentwurfs des Hessischen Gesetzes zur Anpassung Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit.

Ausführungen zum HDSIG-E sind auf S. 2 ff., Ausführungen zum HSOG-E auf S. 16 ff. zu finden. Sowohl die Stellungnahme zum HDSIG-E als auch zum HSOG-E beginnen mit einer Einleitung, bevor auf einzelne Regelungen der Gesetzentwürfe näher eingegangen wird. Beim HSOG-E werden im Rahmen der Einleitung zusätzlich der Begriff der Ordnungswidrigkeit und die Aufgabenzuweisung der Gefahrenabwehr- und Polizeibehörden behandelt. Auf S. 85 erfolgt sodann ein Fazit.

Mit freundlichen Grüßen

Anne Riechert

1. Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG-E)

Einleitung

Um dem Harmonisierungsgedanken der Europäischen Datenschutzgrundverordnung gerecht zu werden, sollten zwar für die Verarbeitung von personenbezogenen Daten möglichst wenige Sonderregelungen in anderen Gesetzen geschaffen werden, dennoch sollte bedacht werden, dass bereichsspezifische Regelungen in einem speziellen Gesetz geregelt sein sollten. Daher stellt sich die Frage, ob die Regelungen der §§ 40 ff. HDSIG-E, die sich auf Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit beziehen, tatsächlich in das Hessische Datenschutzgesetz integriert werden sollten. Durch die zugrundeliegende Richtlinie (EU) Nr. 2016/680 kann das informationelle Selbstbestimmungsrecht stärker eingeschränkt werden als nach den Grundsätzen der Datenschutzgrundverordnung. Das Hessische Datenschutzgesetz gilt daher für Aufgaben der allgemeinen Verwaltung. Für Tätigkeiten der Gefahrenabwehr und polizeiliche Tätigkeiten sind bereichsspezifische Regelungen notwendig, so dass eine Ergänzung des HSOG durch das HDSG nur in Betracht kommen kann, wenn es Regelungen enthält, die allgemein gelten können.[1] Da aber gerade auch die Betroffenenrechte (z.B. Informationspflichten) im dritten Teil abweichend von denen des zweiten Teils geregelt sind, gehen diese Regelungen über allgemein geltende Bestimmungen hinaus..

Insbesondere muss hierbei auch das Transparenzprinzip ein wesentliches Ziel darstellen. Das Gebot der Transparenz sollte ein allgemeiner Gedanke sein, der auf gesetzliche Regelungen ebenso angewendet werden sollte wie auf private Verträge, wobei auch die Gesetze verständlich und zugänglich sein sollten.[2] Die Frage ist allerdings, ob für einen Bürger tatsächlich nachvollziehbar ist, unter welchen Voraussetzungen, die §§ 40 ff. HDSIG-E zur Anwendung gelangen und aus welchem Grunde Regelungen, die in einem Sicherheitsgesetz geregelt sein sollten, in einem Gesetz integriert sind, dass geschaffen wurde, um sein Recht zu schützen, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen bzw. im Sinne von Artikel 8 Grundrechte-Charta seine personenbezogenen Daten zu schützen.

Weiterhin sollte geprüft werden, ob die im Gesetzentwurf enthaltenen Wiederholungen des Textes der Datenschutzgrundverordnung vermieden werden können (siehe hier etwa § 20 HDSIG-E).[3]

Insgesamt sollte Erwägungsgrund 10 der Datenschutzgrundverordnung nicht „vergessen“ werden, in welchem geregelt ist, dass die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten unionsweit gleichmäßig und

[1] Nungesser, HDSG, § 3 Rn. 41, der außerdem unter Rn. 42 unter anderem etwa auf Begriffsbestimmungen, Regelungen zur Auftragsdatenverarbeitung oder zum Datenschutzbeauftragten hinweist und unter Rn. 37 auf die Notwendigkeit bereichsspezifischer Regelungen vor allem im Sicherheitsbereich verweist, da das für die allgemeine Verwaltung geltende Datenschutzgesetz kein Auffanggesetz für gesetzgeberische Versäumnisse in bereichsspezifischen Gebieten sein könne.

[2] Siehe hierzu im Zusammenhang mit verbraucherschützenden Normen die Ausführungen von Heiderhoff, Europäisches Privatrecht, Rn. 256; mit Verweis unter Rn. 257, dass der EUGH aus dem Transparenzgedanken die Pflicht zur klaren und deutlichen Umsetzung der Richtlinien abgeleitet habe.

[3] Dies gilt, auch wenn in der Begründung zum HDSIG-E (s. S. 118) darauf Bezug genommen wird, dass es sich im Gesetzestext lediglich um punktuelle Wiederholungen handelt.

einheitlich angewandt werden sollten. [4] Zur Wahrung der Rechtseinheit sollte daher möglichst überprüft werden, inwieweit die übrigen Landesdatenschutzgesetze wortgleiche Regelungen beinhalten.

Zu den einzelnen Regelungen:

§ 1 Absatz 1 HDSIG-E

Hier wäre eine Klarstellung wünschenswert, dass das Gesetz **zum Schutz natürlicher Personen** bei der Verarbeitung personenbezogener Daten gilt (entsprechend Artikel 1 Absatz 1 Datenschutzgrundverordnung und Artikel 8 GrundrechteCharta). Siehe auch die Ausführungen zu § 40 HDSIG-E.

§ 1 Absatz 3 HDSIG-E

Das Hessische Datenschutzgesetz soll anstatt des Hessischen Verwaltungsverfahrensgesetzes gelten, wenn es sich nicht um die Ermittlung eines Sachverhaltes handelt („Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogenen Daten verarbeitet werden").

Nicht jedes Bundesland hat in der Vergangenheit in seinen Datenschutzgesetzen den Vorrang des Verwaltungsverfahrensgesetzes *bei Ermittlungstätigkeiten* geregelt.

Daher könnte geprüft werden, ob im Rahmen der Regelung des § 1 Absatz 3 aus Gründen der Rechtsklarheit und einer einheitlichen Rechtsanwendung in den Bundesländern die Formulierung „bei der Ermittlung des Sachverhalts" zu streichen ist.

Anderenfalls würden die Vorschriften des Verwaltungsverfahrensgesetzes uneingeschränkt gelten, soweit die Verwaltungstätigkeit nicht in der Ermittlung des Sachverhalts besteht. Abweichende Regelungen hätten damit Vorrang.[5] Der Vorrang des Datenschutzrechts im gesamten Verwaltungsverfahren und nicht nur im Ermittlungsverfahren wurde allerdings bereits im Hinblick auf das Bundesdatenschutzgesetz im Verhältnis zum Bundesverwaltungsgesetz vertreten, auch wenn dies nicht ausdrücklich im Gesetz geregelt ist.[6]

Zu beachten ist zwar, dass es sich beim Akteneinsichtsrecht des § 29 HVwVfG um eine spezielle Regelung handelt, die das rechtliche Gehör sicherstellen soll, da die die Gewährung von Akteneinsicht einen Eingriff in das Recht auf informationelle Selbstbestimmung solcher Personen darstellt, deren personenbezogene Daten auf diese Weise zugänglich gemacht werden, so dass die schutzwürdigen Interessen dieser Personen der Gewährung von Akteneinsicht daher entgegenstehen

[4] Erwägungsgrund 10 der Datenschutzgrundverordnung: „Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden."

[5] Nungesser, HDSG, § 3 Rn. 26.

[6] Dix in: Simitis, BDSG, § 1 Rn. 193.

oder es erforderlich machen können, den Zugang zu den Daten angemessen zu beschränken.[7] Allerdings sind auch im Rahmen des Auskunftsrechts nach Artikel 15 Datenschutzgrundverordnung gemäß Erwägungsgrund 63[8] die Rechte und Freiheiten von Dritten zu berücksichtigen, so dass für Verfahrensbeteiligte eine entsprechende Regelung im Rahmen der Datenschutzgrundverordnung besteht. Im Übrigen ist zu berücksichtigen, dass im englischen Originaltext das Recht mit „Right of access" bezeichnet wird, damit also allgemein ein Zugangsrecht zu personenbezogenen Daten bzw. ein Recht auf Einsichtnahme besteht. Dennoch muss geprüft werden, inwieweit der Wortlaut dieser Regelung den angestrebten Schutzzweck der Datenschutzgrundverordnung im Hinblick auf die Rechte Dritter wiedergibt, was auch aus Harmonisierungsgesichtspunkten wichtig ist, damit auf europäischer Ebene ein einheitliches Recht geschaffen werden kann.

§ 1 Absatz 5 HDSIG-E

Mit § 1 Abs. 5 HDSIG-E soll die Aussage getroffen werden, dass die Vorschriften des HDSIG-E keine Anwendung finden, soweit das Recht der Europäischen Union, insbesondere die Datenschutzgrundverordnung Anwendung finden. Gemäß der Begründung (S. 118) soll dabei der Verordnung (EU) Nr. 2016/679 unmittelbare Geltung zukommen. Da hier auf den selbstverständlichen Anwendungsvorrang des Unionsrechts Bezug genommen wird, ist diese Regelung entbehrlich. Außerdem darf die Formulierung „unmittelbare Geltung" nicht mit dem Begriff eines Geltungsvorrangs verknüpft werden. Entsprechendes gilt im Übrigen für § 3 Absatz 4 HSOG-E.

§ 2 Absatz 4 HDSIG-E

Zu prüfen ist, ob es aus unionsrechtlicher Sicht zulässig ist, für den Begriff der Anonymisierung eine Legaldefinition im Gesetzestext aufzunehmen. In der Datenschutzgrundverordnung erfolgt lediglich eine Definition der Pseudonymisierung (Artikel 4 Nr. 5 Datenschutzgrundverordnung) und beschreibt in Erwägungsgrund 26 nur zusätzlich, was unter anonymen Informationen zu verstehen ist.

Es muss darauf geachtet werden, dass durch eine solche Legaldefinition nicht der Begriff der Anonymisierung bereits festgelegt wird, da eine entsprechende Auslegung unionsrechtlich erfolgen müsste. Dies hat vor allem für die Frage Bedeutung, ob bei anonymen Informationen eine relative oder objektive Sichtweise zugrunde gelegt wird.

Im Zusammenhang mit anonymen Informationen ist zu berücksichtigen, dass die gleiche Formulierung zur Bestimmbarkeit einer natürlichen Person im englischen Originaltext zu abweichenden Formulierungen in den deutschen Übersetzungen der Datenschutzgrundverordnung einerseits und der EU-Richtlinie 96/46/EG andererseits wie folgt geführt hat:

Erwägungsgrund 26 der Datenschutzgrundverordnung:

To determine whether a natural person is identifiable, account ***should be taken of all the means reasonably likely to be used****, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.*

Übersetzung:

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person ***nach allgemeinem Ermessen***

[7] BVerfG, Beschluss vom 24.09.2002 - 2 BvR 742/02.
[8] Erwägungsgrund 63 bezieht sich im Übrigen nicht nur auf die Rechte Dritter im Rahmen von Kopien.

***wahrscheinlich genutzt werden**, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.*

Diese Formulierung wurde bereits in der EU-Richtlinie 95/46/EG verwendet, aber jedoch im Unterschied dazu folgendermaßen übersetzt:

Erwägungsgrund 26 der EU-Richtlinie 95/46/EG:

*whereas, to determine whether a person is identifiable, account **should be taken of all the means likely reasonably to be used** either by the controller or by any other person to identify the said person*

Übersetzung:

*Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die **vernünftigerweise** entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten **eingesetzt werden könnten**, um die betreffende Person zu bestimmen*.

Ohne eine Wortklauberei betreiben zu wollen, muss beachtet werden, dass es einen Unterschied in der Formulierung darstellt, ob Mittel vom Verantwortlichen oder einem Dritten *wahrscheinlich genutzt werden* oder ob diese *Mittel eingesetzt werden könnten*.

Es sollte vermieden werden, bereits im Vorfeld durch Formulierungen eine Definition festzulegen, sondern es muss eine europaweit einheitliche Auslegung eruiert werden. Daher muss auch im Hinblick auf die Übersetzung die Intention des europäischen Gesetzgebers und die Auslegung durch den EUGH mit einbezogen werden.

Durch die Formulierung in § 2 Absatz 4 HDSIG-E könnte sich nun eine Tendenz ergeben, dass die subjektive Planung der Beteiligten maßgeblich ist. Bei anderer Auslegung könnte es jedoch darum gehen, ob eine Identifizierung unter Berücksichtigung der Kosten, des Zeitaufwands und der zur Verfügung stehenden Technologien möglich ist, da sie grundsätzlich eingesetzt werden könnten (so dass die vermeintlichen Absichten oder Möglichkeiten der Verantwortlichen keine Rolle spielen).[9]

Die Fokusgruppe Datenschutz hat sich in diesem Zusammenhang bereits für eine relative Sichtweise ausgesprochen.[10]

Der Gesetzgeber hat nun die Beschreibung der anonymen Informationen in Erwägungsgrund 26 umformuliert und als Legaldefinition eingeführt, wobei er diese allerdings aus dem Kontext der pseudonymen Informationen herausgenommen hat. So heißt es in diesem Erwägungsgrund auch: „*Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, **wie beispielsweise das Aussondern***."

Auf das „Aussondern" nimmt die Definition in § 2 Absatz 4 HDSIG-E allerdings keinen Bezug, was im englischen Originaltext im Übrigen mit „Singling-Out" beschrieben wird und eine anfängliche Forderung der Artikel-29-Datenschutzgruppe darstellt. In seinem ursprünglichen Sinne ist damit die Möglichkeit der Auswahl und unterschiedliche Behandlung von Personen gemeint: „*Eine der*

[9] Es geht im letzteren Falle also darum, ob in vernünftigerweise durchführbar und praktikabel der Personenbezug hergestellt werden könnte.
[10] S. 13, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017.

Hauptschlussfolgerungen dieser Analyse ist es, dass eine natürliche Person als bestimmbar angesehen werden kann, wenn sie innerhalb einer Personengruppe von den anderen Mitgliedern der Gruppe unterschieden und somit unterschiedlich behandelt werden kann."[11] Damit soll bei der Frage, ob eine Person bestimmbar ist, also auch eine entsprechende Auswahlmöglichkeit erfasst sein, die als Singling Out bezeichnet wird.

Wenn nun in § 2 Absatz 4 HDSIG-E eine Definition erfolgt, die aus ihrem Kontext unter Berücksichtigung der pseudonymen Informationen herausgelöst wird, besteht daher außerdem die Gefahr, dass die Kriterien für die Bestimmbarkeit einer Person nicht umfassend berücksichtigt werden. Insgesamt sollte dementsprechend - um nicht der unionsrechtlichen Auslegung und Unterscheidung von anonymen und pseudonymen Informationen bzw. Daten vorzugreifen - die eingeführte Legaldefinition in § 2 Absatz 4 HDSIG-E kritisch geprüft werden. Hierbei sollte auch die oben angesprochene Übersetzung der Formulierungen aus der englischen Originalfassung einbezogen werden. Aufgrund der europaweiten Harmonisierung können dabei ebenso die Übersetzungen von Erwägungsgrund 26 Datenschutzgrundverordnung in den übrigen Mitgliedstaaten von Bedeutung sein.

§ 4 HDSIG-E

Es bestehen - wie bereits in der Vergangenheit im Hinblick auf § 6b BDSG - Bedenken, ob die Regelung des § 4 vollständig den genannten Anforderungen an eine verfassungsgemäße Schranke des Rechts auf informationelle Selbstbestimmung genügt, was insbesondere mit Blick auf die Gebote der Normenklarheit und Bestimmtheit gilt.[12] Die betroffene Person wird nach wie vor auf dieser allgemeinen Grundlage das Ausmaß der Datenverarbeitung nicht vorhersehen können. Anlass, Zweck und Grenzen des Eingriffs müssen in der Ermächtigung aber bereichsspezifisch, präzise und normenklar festgelegt werden.[13]

Dies muss insbesondere unter der Maßgabe gesehen werden, dass der Einsatz von Videotechnik sehr stark in das Recht auf informationelle Selbstbestimmung eingreift. Zu beachten ist daher, dass Maßnahmen zur Videoüberwachung, die die öffentliche Sicherheit betreffen, bereichsspezifisch und mit dem notwendigen Detaillierungsgrad in den Sicherheitsgesetzen geregelt werden müssten.[14] Wie bereits in der Einleitung gesagt, handelt es sich beim HDSG um Bestimmungen für die allgemeine Verwaltung und Ermächtigungsgrundlagen für besonders folgenreiche Eingriffe müssen in bereichsspezifischen Regelungen geschaffen werden, wie im Polizeigesetz.[15]

Zu berücksichtigen ist weiterhin, dass Nr.3 („zur Wahrnehmung berechtigter Interessen") in der Vergangenheit auf bundesgesetzlicher Ebene nur für nicht-öffentliche Stellen Geltung beanspruchen sollte.[16] Dies wäre auch im Rahmen des HDSIG-E im Hinblick auf Artikel 6 Absatz 1f)

---

[11] Artikel-29-Datenschutzgruppe, WP 199, S. 6. So könnte auch die Art festgelegt oder beeinflusst werden, in der die Person behandelt oder beurteilt wird (siehe Artikel-29-Datenschutzgruppe aaO).
[12] Scholz in: Simitis, BDSG, § 6b Rn. 32.
[13] Vgl. BVerfGE 65, 1, 44 ff..
[14] Nungesser, HDSG, 12 Rn. 4.
[15] Nungesser, HDSG, § 1 Rn. 16.
[16] Zscherpe in: Taeger/Gabel, BDSG, § 6b Rn. 47; Scholz in: Simitis, BDSG, § 6b Rn. 77 mit Verweis auf die Beschlussempfehlung und den Bericht des Innenausschusses: Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss zu dem Gesetzentwurf der Bundesregierung– Drucksachen 14/4329, 14/4458 – Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, S. 6.

Datenschutzgrundverordnung sowie Erwägungsgrund 47 folgerichtig. Danach obliegt es dem Gesetzgeber, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, so dass „berechtigte Interessen“ nicht für Verarbeitungen durch Behörden gelten sollten, die diese in Erfüllung ihrer Aufgaben vornehmen.

In Nr. 1 bezieht sich das HDSIG-E allgemein auf die Aufgabenerfüllung öffentlicher Stellen. Hier wurde ebenfalls bereits in der Vergangenheit auf bundesgesetzlicher Ebene darauf verwiesen, dass es ausreicht, wenn die Videoüberwachung die Aufgabenerfüllung unterstützt und dies etwa zur Gebäudesicherung eingesetzt wird, wobei dann Überschneidungen zu Nr. 2 auftreten.[17] Diese Überschneidung somit auch bei § 4 HDSIG-E zukünftig zu erwarten.

Auch wenn die Datenschutzgrundverordnung gemäß § 1 Absatz 5 HDSIG-E Anwendung finden soll, wäre aus Transparenzgründen an dieser Stelle nochmals ein Hinweis auf die Informationspflichten des Verantwortlichen bei der Videoüberwachung angebracht. Gemäß § 4 Absatz 2 HDSIG-E ist für die betroffene Person nicht unbedingt absehbar, was unter geeigneten Maßnahmen zu verstehen ist und wann der frühestmögliche Zeitpunkt beginnt. Wie und auf welche Art die betroffene Person über die Videoüberwachung informiert wird, hätte an dieser Stelle für diesen speziell geregelten Fall der Videoüberwachung konkret geregelt werden können.

Im Übrigen ist im Sinne einer einheitlichen Terminologie der Begriff „Verwendung“ in § 4 Absatz 3 HDSIG-E durch „Verarbeitung“ zu ersetzen. Im Hinblick auf den Begriff der „Weiterverarbeitung“ ist zu berücksichtigen, dass dieser Begriff im HSOG-E eine eigenständige Definition erfährt,[18] im Rahmen des § 20 HSOG-E verwendet wird und auch die Formulierung „zur Abwehr von Gefahren für die öffentliche Sicherheit“ in § 4 Absatz 3 HDSIG-E einen Bezug zum HSOG-E vermuten lässt. Aus den Erwägungsgründen 50, 61 der Datenschutzgrundverordnung ergibt sich zusätzlich, dass mit Weiterverarbeitung stets eine Zweckänderung verbunden ist.[19] Daher müssten die Voraussetzungen von Artikel 6 Absatz 4 Datenschutzgrundverordnung vorliegen, also etwa die Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung sowie der Garantien für die betroffene Person. Im Sinne des Verhältnismäßigkeitsgrundsatzes sollten zudem Ausführungen dazu enthalten sein, welche konkreten Ordnungswidrigkeiten als nicht geringfügig zu betrachten sind. Im Hinblick auf die Einfügung von Ordnungswidrigkeiten in den Gesetzestext ist im Übrigen zu beachten, dass unklar ist inwieweit eine Ordnungswidrigkeit unionsrechtlich vom Begriff der „Straftat“ mit erfasst sind.[20]

§§ 8 ff. HDSIG-E

Diesbezüglich wird auf die Ausführungen des „Netzwerk Datenschutzexpertise“ verwiesen, die die Verbesserung der Transparenz im Bestellungsverfahren als eine zentrale Voraussetzung sehen und auf S. 6 ff. Vorschläge unterbreiten, diese Transparenz zu verbessern.[21]

[17] Scholz: in Simitis, BDSG, § 6b Rn. 71.
[18] Siehe zum Begriff der Weiterverarbeitung im Sinne des HSOG die Ausführungen auf S. 21.
[19] Siehe die Ausführungen auf S. 26.
[20] Siehe auch die Ausführungen auf S. 15 ff..
[21] https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_auswahlblfdi6.pdf

§ 20 HDSIG-E

Der europäische Gesetzgeber hat den Mitgliedstaaten die Möglichkeit eröffnet, die in Artikel 9 Absatz 2 genannten Ausnahmen zu spezifizieren. Aus Gründen der Übersichtlichkeit und der Transparenz und im Hinblick auf die außerordentliche Bedeutung dieses Verarbeitungstatbestandes sollte es in Artikel 20 daher nicht heißen *„Abweichend von Artikel 9 Absatz 1……."*, sondern es sollte konkret auf die Ausnahmeregeln des Artikel 9 Absatz 2 verwiesen werden, die den Mitgliedstaaten eine konkrete Regelungsbefugnis erlauben, so etwa Artikel 9 Absatz 2 Nr. 2b).

Auch Erwägungsgrund 10 bietet den Mitgliedstaaten den notwendigen Spielraum für die Spezifizierung dieser Vorschriften im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten**.** Diesbezüglich schließt die Datenschutzgrundverordnung nicht aus, dass Mitgliedstaaten Rechtsvorschriften erlassen, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

In § 20 HDSIG-E fehlen jedoch die genauere Bestimmung und Konkretisierung der Voraussetzungen, was ebenso der Rechtsprechung des Bundesverfassungsgerichts widerspricht, gemäß derer es einer gesetzlichen Grundlage bedarf, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar für den Bürger ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht.[22] Das Bundesverfassungsgericht führt hierzu aus: „Je schwerwiegender die Auswirkungen sind, desto höhere Anforderungen werden an die Bestimmtheit der Ermächtigung zu stellen sein."[23]

Es muss zudem transparent sein, welche Regelungen nur sinngemäß die ohnehin bestehende Regelung nach der Datenschutzgrundverordnung wiederholen (was nach der Rechtsprechung des EUGH im Übrigen nur unter engen Voraussetzungen zugelassen ist) oder welche Regelungen tatsächlich Abweichungen und eigene inhaltliche Regelungen zu den Ausnahmetatbeständen des Artikel 9 Datenschutzgrundverordnung enthalten.

So erlaubt § 20 Absatz 1 Nr. 4a) HDSIG-E die Verarbeitung besonderer Kategorien personenbezogener Daten „pauschal" aus Gründen eines erheblichen öffentlichen Interesses. In der Datenschutzgrundverordnung ist unter Artikel 9 Absatz g) allerdings geregelt, *dass die Verarbeitung besonderer Kategorien personenbezogener Daten auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats erlaubt ist, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.*

Eine entsprechend konkrete Ausgestaltung enthält jedoch § 20 HDSIG-E nicht, wobei zudem zu berücksichtigen wäre, dass es sich beim Begriff des öffentlichen Interesses, ebenso wie bei der *öffentlichen Sicherheit* in § 20 Absatz 1 Nr. 4b) HDSIG-E,[24] um einen Begriff des Gemeinschaftsrecht

[22] BVerfGE 65, 44.
[23] Nungesser, HDSG, § 1 Rn. 15 mit Verweis und Zitat von BVerfG 56, 12.
[24] Siehe zur öffentlichen Sicherheit die Ausführungen auf S. 15.

handelt. Daher wäre zusätzlich zu prüfen, inwieweit der deutsche Gesetzgeber diesen definieren oder konkretisieren kann.[25]

Dennoch besteht durch die pauschale Wiedergabe des Gesetzestextes ohne Benennung von konkreten Voraussetzungen oder Spezifizierungen die Gefahr, dies als rechtmäßigen und ausreichenden bzw. abschließenden Verarbeitungstatbestand zu sehen, obwohl hierfür nicht die nach Artikel 9 Absatz g) Datenschutzgrundverordnung näheren Voraussetzungen, ggf. auch mit Verweis auf Regelungen in Spezialgesetzen, geschaffen sind. Der Gesetzgeber muss sich zwar grundsätzlich abstrakter und unbestimmter Formulierungen bedienen können. Es muss jedoch im Einzelfall geprüft werden, inwieweit es sinnvoller ist, besonders folgenreiche Eingriffe in bereichsspezifischen Gesetzen zu regeln.

Sofern diese Regelung als abschließender Verarbeitungstatbestand eingestuft wird, könnten die verarbeiteten sensiblen Daten im Übrigen auch zweckändernd verwendet bzw. übermittelt werden. Liegen nämlich Gesundheitsdaten vor, besteht eine besondere Gefahr dadurch, dass § 20 Absatz 2 Nr. 10, § 21 Absatz 2 und § 22 Absatz 3 HDSIG-E Zweckänderungen erlauben.

§ 21 HDSIG-E

Diese Rechtsgrundlage zur Datenverarbeitung im Rahmen der Aufgabenerfüllung einer öffentlichen Stelle muss mit Artikel 6 Absatz 1 e) Datenschutzgrundverordnung übereinstimmen und wegen der zweckändernden Verarbeitung muss insgesamt eine Rechtsgrundlage geschaffen werden, die gemäß Artikel 6 Absatz 4 und Artikel 23 eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt.

Bei Nr. 1 und Nr. 2 fehlt die Klarstellung, dass diese zur Erfüllung der Aufgabe erforderlich sein müssen (siehe Artikel 6 Absatz 3 DSGVO). Hier wird es im Einzelfall jedoch nur um Antragstellung, etc. gehen, also um Maßnahmen, die ohnehin für die Ausübung der Verwaltungstätigkeit erforderlich sind. Es fehlt darüber hinaus der Hinweis, dass der Betroffene informiert werden muss. Dies gilt aus Transparenzgründen, auch wenn in § 1 Absatz 5 HDSIG-E auf die Anwendbarkeit der Datenschutzgrundverordnung verwiesen wird.

Hinsichtlich § 21 Absatz 1 Nr. 4 ist Erwägungsgrund 50 der Datenschutzgrundverordnung zu beachten. Danach sollte in jedem Fall gewährleistet sein, dass die in der Datenschutzgrundverordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird. Im Übrigen können nach diesem Erwägungsgrund *der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten in Einzelfällen oder in mehreren Fällen,*

[25] Beim Begriff der öffentlichen Ordnung wurde vom EUGH im Zusammenhang mit der Einschränkung des freien Dienstleistungsverkehrs ein gewisser Auslegungsspielraum anerkannt, siehe Urteil des Gerichtshofes vom 14.Oktober 2004, Rechtssache C-36/02: *„Außerdem ist der Begriff der öffentlichen Ordnung im Gemeinschaftsrecht, insbesondere, wenn er eine Ausnahme von der Grundfreiheit des freien Dienstleistungsverkehrs rechtfertigen soll, eng zu verstehen, so dass seine Tragweite nicht von jedem Mitgliedstaat einseitig ohne Nachprüfung durch die Organe der Gemeinschaft bestimmt werden darf……. Allerdings können die konkreten Umstände, die möglicherweise die Berufung auf den Begriff der öffentlichen Ordnung rechtfertigen, von Land zu Land und im zeitlichen Wechsel verschieden sein. Insoweit ist den zuständigen innerstaatlichen Behörden daher ein Beurteilungsspielraum innerhalb der durch den EG-Vertrag gesetzten Grenzen zuzubilligen*."

die im Zusammenhang mit derselben Straftat oder derselben Bedrohung der öffentlichen Sicherheit stehen, an eine zuständige Behörde, als berechtigtes Interesse des Verantwortlichen gelten. Daraus wird der Ausnahmecharakter der Übermittlung von personenbezogenen Daten an andere Stellen deutlich. Daher muss auch im konkreten Einzelfall aus Sicht der verantwortlichen Stelle die zweckfremde Nutzung zur Verfolgung von Straftaten erforderlich sein. Es müssen außerdem rechtliche, berufliche oder sonstige verbindlichen Pflichten zur Geheimhaltung berücksichtigt werden. Ein entsprechender Hinweis auf die Geheimhaltungspflichten fehlt jedoch in § 21 HDSIG-E.

Auch liest sich diese Regelung -im Gegensatz zu § 12 Absatz 2 Nr. 4 der aktuellen Fassung des HDSG- so, als könne die Verwaltungsbehörde zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, Daten sammeln, was nicht dem „Hinweisrecht" gemäß Erwägungsgrund 50 entsprechen würde. Eine verantwortliche Stelle wird damit nicht zur Durchführung eigener von der eigentlichen Aufgabenstellung losgelösten gezielten Ermittlungen ermächtigt, sondern es geht um die Befugnis zur Unterrichtung von Strafverfolgungsbehörden. Durch die Formulierung in § 21 HDSIG-E steht nun aber der gelegentliche, zufällige Charakter nicht mehr im Vordergrund. Daher muss diese Regelung wie bereits in der Vergangenheit das Recht von öffentlichen Stellen umfassen, bei Straftaten, die sie „gelegentlich ihrer Aufgabenerfüllung", also zufällig entdeckt, der zuständigen Stelle einen entsprechenden Hinweis zu geben. Der Gesetzgeber wollte in der aktuellen Fassung des HDSG gerade keine gezielten Nachforschungen ermöglichen, da dafür die Verfolgungsbehörden zuständig sind, die ihre Rechtfertigung aus den jeweiligen Spezialgesetzen ableiten.[26] Insbesondere vor dem Hintergrund der hypothetischen Datenneuerhebung im HSOG könnte hier klar gestellt sein, wie das Gesetz zu verstehen ist. Allgemeine Verwaltungsbehörden dürfen nicht die Möglichkeit einer vorbeugenden Speicherung von personenbezogenen Daten haben. Es könnte beispielsweise die folgende Formulierung verwendet werden : „*wenn sich bei der Aufgabenerfüllung ergibt*", wobei § 21 HDSIG-E unmittelbar mit § 22 verknüpft werden könnte, so dass klar geregelt ist, dass eine Speicherung und Zweckänderung nur zulässig sind, um diese Daten an die Strafverfolgungsbehörde zu übermitteln.

Beachtet werden sollte zudem, inwieweit der Begriff der Straftat (Erwägungsgrund 50 der Datenschutzgrundverordnung) mit dem Begriff der Ordnungswidrigkeit gleichgesetzt werden kann.[27] Auf jeden Fall muss auch im Rahmen von § 21 HDSIG-E die Erforderlichkeit und Verhältnismäßigkeit berücksichtigt werden, so dass etwa ein Verdacht aufgrund tatsächlicher Anhaltspunkte vorliegen müsste und es müssen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern in die Verhältnismäßigkeitsprüfung mit einbezogen werden.[28]

§ 21 Absatz 1 Nr. 6 HDSIG-E entspricht Artikel 23 Absatz 1h Datenschutzgrundverordnung, nach dem allerdings zusätzlich Kontroll-, Überwachungs- und Ordnungsfunktionen verlangt sind , „*die dauernd*

[26] Nungesser, § 13, HDSG Rn. 14 ff..
[27] Siehe auch die Ausführungen zum HSOG-E, S. 15 ff.
[28] Taeger in: Taeger/Gabel, BDSG, § 14 Rn. 77 verweist im Rahmen der entsprechenden bundesgesetzlichen Regelung etwa darauf, dass das Ergebnis sein könne, dass Verfolgungsinteressen vor dem Hintergrund des Rechts auf informationelle Selbstbestimmung zurücktreten müssen. Siehe ebenso Dammann in: Simitis, BDSG, § 14 Rn. 80 mit dem Hinweis, dass in Einzelfällen wegen einer Disproportionalität von verfolgtem öffentlichen Interesse und der Schwere des Eingriffs in die informationelle Selbstbestimmung von einer Nutzung oder Übermittlung abzusehen sei. Die Verhältnismäßigkeit bezieht sich ebenso auf den Umfang der Information, Dammann aaO.

oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind."

Im Übrigen ist auch bei den Ausbildungs- und Prüfzwecken des § 21 Absatz 1 Nr. 6 HDSIG-E Erwägungsgrund 50 zu berücksichtigen: „*In jedem Fall sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird*". Gemäß Artikel 21 Datenschutzgrundverordnung steht dem Betroffenen ein solches Widerspruchsrecht zu.

§ 22 HDSIG-E

In § 22 Absatz 1 Satz 2 fehlt der ergänzende Verweis auf die Datenschutzgrundverordnung, da ansonsten suggeriert wird, eine Verarbeitung für andere Zwecke sei abschließend unter den Voraussetzungen des § 21 zulässig. Dies gilt auch aus dem Grunde, da § 21 und § 22 die Zweckänderung sehr pauschal regeln, und insbesondere bei der Verarbeitung besonderer Kategorien personenbezogener Daten auf die Regelung des § 20 HDSIG-E verweisen, die wie oben dargestellt, gerade keine spezifischen Regelungen enthält, sondern nur den Wortlaut der Datenschutzgrundverordnung wiedergibt. Es wäre damit ausreichend, dass ein nicht näher spezifizierter und unbestimmt formulierter Ausnahmetatbestand des § 20 vorliegt, um Daten zweckändernd zu verarbeiten oder zu übermitteln. Es fehlt außerdem der Verweis auf die Amts- und Berufsgeheimnisse.

§ 22 Absatz 2 S. 2 HDSIG-E stellt die Zulässigkeit der Verarbeitung für andere Zwecke unter den Vorbehalt, dass das HDSIG-E (§ 22 Absatz 2 S. 1) dies erlaubt und die übermittelnde Stelle zugestimmt hat. Hier ist zu beachten, dass dem Gesetzgeber die Regelungskompetenz gemäß Artikel 6 Absatz 3 für „rechtliche Verpflichtung" und „Ausübung öffentlicher Gewalt" zusteht, aber nicht pauschal. Die Zweckänderung kann sich daher nur durch Artikel 6 Absatz 4 ergeben. Selbst wenn man unterstellen würde, der Gesetzgeber hätte die Gesetzgebungsbefugnis für die inhaltliche Ausgestaltung der Verarbeitung für „andere Zwecke" (und zwar jedweden), würde an dieser Stelle immer noch die Berücksichtigung der Betroffenenrechte im Sinne von Erwägungsgrund 50 fehlen, wonach „*in jedem Fall sollte gewährleistet sein sollte, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird*". Der pauschale Hinweis darauf, dass (ausschließlich) die Regelungen des HDSG und die Einwilligung der Behörde gelten sollen, ist nicht ausreichend.

§ 22 Absatz 4 HDSIG-E legt der übermittelnden Stelle eine Prüfpflicht auf. Dennoch müssen die Grundsätze der Datenschutzgrundverordnung insoweit gelten, dass die (jeweils) verantwortliche Stelle den Nachweis der Rechtmäßigkeit der Verarbeitung gemäß Artikel 5 Absatz 2 Datenschutzgrundverordnung zu führen hat. Hieraus ergibt sich, dass die Übermittlung in der Verantwortung des Übermittelnden liegt und er den Nachweis der Übermittlung zu führen hat. Die anschließende Verarbeitung liegt in der Verantwortung der anderen Stelle, die ebenfalls den Nachweis zu führen hat. Bei § 22 Absatz 4 HDSIG-E ist demgemäß zu prüfen, inwieweit diese Regelung die Rechenschaftspflicht des Artikel 5 Absatz 2 Datenschutzgrundverordnung abschwächt. Hier geht es um den Nachweis des jeweiligen Verantwortlichen, dass die Datenverarbeitung gemäß Artikel 5 Absatz 1 Datenschutzgrundverordnung auf rechtmäßige Weise erfolgt. Eine

Schlüssigkeitsprüfung im Sinne von § 22 Absatz 4 HDSIG-E könnte hinter diesen Anforderungen jedoch zurückbleiben.

Im Übrigen beschränkt sich die Verantwortlichkeit des Empfängers im Gesetzestext unter § 22 Absatz 4 HDSIG-E folgerichtig auf die Empfänger im Sinne von § 2 Absatz 1 und 3 HDSIG-E, da dem Gesetzgeber keine Regelungskompetenz für nicht-öffentliche Empfänger zusteht.

§ 23 HDSIG-E

Bei den Regelungen zum Beschäftigtendatenschutz handelt es sich um bereichsspezifische Regelungen, die in einem speziellen Gesetz geregelt werden sollten. Sie gehen über den Rahmen eines allgemeinen Gesetzes hinaus und sind nicht anderweitig geregelt, da es weiterhin kein Gesetz zum Beschäftigtendatenschutz gibt.[29]

Nur als Klarstellung sind daher die folgenden Anmerkungen zu werten:

Zunächst hätte hier eine Berücksichtigung der Rechtsprechung des Bundesarbeitsgerichts erfolgen können.[30]

Weiterhin ist zu berücksichtigen, dass der Grundsatz der Direkterhebung nicht in der Datenschutzgrundverordnung verankert ist. Daher ist die Berücksichtigung und Erfüllung von Informationspflichten, gerade auch im Hinblick auf Arbeitnehmer, von besonderer Wichtigkeit. Dies kann etwa für die Fälle gelten, dass ein Arbeitgeber Daten über Bewerber aus sozialen Netzwerken oder beim früheren Arbeitgeber erhebt. Eine entsprechende konkrete Regelung, die gerade die Besonderheiten des Arbeitsverhältnisses berücksichtigt, fehlt jedoch in § 23 HDSIG-E.

Auch könnten Regelungen zum Umgang mit Gesundheitsdaten bei Einstellungsuntersuchungen ergänzt werden. So könnte gesetzlich geregelt werden, dass zwar dem Beschäftigten das vollständige Untersuchungsergebnis mitzuteilen ist, dem Arbeitgeber jedoch nur mitgeteilt werden darf, ob der Beschäftigte nach dem Untersuchungsergebnis für die vorgesehenen Tätigkeiten geeignet ist.

Außerdem findet Erwägungsgrund 50 im Gesetzestext keine Berücksichtigung: „*Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten*.“ Hier hätte ein entsprechender konkreter Ausschlussgrund formuliert werden können anstatt in § 23 Absatz 3 HDSIG-E auf die schutzwürdigen Interessen Bezug zu nehmen.

In diesem Zusammenhang ist auch auf § 20 Absatz 1 Nr. 2 HDSIG-E einzugehen, der auf Artikel 9 Absatz 2 h) Datenschutzgrundverordnung beruht und die Verarbeitung von besonderen Kategorien personenbezogener Daten ohne Einwilligung erlaubt, wenn dies für die Beurteilung der Arbeitsfähigkeit des Beschäftigten erforderlich ist.[31] In diesem Zusammenhang ist besonders zu

[29] Nungesser, HDSG, § 3 Rn. 44.

[30] „Die verdeckte Überwachung eines einer schweren Pflichtverletzung verdächtigen Arbeitnehmers ist nur unter den vergleichbaren Voraussetzungen zulässig wie zur Aufdeckung einer Straftat“ Siehe BAG vom 29.06.2017, 2 AZR 597/16.

[31] Artikel 9 Absatz 2 h) Datenschutzgrundverordnung: „*die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, **für die Beurteilung der Arbeitsfähigkeit des Beschäftigten**, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts*

berücksichtigen, dass diese Verarbeitung Gefahren für den Arbeitnehmer birgt. Erstens erfolgt eine Abweichung vom Wortlaut der Datenschutzgrundverordnung: „für die Beurteilung der Arbeitsfähigkeit der Beschäftigten verarbeitet werden“ anstatt „für die Beurteilung der Arbeitsfähigkeit erforderlich“. Zweitens wiederholt die Regelung den Verordnungstext, ohne spezifische Regelungen zu schaffen, die im Sinne der Normenklarheit erforderlich wären.

Um tatsächlich für die Beschäftigten vorhersehbare und bestimmte gesetzliche Regelungen zu schaffen, sollte geregelt werden, unter welchen Voraussetzungen, die Beurteilung der Arbeitsfähigkeit des Beschäftigten erforderlich ist. Eine medizinische Untersuchung zur Beurteilung der Arbeitsfähigkeit des Beschäftigten könnte beispielsweise durchgeführt werden, wenn bestimmte gesundheitliche Voraussetzungen eine wesentliche Anforderung darstellen, um die Tätigkeit ausüben zu können.

§ 24 HDSIG-E

In § 24 Absatz 3 HDSIG-E wird der Forschungs- und Statistikzweck nicht näher bestimmt bzw. kann in diesem für die allgemeine Verwaltung anzuwendenden Gesetz auch nicht näher bestimmt werden, da die relevanten Bereiche fehlen. Fraglich ist auch, welche berechtigten Interessen der betroffenen Person entgegenstehen können und wer darüber entscheidet. Hier müsste die betroffene Person gefragt werden bzw. einwilligen. Zudem muss der Begriff der Anonymisierung noch ausgelegt werden (siehe hierzu die Ausführungen unter § 2 Absatz 4 HDSIG-E).

§ 31 HDSIG-E :

Zu den Informationsplichten des zweiten Teils (§ 31 HDSIG-E) wird im Rahmen des HSOG-E Stellung genommen (siehe dort unter § 29 HSOG-E)

§ 34 HDSIG-E

Zu beachten ist, dass Artikel 18 Datenschutzgrundverordnung dem Betroffenen ein Recht auf Einschränkung der Verarbeitung gibt, aber diese Regelung in § 34 Absatz 1 als Recht des Verantwortlichen ausgestaltet ist. Dies geht über den Wortlaut des Artikel 18 Datenschutzgrundverordnung hinaus, insbesondere da nicht konkretisiert wird, aus welchem Grunde eine solche Beschränkung im Sinne von Artikel 23 erforderlich sein könnte.

§ 35 HDSIG-E

Dem Betroffenen stehen nach Artikel 21 Datenschutzgrundverordnung Widerspruchsrechte zu, die in § 35 HDSIG-E durch den unbestimmten Rechtsbegriff des „zwingenden öffentlichen Interesses“ eingeschränkt werden, aus dem sich allein jedoch nicht die Verhältnismäßigkeit dieser Regelung ableiten lässt. Dies gilt auch unter dem Gesichtspunkt, dass es sich um einen unionsrechtlichen Begriff handelt (siehe hierzu auch die obigen Ausführungen auf S. 9 und S. 53).

§ 40 HDSIG-E

Festzustellen ist, dass das Gesetz nicht das Ziel der Richtlinie (EU) Nr. 2016/680 wiedergibt, und damit auch nicht vorrangig den Charakter eines Gesetzes zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten innehat.

---

eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich.“

In Artikel der Richtlinie (EU) Nr. 2016/680 wird geregelt:

Diese Richtlinie enthält Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

In § 40 HDSIG-E heißt es indes:

Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Ordnungswidrigkeiten oder Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständigen öffentlichen Stellen. Dies gilt, soweit die öffentlichen Stellen zum Zwecke der Erfüllung dieser Aufgaben personenbezogene Daten verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche.

Hierbei wird anders als in der Richtlinie (EU) Nr. 2016/680 nicht der Schutz der personenbezogenen Daten bei der Datenverarbeitung in den Vordergrund gerückt, sondern die Möglichkeiten der Datenverarbeitung im Rahmen der genannten Zwecke. Im Rahmen eines Datenschutzgesetzes sollte aber der Zweck und Anwendungsbereich stets unmissverständlich und deutlich darauf abzielen, personenbezogene Daten bei der Datenverarbeitung schützen zu wollen.

Unklarheiten im Anwendungsbereich und in der Aufgabenzuweisung des HSOG-E ergeben sich darüber hinaus aus der weiteren Gesetzesbegründung im Hinblick auf § 40 HSOG-E. Im Sinne von § 1 Absatz 2 HSOG sind den allgemeinen Ordnungsbehörden Ahndung und Verfolgung von Ordnungswidrigkeiten zugewiesen.[32] Die Unklarheit, die sich aus der Gesetzesbegründung (S. 136) ergibt, ist die Formulierung der Aufgabenzuweisung: „*…die Datenverarbeitung bei Verwaltungsbehörden, deren Aufgabenzuweisung nicht mit den in § 40 HDSGI genannten Zwecken übereinstimmt…*“. Im Umkehrschluss stellt sich die Frage, ob Ordnungsbehörden, denen diese Aufgabe zugewiesen ist, immer unter den Anwendungsbereich fallen sollen. Wenn nun aber in einem konkreten Ordnungswidrigkeitsverfahren die Regelungen des OWIG gelten, was sich bereits aus der konkurrierenden Gesetzgebungskompetenz ergibt, stellt sich die Frage nach dem verbleibenden Anwendungsbereich und/oder ob der Gesetzgeber gegebenenfalls mangels abschließender Regelungen durch den Bundesgesetzgeber einen solchen Anwendungsbereich sieht.

Weiter heißt es in der Begründung „*Hieraus resultiert, dass die Datenverarbeitung bei Verwaltungsbehörden, deren Aufgabenzuweisung nicht mit den in § 40 HDSGI genannten Zwecken übereinstimmt, grundsätzlich solange und soweit nicht in den Anwendungsbereich der Richtlinie fällt, wie die von ihnen geführten Verwaltungsverfahren nicht in ein konkretes Ordnungswidrigkeitsverfahren übergehen*.“ Dementsprechend müssen Verwaltungsbehörden unter den Anwendungsbereich der Datenschutzgrundverordnung fallen. Das Verwaltungsverfahren wird durch die Überleitung in ein Bußgeldverfahren abgeschlossen. Die vorhergehende Sachverhaltsermittlung im Verwaltungsverfahren, etwa aufgrund einer Anzeige, darf damit nicht unter die Regelungen des §§ 40 HDSIG-E fallen, auch wenn diese Ermittlung noch ein konkretes Ordnungswidrigkeitsverfahren nach sich ziehen sollte. Im „vorgelagerten“ Verwaltungsverfahren

[32] Siehe die einschlägigen Verordnungen, etwa Verordnung über die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Waffengesetz.

müssen daher die Regelungen der Datenschutzgrundverordnung zur Anwendung gelangen, da ansonsten eine Beschränkung der Betroffenenrechte vorliegen würde.

Im Hinblick auf die Ordnungsbehörden, denen gemäß § 1 Absatz 2 HSOG die Ahndung und Verfolgung von Ordnungswidrigkeiten zugewiesen sein kann, ist daher zum einen fraglich, ob der Begriff der Ordnungswidrigkeiten tatsächlich von der Richtlinie (EU) Nr. 2016/680 gedeckt ist.[33] Zum anderen sollte der Gesetzgeber klarstellen, inwieweit er das von ihm vorgeschlagene Gesetz (§§ 40 ff. HDSIG-E) aufgrund der konkurrierenden Gesetzgebungsbefugnis des Bundes (OWIG) noch für anwendbar hält. Dies ist aus Transparenzgründen erforderlich. Im Übrigen wird auf die Ausführungen zum HSOG verwiesen, die sich gleichermaßen auf den Regelungsinhalt des § 40 HDSIG-E beziehen (siehe S. 44 ff.).

§ 44 HDSIG-E

§ 44 formuliert die Verarbeitung zu anderen Zwecken im Passiv. Satz 1 und Satz 2 unterscheiden sich nach der Gesetzesbegründung (S. 137) wie folgt: Verantwortliche dürfen gemäß Satz 1 personenbezogene Daten zu anderen Zwecken als zu denen sie ursprünglich erhoben wurden verarbeiten, solange es sich bei diesen anderen Zwecken um einen Zweck des § 40 HDSIG-E handelt. Satz 2 betrifft die Weiterverarbeitung von zu Zwecken des § 40 erhobenen Daten zu anderen als den dort genannten Zwecken, wenn sie in einer Rechtsvorschrift vorgesehen ist (z.B. § 22 HDSIG-E). Erhalten Ordnungsbehörden nun beispielsweise Daten auf der Grundlage von § 21 Absatz 1 Nr. 4 HDSIG-E, könnte § 44 HDSIG-E sicherstellen, dass diese Daten auch für Zwecke der Verfolgung von Ordnungswidrigkeiten rechtmäßig verarbeitet werden dürften. Allerdings wird hier erneut die unter § 40 HDSIG-E gestellte Frage relevant, inwieweit § 44 noch eine eigenständige Bedeutung neben den Regelungen des OWIG, aber auch des HSOG zukommt. Insgesamt sollte klar sein, dass Verwaltungsbehörden –anders als Polizeibehörden- nicht präventiv zur Ahndung von Ordnungswidrigkeiten tätig werden können, etwa durch „Ordnungswidrigkeitenvorsorge“ und in diesem Sinne Daten zweckändernd sammeln könnten (siehe auch die Ausführungen zum HSOG, S. 16 ff.).

§ 52 HDSIG-E:

Ausführungen zu den Rechten der Betroffenen erfolgen im Rahmen der Ausführungen zum HSOG (§ § 13 Absatz 6, 27, 29 HSOG- E).

§ 80 ff. HDSIG-E

Der Anspruch auf Informationszugang sichert die Rechte der betroffenen Personen, insbesondere auch im Hinblick auf ihr informationelles Selbstbestimmungsrecht. Zu begrüßen ist ebenso, dass die begehrten Informationen gemäß § 87 spätestens innerhalb eines Monats nach Eingang des Antrags zugänglich zu machen sind. Allerdings erfolgen keine Regelungen dazu, ob gegenüber dem Betroffenen eine Auskunft zu erteilen ist oder ihm die Informationsträger zugänglich zu machen sind. Die „nachteiligen Auswirkungen“ in § 82 Nr. 2 HDSIG-E werden im Übrigen nicht konkretisiert. In Bezug auf zum persönlichen Lebensbereich gehörenden Geheimnissen oder Betriebs- und Geschäftsgeheimnissen hätte der Anspruch im Übrigen davon abhängig gemacht werden können, ob überwiegende schutzwürdige Belange entgegenstehen oder dass eine Informationspflicht besteht, soweit das Informationsinteresse das Geheimhaltungsinteresse überwiegt.

[33] Siehe hierzu die Ausführungen auf S. 17 ff.

2. Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG-E)

Einleitung

- **Allgemein**

Das HSOG-E gilt für Gefahrenabwehrbehörden und Polizeibehörden. Subsidiär dazu gelten die Regelungen der §§ 40 ff. HDSIG-E, was vor allem durch Verweise auf diese Regelungen deutlich wird (siehe etwa § 27 HSOG-E, § 29 HSOG-E). §§ 40 ff. HDSIG-E setzen die Richtlinie (EU) Nr. 2016/680 um bzw. wiederholen den Wortlaut dieser Richtlinie in Form einer Verpflichtung für die öffentlichen Stellen. Bei Zwecken außerhalb des § 40 HDSIG-E sollen die Regelungen des zweiten Teils des HDSIG-E bzw. die Datenschutzgrundverordnung gelten.

Die Frage ist, ob für einen Bürger tatsächlich nachvollziehbar ist, unter welchen Voraussetzungen, die §§ 40 ff. HDSIG-E oder die Regelungen der Datenschutzgrundverordnung bzw. die Regelungen des zweiten Teils des HDSIG-E zur Anwendung gelangen. Gesetze sollten jedoch verständlich sein. So muss im Rahmen des HSOG etwa innerhalb der gleichen Regelung entschieden werden,[34] ob die Erhebung personenbezogener Daten für Zwecke der §§ 40 ff. bzw. der Richtlinie (EU) Nr. 2016/680 oder für Zwecke erfolgt, die von der Datenschutzgrundverordnung gedeckt sind. Die Zulässigkeit der gesetzlichen Regelung wird beispielsweise im Rahmen des § 13 HSOG-E inhaltlich begründet und sowohl im Rahmen der Richtlinie (EU) Nr. 2016/680 als auch im Rahmen der Datenschutzgrundverordnung bejaht.[35] Eine solche Begründung und Unterscheidung zwischen den Zwecken der Richtlinie (EU) Nr. 2016/680 und der Datenschutzgrundverordnung erfolgt hingegen bei der Regelung des § 20 HSOG-E nicht entsprechend, die im Übrigen nur für nach §§ 13 ff. HSOG (Befugnisnormen) erhobene Daten in Betracht kommen kann.[36]

Im Übrigen muss bei der Umsetzung der Richtlinie (EU) Nr. 2016/680 berücksichtigt werden, dass der Begriff der „öffentlichen Sicherheit“ als unionsrechtlicher Begriff nicht automatisch mit dem Begriff aus dem deutschen Polizei- und Ordnungsrecht gleichzusetzen ist. Es handelt sich um einen Begriff des Gemeinschaftsrechts, der selbstständig ausgelegt werden muss, so dass zweifelhaft ist, ob hier tatsächlich ein Rückgriff auf die Definition nach deutschem Polizei- und Ordnungsrecht zulässig ist.[37] Der EuGH hat den Begriff der „öffentlichen Sicherheit“ für eine Einschränkung der Grundrechte näher ausgeformt.[38] Gemäß dieser Ausführungen muss eine tatsächliche und hinreichende schwere Gefährdung vorliegen, die ein Grundinteresse der Gesellschaft berührt, wobei beispielhaft als solches Grundinteresse die Grundversorgung mit Dienstleistungen von strategischer Bedeutung oder allgemeinen Interesse genannt wird (Erdölprodukte, Elektrizität oder Telekommunikation). [39] Aus diesem Grunde muss eine Prüfung im Besonderen dahingehend erfolgen, ob der Begriff der Straftat, einschließlich der Abwehr von Gefahren für die öffentliche Sicherheit, pauschal auf sämtliche Ordnungswidrigkeiten erweitert werden kann und damit gleichzeitig die Ziele der Richtlinie (EU) Nr.

[34] Siehe etwa § 13 HSOG-E und Begründung, S. 208 ff.
[35] Siehe S. 209 der Gesetzesbegründung.
[36] Siehe hierzu die Ausführungen zu § 20 HSOG-E.
[37] Frenz, Handbuch Europarecht Band 4: Europäische Grundrechte, Rn. 4666 im Rahmen der Ausführungen zur Transparenzverordnung unter Verweis auf Frenz, Europarecht 1, Rn. 943 und 2833.
[38] Frenz, aaO Rn. 4667.
[39] Frenz, aaO Rn. 4667.

2016/680 auf Aufgaben der Verwaltung zur Gefahrenabwehr auszudehnen (siehe hierzu die folgenden Ausführungen).

- **Ordnungswidrigkeit**

Ausweislich der Gesetzesbegründung (S. 136) soll der Begriff der Ordnungswidrigkeit von der Richtlinie (EU) Nr. 2016/680 erfasst sein, was zu einer Erweiterung der Befugnisse der Behörden im Rahmen der subsidiär geltenden §§ 40 ff. HDSIG-E als auch des HSOG beiträgt. Gemäß § 1 Absatz 2 HSOG ist den allgemeinen Ordnungsbehörden die Ahndung und Verfolgung von Ordnungswidrigkeiten zugewiesen. Wird nun die Richtlinie (EU) Nr. 2016/680 auf Behörden erweitert, denen die Ahndung und Verfolgung von Ordnungswidrigkeiten zugewiesen ist, kann damit auch die Beschränkung der Rechte der Betroffenen verbunden sein (da diese Richtlinie andere Zwecke und Ziele verfolgt als die Datenschutzgrundverordnung).

In diesem Zusammenhang stellt sich zum einen die Frage nach der Gesetzgebungskompetenz, da unklar ist, inwieweit dem hessischen Landesgesetzgeber im Rahmen eines Ordnungswidrigkeitenverfahrens und der konkurrierenden Gesetzgebung des Bundes noch die Regelungskompetenz zustehen kann.[40] Zum anderen ist gemäß Erwägungsgrund 13 der Richtlinie (EU) Nr. 2016/680 eine Straftat im Sinne dieser Richtlinie ein eigenständiger Begriff des Unionsrechts, der durch den Gerichtshof der Europäischen Union auszulegen ist. Die Gesetzesbegründung (S. 136) beruft sich zwar ebenso auf diesen Erwägungsgrund, legt den Begriff der Straftat dennoch weit aus und erweitert ihn ebenso auf Ordnungswidrigkeiten. Zu berücksichtigen ist, dass einer Ordnungswidrigkeit kein Strafcharakter zukommt. Allerdings wird ebenso darauf verwiesen, dass nicht alle EU-Mitgliedstaaten über ein dem deutschen Ordnungswidrigkeitenrecht vergleichbares Recht der Verwaltungssanktionen verfügen und daher der Straftatenbegriff auch Ordnungswidrigkeiten mit einschließen müsse.[41] Zu beachten ist trotzdem das Ungleichgewicht zwischen Ordnungswidrigkeiten und Straftaten. Der Grundsatz der Verhältnismäßigkeit erfordert gerade, dass im Zusammenhang mit Strafverfahren gewährte Eingriffsbefugnisse nicht oder nur mit Einschränkungen im OWIG-Verfahren zu gewähren sind. Im Übrigen muss dies durch gesetzliche Regelungen, aus denen sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben.[42] Zudem ergibt sich aus der Richtlinie (EU) Nr. 2016/680 und dem in Erwägungsgrund 11 ebenfalls vorgenommenen Bezug auf die öffentliche Sicherheit, dass es sich um höherrangige Werte handeln sollte als um „Verwaltungsunrecht“.[43] Vor allem sollte der Verhältnismäßigkeitsgrundsatz bei der Umsetzung berücksichtigt werden, da das Recht auf informationelle Selbstbestimmung bei Ordnungswidrigkeiten mehr Raum einnehmen muss als bei Regelungen, die sich auf Straftaten beziehen. Das Bußgeldverfahren hat geringere Bedeutung.

- **Aufgabenzuweisung**

Die gerade gemachten Ausführungen sind auch aus dem Grunde wichtig, da in der Gesetzesbegründung (S. 136) formuliert ist, dass die Verhütung, Ermittlung, Verfolgung, Ahndung und Vollstreckung von Ordnungswidrigkeiten vom Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 auch ohne deren ausdrückliche Aufführung in Art. 1 Abs. 1 umfasst ist, so dass der Begriff

[40] Siehe hierzu die Ausführungen zu §§ 40 ff. HDSIG-E auf S. 13 ff.
[41] Hörauf, ZIS 2013, S. 276 ff., 278 ff.
[42] Hier bestehen etwa bei § 20 HSOG-E Zweifel, siehe die dortigen Ausführungen.
[43] Siehe die allgemeinen Ausführungen oben auf S. 15.

der Ordnungswidrigkeit in § 40 Abs. 1 ausdrücklich genannt werden kann. Dies schließe auch hierauf bezogene Gefahrenabwehrzwecke wie im HSOG ein. In diesem Sinne sollen die Regelungen der Richtlinie (EU) Nr. 2016/680 im Bereich der Gefahrenabwehr gelten, *wenn die Behörden die Datenverarbeitung zum Zwecke der auf die Verhütung von Straftaten oder Ordnungswidrigkeiten bezogenen Gefahrenabwehr vornehmen und eine solche gesetzliche Aufgabenzuweisung besteht* (S. 136 Gesetzesbegründung).

Eine entsprechende Aufgabenzuweisungsnorm ist in § 1 HSOG verankert. Diese nimmt allerdings dahingehend eine Trennung vor, dass gemäß § 1 Absatz 4 HSOG lediglich Polizeibehörden zur Verhütung von Straftaten befugt sind (nicht allgemeine Verwaltungsbehörden). Im Sinne von § 1 Absatz 2 HSOG können den allgemeinen Ordnungsbehörden zwar die Ahndung und Verfolgung von Ordnungswidrigkeiten zugewiesen sein.[44] Im letzteren Fall finden jedoch im Rahmen der Ahndung und Verfolgung von Ordnungswidrigkeiten in einem Ordnungswidrigkeitenverfahren aufgrund der konkurrierenden Gesetzgebungsbefugnis des Bundes die Regelungen des Ordnungswidrigkeitengesetzes Anwendung. Daher ist fraglich, welche Tätigkeiten der Verwaltungsbehörden nach der Intention des Gesetzesentwurfs in den Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 und der entsprechenden Umsetzung im HSOG fallen sollen. Wollte man den Anwendungsbereich auf Gefahrabwehrbehörden erweitern, müsste konsequenterweise auch die Aufgabenzuweisungsnorm des § 1 HSOG erweitert werden. Anderenfalls würden die unterschiedlichen Aufgaben der Polizeibehörden und der Gefahrabwehrbehörden vermengt: Nur der Polizei stehen im Rahmen der Gefahrenabwehr gemäß § 1 Absatz 4 HSOG die Aufgabe zugewiesen, zu erwartende Straftaten zu verhüten. Ansonsten bedeutet Gefahrenabwehr, die Abwehr einer bestehenden **konkreten** Gefahr für die öffentliche Sicherheit und Ordnung (siehe § 11 HSOG als Befugnisnorm). Die Verhütung von Straftaten oder Ordnungswidrigkeiten ist hierbei nicht Tatbestandsvoraussetzung. Die Gefahr kann natürlich auch in der Verhütung einer drohenden Straftat oder Ordnungswidrigkeit liegen. Dann stellt sich aber dennoch die Frage, inwieweit der repressive Bereich beschritten ist, da die „Verbrechensbekämpfung“ in diesem Falle nicht vorbeugend sondern ganz konkret ist.

Fraglich ist daher, wie die Formulierung in der Gesetzesbegründung (S. 136) „*wenn die Behörden die Datenverarbeitung zum Zwecke der auf die Verhütung von Straftaten oder Ordnungswidrigkeiten bezogenen Gefahrenabwehr vornehmen und eine solche gesetzliche Aufgabenzuweisung besteht*“ im Einzelfall zu verstehen ist und inwieweit damit Verwaltungsbehörden, die gemäß §§ 2, 82 HSOG die primäre Zuständigkeit für Aufgaben der Gefahrenabwehr innehaben, und/oder Ordnungsbehörden unter den Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 und die §§ 40 ff. HDSIG-E fallen sollen. Diese Frage ist vor allem auch unter dem Gesichtspunkt der konkurrierenden Gesetzgebungskompetenz des Bundes zu stellen.

Insgesamt ist, wie gerade ausgeführt, zu berücksichtigen, dass für Gefahrenabwehrbehörden die grundsätzliche Zuweisung im HSOG fehlt, entsprechend der Polizei im Rahmen der Gefahrenabwehr Ordnungswidrigkeiten zu verhüten. Dies gilt, auch wenn etwa in § 20 Absatz 2 HSOG-E den Gefahrenabwehrbehörden allgemein die Möglichkeit zugesprochen wird, erhobene Daten zur Verhütung von Ordnungswidrigkeiten weiterzuverarbeiten, da eine Aufgabenzuweisung nicht durch

[44] Siehe die einschlägigen Verordnungen, etwa Verordnung über die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Waffengesetz.

„spätere“ Befugnisnormen zur Erhebung von Daten (siehe §§ 13 ff. HSOG) oder Ermächtigungsgrundlagen (z.B. § 20 HSOG) für eine zulässige Verarbeitung von erhobenen Daten geschaffen werden kann. Anderenfalls müssten konsequenterweise lediglich Polizeibehörden unter den Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 fallen.

Ansonsten muss die Datenverarbeitung der Verwaltungsbehörden nach der Datenschutzgrundverordnung erfolgen. In Artikel 6 Absatz 1e), Absatz 3 DSGVO ist die Möglichkeit der Mitgliedstaaten geregelt, spezifische zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beizubehalten oder einzuführen, indem sie Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten. Gemäß Artikel 6 Absatz 1e) DSGVO ist eine Verarbeitung rechtmäßig, wenn diese für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Zu berücksichtigen ist, dass es sich bei dem öffentlichen Interesse ebenso um einen Begriff des Unionsrechts handelt, bei dem zusätzlich zu prüfen ist, inwieweit der deutsche Gesetzgeber diesen definieren oder konkretisieren kann.[45] Allerdings muss bei der Umsetzung der einzelnen Regelungen im HSOG-E stets der Verhältnismäßigkeitsgrundsatz beachtet werden und das im öffentlichen Interesse verfolgte Ziel muss in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen. Es müsste zumindest ein berechtigtes Interesse im Sinne des Gemeinschaftsrechts vorliegen, das geeignet ist, die Maßnahme zu rechtfertigen, und dadurch die ebenfalls nach Gemeinschaftsrecht bestehenden Rechte der betroffenen Personen zulässigerweise einzuschränken.

Dies soll nicht heißen, dass die Datenverarbeitung durch Verwaltungsbehörden zum Zwecke der Gefahrenabwehr nicht gesondert im HSOG geregelt werden könnte. Es sollten nur Unklarheiten vermieden werden, die sich durch die unterschiedlichen Zielrichtungen der Richtlinie (EU) Nr. 2016/680 und der Datenschutzgrundverordnung ergeben.

Zu den einzelnen Regelungen:

§ 3 Absatz 4 HSOG-E

Mit § 3 Absatz 4 HSOG-E soll die Aussage getroffen werden, dass die Vorschriften des HSOG-E keine Anwendung finden, soweit das Recht der Europäischen Union, insbesondere die Verordnung (EU) Nr. 2016/679, Anwendung finden. Gemäß der Begründung (S. 208) soll dabei der Verordnung (EU) Nr. 2016/679 unmittelbare Geltung zukommen. Die Formulierung „unmittelbare Geltung“ darf nicht mit dem Begriff eines Geltungsvorrangs verknüpft werden.

Wie gerade dargestellt sollen zudem der dritte Teil des HDSIG-E (§§ 40 ff.), aber auch der zweite Teil des HDSIG-E und die Datenschutzgrundverordnung gelten. Bei Datenverarbeitungen ohne jeglichen Straftaten- oder Ordnungswidrigkeitenbezug sollen die Regelungen der Datenschutzgrundverordnung und die ihrer Durchführungen dienenden Vorschriften des zweiten

[45] Beim Begriff der öffentlichen Ordnung wurde vom EUGH im Zusammenhang mit der Einschränkung des freien Dienstleistungsverkehrs ein gewisser Auslegungsspielraum anerkannt, siehe Urteil des Gerichtshofes vom 14.Oktober 2004, Rechtssache C-36/02.

Teils des HDSIG-E gelten (Begründung, S. 208). Dennoch wird im HSOG-E pauschal auf die Gefahrenabwehrbehörden, etwa auch in § 20 HSOG-E, Bezug genommen. Teilweise wird lediglich, wie etwa in § 13, begründet, warum die entsprechende Regelung sowohl der Datenschutzgrundverordnung als auch der Richtlinie (EU) Nr. 2016/680 entspricht. Insgesamt darf dies - wie in den obigen Ausführungen bereits formuliert – nicht zu Unklarheiten führen.

§ 13 HSOG-E

Bei der Einwilligungsmöglichkeit ist Erwägungsgrund 35 der Richtlinie (EU) Nr. 2016/680 zu berücksichtigen:

….

Bei der Wahrnehmung der ihnen als gesetzlich begründeter Institution übertragenen Aufgaben, Straftaten zu verhüten, zu ermitteln, aufzudecken und zu verfolgen, können die zuständigen Behörden natürliche Personen auffordern oder anweisen, ihren Anordnungen nachzukommen. ***In einem solchen Fall sollte die Einwilligung der betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen. Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann****.*

Hier ist sicherzustellen, dass es bei der Beurteilung der Freiwilligkeit nicht nur darum geht, auf den gemäß § 46 Absatz 4 HSOG-E vorgesehenen Zweck der Verarbeitung hinzuweisen, sondern die betroffene Person auch darüber zu informieren, inwieweit eine Speicherung, Übermittlung oder Weiterverarbeitung geplant ist. Die betroffene Person ist damit nicht nur auf die Freiwilligkeit hinzuweisen, sondern auf alle damit zusammenhängenden Umstände, die gerade durch eine mögliche Weiterverarbeitung ihrer Daten besondere Eingriffsintensität erhalten.

§ 13 Absatz 5 HSOG-E

Die Streichung der ursprünglichen Klarstellung, dass Daten nicht zu unbestimmten oder noch nicht bestimmten Zwecken, erhoben werden dürfen, ist im Sinne der Gesetzeslogik und mit Blick auf die Möglichkeiten der Weiterverarbeitung gemäß § 20 HSOG-E zwar konsequent. Die Aufrechterhaltung dieser Regelung im Gesetzestext hätte jedoch eine warnende Funktion erfüllen können. Ein Verstoß gegen diese Regelung würde stets ein Verwertungsverbot nach sich ziehen, was hinsichtlich einer möglichen Weiterverarbeitung von Daten besonders relevant ist. Im Sinne der Sicherung des informationellen Selbstbestimmungsrechts sollte die Formulierung eines strengen Zweckbindungsgrundsatzes weiter erhalten bleiben.

§ 13 Absatz 6 HSOG-E

Zunächst ergibt sich aus der Gesetzesbegründung nicht eindeutig, inwieweit die zweite Alternative in Nr. 1 (mutmaßliche Einwilligung) der ursprünglichen Fassung aufrechterhalten werden soll oder weiterhin hineininterpretiert werden soll, da in diesem Falle eine Ausnahme von der Direkterhebung erfolgt.

Weiterhin ist fraglich (insbesondere mit Blick auf § 13 Absatz 6 Satz 2, der wohl bestehen bleiben soll), wie die Information des Betroffenen im Einzelfall erfolgen soll, sobald die Maßnahme dadurch nicht mehr gefährdet wird. Im aktuellen HSOG besteht diese Verpflichtung über § 12 Absatz 5 HDSG.

Bei der Verarbeitung für Zwecke §§ 40 ff. HDSIG-E bzw. der Richtlinie (EU) Nr. 2016/680 erfolgt diese Verpflichtung über § 29 Absatz 1 HSOG-E iVm § 51 HDSIG-E. Dies gilt aber auch nur für den Fall, sofern man im Sinne von § 51 HDSIG-E unterstellt, bei § 29 Absatz 1 HSOG handelt es sich um eine solche genannte spezielle Rechtsvorschrift, die eine Benachrichtigung vorsieht. In diesem Falle fehlen jedoch gemäß Artikel 12 Richtlinie (EU) Nr. 2016/680 konkrete Regelungen dahingehend, dass dem Betroffenen die Informationen in präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und in einer geeigneten Form (etwa auch elektronisch) zu übermitteln sind. Die Regelungen in § 50 HDSIG-E beziehen sich lediglich auf allgemeine Informationen für jedermann, aber nicht speziell für den hier vorliegenden Sachverhalt. Es ist daher fraglich, ob mit den Regelungen in § 50 HDSIG-E tatsächlich die Vorgabe des Richtliniengebers in gemäß Artikel 12 Richtlinie (EU) Nr. 2016/680 ausreichend umgesetzt ist, nach der die Mitgliedstaaten vorsehen, dass der Verantwortliche alle angemessenen Maßnahmen trifft, um der betroffenen Person alle Informationen gemäß Artikel 13 sowie alle Mitteilungen gemäß den Artikeln 11, 14 bis 18 und 31, die sich auf die Verarbeitung beziehen, in präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, wozu etwa auch die elektronische Form zählen kann.

Hier hätte beispielsweise im Sinne einer transparenten Gestaltung unmittelbar in § 13 HSOG-E geregelt werden können, dass die betroffene Person zu informieren ist, sobald die Maßnahme nicht mehr gefährdet wird.

Im Sinne einer einheitlichen Terminologie sollte an dieser Stelle außerdem nicht der Begriff „Benachrichtigung“ verwendet werden, sondern „Information“. „Benachrichtigung“ wird von Artikel 31 der Richtlinie (EU) Nr. 2016/680 verwendet, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Für Zwecke außerhalb der §§ 40 ff HDSIG-E enthält § 32 HDSIG-E die entsprechende Informationsplicht, wobei hier anzumerken ist, dass der Begriff in § 32 Absatz 1 Nr. 2 HDSIG-E geregelte Begriff der öffentlichen Ordnung in der Datenschutzgrundverordnung nicht verwendet wird und der Begriff „öffentlichen Sicherheit“ (siehe auch § 51 Absatz 2 HDSIG-E) im Übrigen einen unionsrechtlichen Begriff darstellt, der nicht automatisch mit materiellem Polizeirecht gleichzusetzen ist.[46]

§ 13 Absatz 8 HSOG-E

Dieser Absatz ist im Laufe der vergangenen Gesetzgebungsverfahren immer weiter gekürzt worden. Zwar sollen gemäß der Gesetzesbegründung (S. 210) § 29 Absatz 1 und Absatz 2 HSOG-E Anwendung finden. Dennoch wäre aus Transparenzgründen an dieser Stelle eine Regelung vorteilhaft, die konkret auf die Verpflichtung zur Information Bezug nimmt. So hätte positiv formuliert werden können, dass über sämtliche Zwecke, Speicherung, Weiterverarbeitung zu informieren ist, auch etwa über die Verarbeitung in polizeilichen Verbundsystemen.

Für Zwecke der Richtlinie (EU) Nr. 2016/680 können die Mitgliedstaaten gemäß Artikel 13 Absatz 3 Gesetzgebungsmaßnahmen erlassen, nach denen die Unterrichtung der betroffenen Person gemäß Absatz 2 soweit und solange aufgeschoben, eingeschränkt oder unterlassen werden kann, wie diese Maßnahme in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und sofern den

[46] Siehe hierzu auch die obigen Ausführungen zur „öffentlichen Sicherheit“, S. 15.

Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird.[47] Unterstellt, dass § 29 Absatz 1 HSOG eine spezielle Rechtsvorschrift darstellen soll, die eine Benachrichtigung anordnet, wäre § 51 Absatz 2 HDSIG-E einschlägig. Diese Regelung enthält aber weder Voraussetzungen für die Art und Weise der Unterrichtung (siehe hierzu bereits die obigen Ausführungen unter § 13 Absatz 6), noch sind Regelungen dazu getroffen, ob die Gründe festgehalten werden müssen oder dass bei vorübergehenden Hinderungsgründen die Information innerhalb einer angemessenen Frist nachzuholen wäre, was im Sinne der oben geforderten Verhältnismäßigkeit angebracht wäre.

Außerhalb der Zwecke der Richtlinie enthält § 31 Absatz 2, 3 HDSIG-E eine entsprechende Regelung, die über den Verweis in § 29 HSOG-E Anwendung findet.

§ 15 Absatz 6 HSOG-E

Durch die aktuelle Änderung im HSOG-E werden der Zweckbindungsgrundsatz und die Anforderungen an die Verhältnismäßigkeit beschränkt, da die enge Ausnahme der Verarbeitung für Zwecke der unerlässlichen Abwehr für Leib, Leben oder Freiheit nun umformuliert wurde und „Erkenntnisse zum Zwecke der Gefahrenabwehr“ verwertet werden dürfen. Der Begriff der Verwertung ist an dieser Stelle unklar und nicht näher begründet. Im Sinne einer einheitlichen Terminologie sollte daher weiterhin der Begriff „Verarbeitung“ verwendet werden. Im Übrigen stellt sich die Frage nach der Verhältnismäßigkeit der Verarbeitung im Einzelfall, wenn nun der Maßstab „Leib, Leben oder Freiheit“ nicht mehr die gesetzliche Voraussetzung darstellt.

§ 20 HSOG-E

Absatz 1 und Absatz 2

In § 20 HSOG-E sind neben Polizeibehörden pauschal Gefahrenabwehrbehörden genannt. Unter der Maßgabe, dass daher § 20 für alle Gefahrenabwehrbehörden gilt und nicht nur für diejenigen, denen die Vollstreckung und Ahndung von Ordnungswidrigkeiten gemäß § 1 Absatz 2 HSOG zugewiesen ist, muss diese Regelung sowohl der Richtlinie (EU) Nr. 2016/680 als auch den Grundsätzen der Datenschutzgrundverordnung entsprechen bzw. unter Anwendung der Regelungen der Datenschutzgrundverordnung als rechtmäßige Datenverarbeitung gelten.[48] Insgesamt wird aufgrund der Regelung in § 20 Absatz 2, 5 HSOG-E nicht zwischen den Befugnissen zur Datenerhebung zur Gefahrenabwehr und vorbeugenden Bekämpfung von Straftaten unterschieden, da sowohl Gefahrenabwehrbehörden als auch Polizeibehörden Daten zur Verhütung von Ordnungswidrigkeiten verarbeiten können. Eine konkrete Gefahr im Sinne von § 11 HSOG ist nicht erforderlich. So wird außerdem in § 20 Absatz 2 Nr. 2b) HSOG-E „*eine drohende Gefahr in einem übersehbaren Zeitraum*“ für ausreichend erachtet. Auch diese Formulierung ist weniger als eine konkrete Gefahr. Die Gesetzesbegründung beschreibt dies selbst „als eine in ersten Umrissen absehbare und konkretisierte Möglichkeit eines Schadenseintrittes“ (S. 214).

---

[47] Konkret: *zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden, zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, zum Schutz der öffentlichen Sicherheit, zum Schutz der nationalen Sicherheit sowie zum Schutz der Rechte und Freiheiten anderer*.

[48] Dies gilt unter der unterstellten Annahme, dass die Richtlinie (EU) Nr. 2016/680 auf Ordnungswidrigkeiten überhaupt anwendbar ist, siehe S. 15 ff. unter Ordnungswidrigkeiten.

Konsequenterweise können allerdings die Regelungen des § 20 Absatz 1 Nr. 2, Absatz 2 Nr. 1a), Nr. 2a) HSOG-E, die sich explizit auf die Verhütung von Ordnungswidrigkeiten beziehen, nur für Ordnungsbehörden gelten, denen kraft Aufgabenzuweisung des § 1 Absatz 2 HSOG die Ahndung und Vollstreckung von Ordnungswidrigkeiten bereits zugewiesen ist. Nur diese Behörden könnten überhaupt mit den erhobenen Daten vergleichbare Ordnungswidrigkeiten verhüten. Dies ist in dieser Form im Gesetz aber nicht klar benannt. Anderenfalls würde sich diese Ermächtigungsgrundlage, die die Durchführung der Datenverarbeitung regelt, zu einer Aufgabenzuweisungsnorm umwandeln, sofern davon auch Verwaltungsbehörden erfasst würden und ihnen die Verhütung von Ordnungswidrigkeiten erlaubt wäre. Auch in der Begründung (S. 136) ist geregelt, dass die Verarbeitung allein zu diesen Zwecken nicht ausreicht, sondern auch eine Aufgabenzuweisung (Zuständigkeit) zu Richtlinienzwecken vorliegen muss. § 20 HSOG-E kann jedoch insoweit keine Aufgabenzuweisungsnorm darstellen, da darin lediglich die Ermächtigung für die Weiterverarbeitung von Daten geregelt ist, nachdem diese bereits erhoben worden sind.

Ansonsten wäre für Verwaltungsbehörden fraglich, ob und unter welchen Voraussetzungen eine Weiterverarbeitung der Daten, die für die Abwehr einer konkreten Gefahr erhoben wurden, für vergleichbar bedeutsame Rechtsgüter überhaupt erforderlich und verhältnismäßig wäre (§ 20 Absatz 2 Nr. 1a) HSOG-E). In diesem Sinne müsste eigentlich von der betroffenen Person weiterhin eine konkrete Gefährdung ausgehen.

Für die Polizeibehörden und Ordnungsbehörden stellt sich aber dennoch zusätzlich die Frage nach dem verbleibenden Anwendungsbereich unter dem Blickwinkel der konkurrierenden Gesetzgebung.

Wenn eine drohende Straftat oder Ordnungswidrigkeit verhindert/verhütet werden soll, ist diese Bekämpfung nicht vorbeugend gemäß § 1 Absatz 4 HSOG, sondern ganz konkret, so dass es sich um eine repressive Maßnahme handelt (StPO). Es könnten allenfalls Maßnahmen der Strafverfolgungsvorsorge für Polizeibehörden in Betracht kommen,[49] aber nur wenn auch festgestellt wird, dass der Betroffene in den Kreis Verdächtiger einer noch anderen strafbaren Handlung einbezogen werden könnte und die erkennungsdienstlichen Unterlagen die dann zu führenden Ermittlungen fördern könnten.[50]

Berücksichtigt werden muss jedoch einerseits, dass § 1 Absatz 4 HSOG nur für Polizeibehörden (und nicht für Verwaltungs-/Ordnungsbehörden) und nur für Straftaten Anwendung findet. Andererseits wird durch § 20 HDSOG-E die Möglichkeit eröffnet, präventiv zur Ahndung von Ordnungswidrigkeiten tätig werden zu können, quasi im Sinne einer „Ordnungswidrigkeitenvorsorge“ und in diesem Sinne Daten zu sammeln. Auch hier muss besonderes Augenmerk auf die Frage der Verhältnismäßigkeit gelegt werden, zumal keine Regelungen im Zusammenhang mit den konkreten Personen getroffen wurden, die von der Weiterverarbeitung betroffen sind, sondern die Zulässigkeit von der Vergleichbarkeit der Rechtsgüter abhängig gemacht wird.

In diesem Zusammenhang muss zwar berücksichtigt werden, dass sich der Gesetzesentwurf des HSOG am BKAG-Gesetz und der Rechtsprechung des Bundesverfassungsgerichts orientiert.[51] Der Begriff der Weiterverarbeitung wird hier entsprechend der Begriffsbestimmung des BKAG-Gesetzes

[49] Hier könnte etwa § 81b 2. Alt. StPO als Regelung in Betracht, die trotz ihrer Stellung in der StPO dem materiellen Polizeirecht zugewiesen wird.
[50] BVerwG , Urteil vom 23.11.2005, Az. 6 C 2.05.
[51] BVerfG, Urteil vom 20.04.2016, 1 BvR 966/09.

weit ausgelegt. Demnach sind darunter die Speicherung, die Organisation, das Ordnen, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, der Abgleich oder die Verknüpfung von Daten zu verstehen.[52] Es fehlt allerdings eine Entscheidung, ob die hypothetische Datenneuerhebung tatsächlich als allgemeiner Grundsatz vertretbar ist, da das Bundesverfassungsgericht seine Ausführungen im Zusammenhang mit terroristischen Aktivitäten getätigt hat. Eine Rechtsprechung zu dem hier zu regelnden Sachverhalt ist noch nicht erfolgt. Im Rahmen der Generalklausel des § 20 HSOG-E sollen nun Ordnungswidrigkeiten ausreichen und eine Weiterverarbeitung möglich sein, auch wenn es nicht um die Verletzung schwerwiegender bzw. hochrangiger Rechtsgüter geht, wie diese der Entscheidung des Bundesverfassungsgerichts im Zusammenhang mit der Strafverfolgung von terroristischen Anschlägen zugrunde liegt. Die zu schützenden Rechtsgüter lassen sich damit aus dem Regelungszusammenhang ableiten. Dies ist beim HSOG-E nicht möglich, so dass hier die Benennung konkreter Rechtsgüter erfolgen müsste und nicht nur die Vergleichbarkeit von Rechtsgütern, Straftaten oder Ordnungswidrigkeiten. Erst aus der Gesetzesbegründung (S. 212) lässt sich ermitteln, dass damit ebenso gemeint ist, dass eine „Lebensgefahr“ mit einer „Freiheitsgefahr“ vergleichbar ist oder eine Gefahr für Leib und Leben ebenso mit dem Eigentumsschutz vergleichbar sein soll. Es hätten allerdings im Gesetzestext selbst ganz klare Vorgaben im Hinblick auf zu schützende Rechtsgüter und Straftaten gemacht werden können. Hier könnten für die betroffenen Person nicht absehbare Verknüpfungen vorgenommen werden, die im Übrigen Maßnahmen betreffen, die sich alle noch im Bereich der Gefahrenabwehr bzw. Strafverfolgungsvorsorge und noch nicht im Bereich der Strafverfolgung befinden, da hier die Gesetzgebungskompetenz fehlt, wie die Gesetzesbegründung selbst hervorhebt (S. 212). Es fehlen gesetzliche Regelungen dahingehend, inwieweit welche Informationen, die im Rahmen der Vorsorge für die Verfolgung **zukünftiger Straftaten** erhoben werden, tatsächlich weiterverarbeitet werden dürfen.[53]

Insgesamt ergeben sich daher Zweifel an der Bestimmtheit und Verhältnismäßigkeit. Die Grenzziehung wird hier mehr oder weniger dem Ermessen der Behörden überlassen. Diese Regelungen beziehen sich darüber hinaus gemäß § 20 Absatz 5 auf sämtliche Personen gemäß § 13 HSOG, auch auf Zeugen und Hinweisgeber. Dabei geht es stets darum, bei zukünftigen Verfahren bessere Ermittlungsansätze zu haben, so dass durch die gesammelten Informationen die spätere Aufklärung anderer Straftaten oder Ordnungswidrigkeiten erleichtert wird. Dabei ist wie gesagt fraglich, ob es sich bei dieser Tätigkeit nicht (doch) um eine Aufgabe der Erforschung und Aufklärung von Straftaten handelt und damit dem repressiven Bereich der Strafverfolgung zuzuordnen ist, für den der Bund die konkurrierende Gesetzgebungszuständigkeit gemäß Art. 74 Abs. 1 Nr. 1 GG hat.

Insgesamt erlaubt diese Regelung eine Weiterverarbeitung als Datenabgleich oder Datenverknüpfung, ohne dass eine Zweckbindung erforderlich wäre. Die betroffene Person kann gerade nicht hinreichend deutlich erkennen, bei welchen Anlässen und unter welchen Voraussetzungen ihr Verhalten zu einer Weiterverarbeitung führt. Die Daten Betroffener könnten mit unterschiedlichen Ereignissen verknüpft werden. Letztendlich könnte dies auch mit Blick auf die polizeilichen Verarbeitungssysteme für die betroffene Person zu einer Datensammlung führen, die

[52] Gesetzesbegründung S. 208 – davon abzugrenzen ist die Datenerhebung, die Datenübermittlung, die Einschränkung der Datenverarbeitung und das Löschen der Daten.
[53] Siehe zu den erkennungsdienstlichen Maßnahmen gemäß § 81b 2. Alt. StPO die obigen Ausführungen.

sie rein praktisch nicht mehr durchschauen kann (siehe hierzu die Ausführungen unter § 20 Absatz 6 HSOG-E).

Die Erforderlichkeit und Verhältnismäßigkeit dieser gesetzlichen Regelung, die sowohl gemäß Artikel 4 Absatz der Richtlinie (EU) Nr. 2016/680 als auch gemäß Artikel 6 Absatz 4 Datenschutzgrundverordnung erforderlich ist, wird pauschal unterstellt, ohne dass dazu nochmals detaillierte Regelungen getroffen oder die ursprüngliche Entscheidung des Bundesverfassungsgerichts, welche auf terroristische Aktivitäten und „hinreichend gewichtige Rechtsgüter" abstellt, besondere Berücksichtigung finden würden. Auch in der Gesetzesbegründung lässt der Gesetzgeber die Vereinbarkeit mit der Richtlinie (EU) Nr. 2016/680 und der Datenschutzgrundverordnung offen. Gemäß letzterer ist im Sinne von Artikel 6 Absatz 1e) Datenschutzgrundverordnung eine Verarbeitung rechtmäßig, wenn diese für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Bei den Regelungen des § 20 HSOG-E sollte daher kritisch überprüft werden, ob die Anforderungen erfüllt sind, die an ein transparentes, normenklares Gesetz zu stellen sind.

§ 20 Absatz 6 HSOG-E

Der Begriff der „gewonnenen Daten" entstammt nicht der Richtlinie (EU) Nr. 2016/680, sondern dem aktuellem Gesetzestext des HSOG. Nach derzeitigem Recht sollen damit erhobene, aufgedrängte Informationen (ohne Aufforderung angegebene Daten) oder in sonstiger Weise erlangte Daten (z.B. gesprächsweise erlangte personenbezogene Daten) umfasst sein.[54]

Wie auch bereits unter § 20 Absatz 4 HSOG in der aktuellen Fassung ist wohl auch mit der Vorschrift des § 20 Absatz 6 HSOG-E aufgrund der Regelung in § 481 StPO weiterhin die Umwidmung und Zweckänderung von Daten der Strafverfolgung erlaubt und kann auch als Grundlage für polizeiliche Datenverarbeitung dienen.[55] Aus § 20 Absatz 6 HSOG-E könnte damit auch weiterhin die Befugnis zur Installation und Betrieb der polizeilichen Informations-/Verbundsysteme hergleitet werden.[56]

Zudem ist nun entfallen, dass eine automatisierte Verarbeitung nur zulässig ist, wenn es sich um Personen handelt, die verdächtig sind, eine Straftat begangen zu haben (siehe § 20 Absatz 4 in der aktuellen Fassung). Hier fehlt zum einen -anders als in der aktuellen Fassung - der Bezug zum automatisierten Verfahren, welches jedoch ausweislich der Gesetzesbegründung (S. 215) im Rahmen dieser Regelung insgesamt gelten soll. Zum anderen sind in der gesetzlichen Regelung § 20 Absatz 6 HSOG-E (wie in der aktuellen Fassung) die Voraussetzungen der polizeilichen Datenverarbeitung bzw. des polizeilichen Datenverarbeitungssystems ungeregelt.[57]

Verfassungsrechtliche Bedenken wurden daher bereits gegenüber § 20 Absatz 4 HSOG in der aktuellen Fassung vorgebracht, da etwa auch die Grenzen zwischen Repression und Prävention

[54] Hornmann, HSOG, § 20 Rn. 28.
[55] Siehe hierzu insgesamt Hornmann, HSOG, § 20 Rn. 31, der außerdem auf verfassungsrechtliche Bedenken verweist. Im Übrigen werden Daten, die von „Hilfsbeamten" der Staatsanwaltschaft erhoben wurden, nunmehr weiterverarbeitet, ohne dass die Staatsanwaltschaft die Verfügungsgewalt darüber ausüben könnte.
[56] Vgl. Hornmann, HSOG, § 20 Rn. 29.
[57] Siehe hierzu auch die Kritik zu § 20 Absatz 4 HSOG von Hornmann, HSOG, § 20 Rn. 56 mit dem Hinweis auf ungeregelte Zugriffsbefugnisse und Online-Abrufe, Bedeutung von Freispruch und Verfahrenseinstellung als Speichervoraussetzung. Für den polizeilichen Informationsverbund zwischen Bund und Ländern enthält das BKAG Regelungen, siehe hierzu §§ 29 ff., 12 ff. BKAG-neu.

aufgehoben werden.[58] Dies ändert auch die Neuregelung des § 20 Absatz 6 HSOG-E nicht. Für eine Weiterverarbeitung ist zudem weder eine Wiederholungsgefahr noch die Gefahr vorausgesetzt, die Person könne eine weitere Straftat begehen. Es könnte somit eine umfassende automatisierte Datenverarbeitung vorgenommen werden, so dass auch zukünftig für eine verfassungskonforme Auslegung der vertiefte Blick immer auf die Einzelfallprüfung notwendig sein wird, insbesondere hinsichtlich der Löschungspflichten und der Prüfung durch die Polizeibehörden, inwieweit tatsächlich eine automatisierte Datenverarbeitung erforderlich ist.[59] Es darf dabei nicht vergessen werden, dass gerade die automatisierte Datenverarbeitung erhöhte Eingriffsintensität in das informationelle Selbstbestimmungsrecht aufweist. Außerdem dürfen ebenso Daten von allen Personen, und nicht nur derjenigen, die verdächtig sind, eine Straftat begangen zu haben, automatisiert weiterverarbeitet werden. In Absatz 7 wird zwar ergänzend geregelt, dass eine automatisierte Weiterverarbeitung von Daten von Hinweisgebern, Zeugen, etc. nur bei erheblichen Straftaten in Betracht kommt. Der Begriff der erheblichen Straftat ist jedoch nicht konkretisiert und die Weiterverarbeitung dieser personenbezogenen Daten ist zudem immer erlaubt, wenn sie nicht in Dateien bzw. in nicht-automatisierter Form erfolgt. Nur § 20 Absatz 3 Satz 1 HSOG in der aktuellen Fassung enthält für Gefahrenabwehr- und Polizeibehörden eine strenge Zweckbindung für Personen, von denen nicht aufgrund tatsächlicher Anhaltspunkte davon ausgegangen werden kann, dass sie Straftaten mit erheblicher Bedeutung begehen werden (Zeugen, Hinweisgeber). Problematisch ist außerdem, dass nunmehr keine Höchstspeicherdauer von drei Jahre für diese Personen mehr festgelegt ist (siehe § 20 Absatz 5 HSOG in der aktuellen Fassung), sondern lediglich eine Prüffrist von höchstens drei Jahren gemäß § 27 Absatz 4 Satz 5 HSOG-E normiert wurde. Somit ist nicht sichergestellt, dass nach einem Jahr geprüft wird, ob die Speicherung dieser personenbezogenen Daten überhaupt noch erforderlich ist.

Zurzeit wird unterstellt, dass sich die Gesetzgebungskompetenz zur automatisierten Verarbeitung von personenbezogenen Daten durch die Polizeibehörden, die sie im Rahmen von strafrechtlichen Ermittlungsverfahren gewonnen haben, daraus ergibt, dass der Bund von seiner konkurrierenden Gesetzgebungskompetenz keinen abschließenden Gebrauch gemacht hat (Hornmann, HSOG, § 20 Rn. 53). Dennoch fehlen – wie gerade dargestellt- konkrete Regelungen der Durchführung. Daher stellt sich im besonderen Maße auch die Frage nach Verhältnismäßigkeit der Speicherung von Informationen der Strafverfolgungsvorsorge als Verwaltungsaufgabe der Polizei.

§ 20a HSOG-E

§ 20a HSOG-E regelt Kennzeichnungspflichten bei der Speicherung von Daten in polizeilichen Informationssystemen. Rechtsgrundlage sowie der Zweck der Speicherung müssen jedoch nicht zwingend angegeben werden (siehe hierzu auch § 14 BKAG-neu).

Wenn nun sämtliche Daten ohne entsprechende Angabe von Zweck und Rechtsgrundlage gespeichert werden, kann im Nachhinein allerdings nicht mehr ohne weiteres die Erforderlichkeit und Verhältnismäßigkeit festgestellt werden.[60]

[58] Hornmann, aaO.
[59] Siehe hierzu Hornmann, HSOG, § 20 Rn. 56 ff., 59.
[60] Siehe hierzu auch die Ausführungen zum „horizontalen“ Datenschutzkonzept; S. 113, S. 86 mit Verweis auf die Rechtsprechung des Bundesverfassungsgerichts Rn. 281 – Bundesrat Drucksache 109/17.

Insgesamt ist zwar ein Verzeichnis von Verarbeitungstätigkeiten gemäß § 65 HDSIG-E zu erstellen. Allerdings ist lediglich ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen. Hier ist unklar, in welcher Form diese Kategorien gebildet werden sollen und wie sich unterscheiden, zumal auch nur eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten zu erfolgen hat. Im Hinblick auf eine Kontrolle ist zu ergänzen, dass nach § 65 Absatz 4 HDSIG-E diese Verzeichnisse dem Hessischen Datenschutzbeauftragten nur auf Anfrage zur Verfügung zu stellen sind. Die Regelung des § 65 HDSIG-E beinhaltet zwar den Wortlaut von Artikel 24 der Richtlinie (EU) Nr. 2016/680. Dennoch muss eine Gesamtschau der polizeilichen Befugnisse und mit Blick auf die Weiterverarbeitungsmöglichkeiten des § 20 Absatz 6 HSOG-E und der Vorhersehbarkeit der Datenverarbeitung für den Bürger als betroffene Person erfolgen.

Insgesamt ist jedoch zu berücksichtigen, dass gemäß der Richtlinie (EU) Nr. 2016/680 die Verpflichtung besteht, den Nachweis der Rechtmäßigkeit der Verarbeitung zu erbringen (Artikel 4 Absatz 4).

§ 21 HSOG-E

Bei der Übermittlung von Daten im Sinne von § 21 Absatz 5 HSOG-E ist zu berücksichtigen, dass gemäß Artikel 4 Absatz 4 der Richtlinie (EU) Nr. 2016/680 der Verantwortliche für die Einhaltung der Absätze 1, 2 und 3 verantwortlich ist und deren Einhaltung nachweisen können muss. Dazu gehören ebenso Dokumentationspflichten. Da jedoch sowohl übermittelnde als auch empfangende Behörde als Verantwortliche einer rechtmäßigen Datenverarbeitung einzustufen sind, unterliegen beide entsprechenden Dokumentationspflichten. Dies muss auch gelten, wenn innerhalb einer Behörde Stellen mit unterschiedlichen Aufgaben Daten austauschen.

§ 27 HSOG-E

In § 27 Absatz 4 Satz 3 HSOG wird der Beginn der Prüffrist an den letzten Anlass der Speicherung geknüpft. Satz 4 führt weiter aus, dass im Falle der Speicherung von weiteren personenbezogenen Daten über dieselbe Person, für alle Speicherungen gemeinsam die Frist gilt, die als letzte abläuft. In der Gesetzesbegründung (S. 223) wird zwar darauf verwiesen, dass im Rahmen von Absatz 4 nur redaktionelle Änderungen vorgenommen wurden. Dennoch muss hier eine verfassungskonforme Auslegung erfolgen, da bei jeder neuen Speicherung nach dem Wortlaut sämtliche bisherigen mit einer Person verknüpften Daten ebenso zukünftig gespeichert werde könnten, und zwar auch dann, wenn der Betroffene Auskunftsperson (siehe § 13 Absatz 2 Nr. 3) ist. Bei letzteren gilt eine verkürzte Prüffrist von drei Jahren. Allerdings ist nunmehr keine Höchstspeicherdauer von drei Jahre für diese Personen festgelegt (siehe § 20 Absatz 5 HSOG in der aktuellen Fassung), sondern lediglich eine Prüffrist von höchstens drei Jahren gemäß § 27 Absatz 4 Satz 5 HSOG-E.

In § 17 HSOG-DVO (Verordnung zur Durchführung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung) werden aktuell die Prüffristen dahingehend näher präzisiert, dass die Prüffrist mit dem letzten Ereignis beginnt, dass die Speicherung begründet hat. 10 Jahre nach dem angenommenen Tatzeitpunkt müsste daher überprüft werden, ob die Speicherung der personenbezogenen Daten noch erforderlich ist. Gemäß § 27 Absatz 4 S. 3 und S. 4 HSOG-E ist indessen der letzte Anlass einer Speicherung von Daten über eine Person für den Fristbeginn entscheidend und bezieht sich damit auf sämtliche Daten und nicht auf die im Zusammenhang mit einem speziellen Ereignis verknüpften Daten. Wenn nun Angaben zu dieser Person aus einem speziellen Anlass innerhalb dieser 10 Jahre erneut gespeichert werden, löst dieser Anlass die Frist

aus, da das erstmalige Ereignis der Speicherung nicht relevant ist bzw. nicht relevant ist, ob die Daten aus diesem Ereignis zu löschen wären. Es müsste also nicht geprüft werden, ob die Speicherung der jeweiligen im Zusammenhang mit einem Ereignis stehenden Daten zur Aufgabenerfüllung weiterhin erforderlich sind, sondern es ist lediglich die letzte Speicherung entscheidend.

Es wurde daher bereits in der Vergangenheit darauf verwiesen, dass eine verfassungskonforme Auslegung erfordert, dass rechtswidrig gespeicherte Daten sofort zu löschen sind und dass bei Prüffrist und Löschung auf jeden einzelnen Fall gesondert abzustellen ist.[61] In diesem Zusammenhang sollte auch die Einschränkung der Verarbeitung anstatt der Löschung im Einzelfall kritisch geprüft werden (§ 53 Absatz 3 HDSIG-E; Art. 16 Absatz 3 der Richtlinie (EU) Nr. 2016/680), und zwar wenn nach Auffassung der Polizeibehörden Daten zu Beweiszwecken weiter aufbewahrt müssen.

Im Übrigen wird der Begriff der Akte in § 27 Absatz 3 HSOG-E verwendet, der aktuell in § 2 Absatz 7 HDSG definiert ist, aber in der Neufassung im HDSIG-E und dem HSOG keine Definition erfährt.

Zu § 27a HSOG-E

Diese Regelung soll für Gefahrenabwehrbehörden und Polizeibehörden gelten, die Daten für Zwecke außerhalb von der Richtlinie (EU) Nr. 2016/680 verarbeiten. Hier sollte überprüft werden, ob tatsächlich im HSOG eine eigenständige Regelung erforderlich ist, wenn die Datenverarbeitung unter den Anwendungsbereich der Datenschutzgrundverordnung fällt.

Zu beachten ist, dass Artikel 18 Datenschutzgrundverordnung dem Betroffenen ein Recht auf Einschränkung der Verarbeitung gibt, aber diese Regelung in § 27a HSOG-E als Recht des Verantwortlichen ausgestaltet ist. Zudem stehen dem Betroffenen nach der Datenschutzgrundverordnung ebenso Widerspruchsrechte und Berichtigungsrechte zu.

Das Recht auf Berichtigung kann im Übrigen gemäß der Datenschutzgrundverordnung nicht durch die Einschränkung der Verarbeitung ersetzt werden, lediglich die Löschung (Artikel 16, 18 Datenschutzgrundverordnung regeln dies nur für die Dauer der Prüfung).

§ 29 HSOG-E

Die Regelung des § 29 Absatz 2 HSOG-E gilt für Gefahrenabwehrbehörden, wenn keine Zwecke der §§ 40 ff. HDSIG-E verfolgt werden.

Beim Verweis auf § 31 Absatz 1 HDSIG-E ist zu berücksichtigen, dass der Begriff der Weiterverarbeitung vom hessischen Gesetzgeber im Rahmen der Richtlinie (EU) Nr. 2016/680 definiert wurde (siehe Gesetzesbegründung S. 208 und oben unter § 20, S. 66), aber es sich bei § 31 HDSIG-E um eine Regelung für eine Datenverarbeitung für Zwecke außerhalb des § 40 HDSIG-E bzw. der Richtlinie (EU) Nr. 2016/680 handelt. Der Begriff der Weiterverarbeitung ist in der Datenschutzgrundverordnung nicht definiert. Aus den Erwägungsgründen 50, 61 der Datenschutzgrundverordnung ergibt sich jedoch, dass mit Weiterverarbeitung stets eine Zweckänderung verbunden ist. Dies ist bei Verwendung dieser Begrifflichkeiten und bei Anwendung der Regelungen zu berücksichtigen.

Nach dieser Regelung dürften Gefahrenabwehrbehörden etwa Daten in Akten ohne Information des Betroffenen weiterverarbeiten, wenn das Interesse des Betroffenen an der Informationserteilung als

[61] Hornmann, HSOG, § 27 Rn. 29.

gering anzusehen ist. Allerdings ist unklar, wann ein solches Interesse als gering einzustufen wäre, so dass diese Regelung für den Betroffenen nicht bestimmt ist.

Desweiteren besteht nach § 31 Absatz 1 Nr. 2 HDSIG-E die Möglichkeit, die Informationspflicht im Interesse der öffentlichen Sicherheit und Ordnung einzuschränken. Auch hier sei wieder darauf verwiesen, dass diese Begriffe unionsrechtlich auszulegen sind und nicht zwangsläufig mit dem deutschen materiellen Polizeirecht gleichzusetzen sind (siehe S. 45).

Zudem müssen die Rechtsstaatsgarantie und der Verhältnismäßigkeitsgrundsatz beachtet werden, da das Recht auf Information eingeschränkt wird. In diesem Sinne bestehen Zweifel an der Regelung des § 31 Absatz 1 Nr. 3 HDSIG-E, die ohne entsprechende Konkretisierung bzw. pauschal darauf verweist, dass eine Information unterbleiben kann, wenn die beabsichtigte Weiterverarbeitung eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.

Gemäß § **29 Absatz 5** HSOG-E sind bei verdeckten Maßnahmen, wie sie von § 15 HSOG erfasst sind, die betroffenen Personen nach Abschluss der Maßnahmen zu benachrichtigen. Es folgen allerdings keine Ausführungen zur Form dieser Information. Für Zwecke der Richtlinie (EU) Nr. 2016/680 und § 40 HDSIG-E folgen die Modalitäten aus Artikel 12 Absatz 1 der Richtlinie (EU) Nr. 2016/680, so dass alle Mitteilungen in einer präzisen, verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache zu übermitteln sind. Die Übermittlung kann dabei auch in elektronischer Form erfolgen. Weder in § 29 HSOG noch in § 51 HDSIG-E findet sich allerdings eine entsprechende gesetzliche Umsetzung dieser Vorgaben für diesen konkreten Fall (in § 50 HDSIG-E sind zwar allgemeine Informationen für jedermann geregelt, aber es sind keine Regelungen hinsichtlich der Modalitäten getroffen).[62] Diese sollten daher noch im Gesetzestext umgesetzt werden, da der pauschale Verweis in § 29 Absatz 1 HSOG auf die Datenschutzgrundverordnung an dieser Stelle nicht ausreichend ist, zumal dort gerade nicht auf Artikel 12 Datenschutzgrundverordnung, sondern nur auf Artikel 13 bis 15 Datenschutzgrundverordnung verwiesen wurde und im Übrigen diese Regelungen bei Zwecken des § 40 HDSIG-E nicht zur Anwendung gelangen können.

Aufgrund dessen, dass in § 29 Absatz 1 HSOG-E geregelt ist, dass u.a. § 51 HDSIG-E nur gilt, wenn in § 29 Absatz 2 bis Absatz 7 nichts Abweichendes geregelt ist, muss geprüft werden, ob § **29 Absatz 6** HSOG-E überhaupt mit den Vorgaben des Artikel 13 Absatz 3 Richtlinie (EU) Nr. 2016/680 übereinstimmt. Die Mitgliedstaaten dürfen Gesetzgebungsakte erlassen, nach denen die Unterrichtung aufgeschoben oder eingeschränkt oder unterlassen werden kann, allerdings nur unter dem Grundsatz der Verhältnismäßigkeit und Erforderlichkeit, wenn insbesondere Untersuchungen, Ermittlungen oder Verfahren behindert werden oder die Verhütung und Verfolgung von Straftaten beeinträchtigt werden könnte. Dies regelt § 29 Absatz 6 HSOG-E allerdings nicht. Hiernach ist bereits eine Gefährdung des Zwecks ausreichend, so dass fraglich ist, ob dies nicht hinter den Vorgaben des EU-Richtliniengebers zurückbleibt und ob die Interessen der betroffenen Person gebührend berücksichtigt sind.[63] Die Information ist allein schon wegen der Rechtsschutzgarantie geboten und die Möglichkeit einer unterbliebenen Information muss eine Ausnahme bleiben. Es muss vielmehr klar sein, dass unabhängig davon, ob der Wortlaut sich auf eine „Gefährdung“ oder „Behinderung“ bezieht, das Interesse an der Geheimhaltung deutlich überwiegen muss.

[62] Siehe hierzu bereits die Ausführungen auf S.20.
[63] Siehe auch Erwägungsgrund 26, der unter anderem auf die Möglichkeiten verdeckter Maßnahmen Bezug nimmt.

Zudem soll bereits die Gefährdung der Möglichkeit der weiteren Verwendung der V-Person oder VE-Person auseichend sein. Daher muss auch an dieser Stelle kritisch geprüft werden, ob diese Einschränkung verhältnismäßig ist, insbesondere wenn keine Lebens- oder Gesundheitsgefahr der V-Person der VE-Person bestehen soll.

Im Übrigen gilt das bereits oben Gesagte, dass im Sinne einer einheitlichen Terminologie nicht der Begriff „Benachrichtigung“, sondern „Information“ verwendet werden sollte.

3. Fazit

Die Gefahren- und Abwehrbehörden erhalten erheblich erweiterte Befugnisse. Bislang ist jedoch die Frage noch nicht beantwortet, ob es bereits bei präventiven Maßnahmen zum Schutz von „vergleichbaren Rechtsgütern“ oder zur „Verhütung vergleichbar schwerwiegender Straftaten oder Ordnungswidrigkeiten“ verhältnismäßig ist, die angestrebten Datenverarbeitungen zuzulassen.[64] Hierbei ist im Hinblick auf den Begriff der Ordnungswidrigkeit zu berücksichtigen, dass nicht alle EU-Mitgliedstaaten über ein vergleichbares Ordnungswidrigkeitenrecht verfügen und dass der Begriff der Straftat ein eigenständiger Begriff des Unionsrechts in der Auslegung durch den Gerichtshof der Europäischen Union ist. Ebenfalls ist zu beachten, dass es sich gleichermaßen bei dem in der Datenschutzgrundverordnung und der Richtlinie (EU) Nr. 2016/680 verwendeten Begriff der öffentlichen Sicherheit um einen Begriff des Gemeinschaftsrechts handelt und insoweit nicht die Definition nach deutschem Polizei- und Ordnungsrecht maßgeblich ist. Dementsprechend ist in der Gesetzgebung stets der unionsrechtliche Bezug zu berücksichtigen, wobei im Einzelfall den innerstaatlichen Behörden vom Europäischen Gerichtshof ein Beurteilungsspielraum zugebilligt wurde.[65] Bei der Verwendung von unbestimmten Rechtsbegriffen sollte zudem überprüft werden, ob dies der Rechtssicherheit und der Transparenz entgegenstehen könnte.[66] Der Gesetzgeber muss sich zwar grundsätzlich abstrakter und unbestimmter Formulierungen bedienen können. Es muss jedoch im Einzelfall ebenfalls bedacht werden, inwieweit es sinnvoller sein könnte, besonders folgenreiche Eingriffe in bereichsspezifischen Gesetzen detailliert zu regeln. So ist das Hessische Datenschutzgesetz für die allgemeine Verwaltung konzipiert.[67] Überlegungsbedürftig ist daher auch, ob die Richtlinie (EU) Nr. 2016/680 in Form der eigenständigen und bereichsspezifischen Regelungen gemäß §§ 40 ff. HDSIG-E in das Hessische Datenschutzgesetz integriert werden sollte. In diesem Zusammenhang ist gleichermaßen an die Nachvollziehbarkeit der gesetzlichen Regelungen für die

[64] Das BKA-Gesetz und die Rechtsprechung des Bundesverfassungsgerichts beziehen sich auf andere Schutzziele und „hinreichend gewichtige Rechtsgüter“ (BVerfG, Urteil vom 20.04. 2016 - 1 BvR 966/09 -)

[65] Beim Begriff der öffentlichen Ordnung wurde vom EUGH im Zusammenhang mit der Einschränkung des freien Dienstleistungsverkehrs ein gewisser Auslegungsspielraum anerkannt, siehe Urteil des Gerichtshofes vom 14.Oktober 2004, Rechtssache C-36/02. Siehe hierzu außerdem die Ausführungen auf S. 8.

[66] Siehe etwa die in § 20 HDSIG-E verwendeten Regelungen in Bezug zur öffentlichen Sicherheit und zum öffentlichen Interesse. Wiederholungen des Textes der Datenschutzgrundverordnung -wie etwa in § 20 HDSIG-E- die Rechtsprechung des EUGH zu beachten, die dies nur in engen Grenzen erlaubt,

[67] Dies kann für das Polizeirecht gelten. Aber auch mit der Verarbeitung von besonderen Kategorien personenbezogener Daten ohne Einwilligung des Betroffenen für Zwecke der „öffentlichen Sicherheit“ können folgenreiche Eingriffe verbunden sein. Siehe Nungesser, HDSG, § 1 Rn. 14 ff. mit Verweis auf die Rechtsprechung des Bundesverfassungsgerichts, BVerfGE 56, 12.

Bürgerinnen und Bürger zu denken.[68] Transparenz als allgemeiner Gedanke ist ebenso bei den Gesetzen wichtig.[69]

Zur Wahrung der Rechtseinheit und der angestrebten europaweiten Harmonisierung der Datenschutzgrundverordnung kann sich darüber hinaus eine Prüfung dahingehend empfehlen, inwieweit die übrigen Landesdatenschutzgesetze wortgleiche Regelungen beinhalten. Mit den Vorgaben des Gemeinschaftsrechts hängt im Übrigen auch zusammen, ob eigene Legaldefinitionen geschaffen werden dürfen.[70]

Mit freundlichen Grüßen

Anne Riechert

[68] Das Zusammenspiel zwischen den Regelungen des zweiten und des dritten Teils des HDSIG-E und des HSOG-E könnte jedoch schwer verständlich sein. Dies gilt insbesondere für die Unterteilung im HSOG-E zu den in § 40 HDSIG-E genannten Zwecken und zu Zwecken außerhalb des § 40 HDSIG-E, die mit einer unterschiedlichen Beschränkung der Rechte des Betroffenen und Verweisen auf unterschiedliche Informations- und Auskunftsrechten verbunden sein kann. Wenn die Transparenz nicht erfüllt ist, kann im Einzelfall die transparente Information der Betroffenen über ihre jeweiligen Rechte immer wichtig werden.

[69] Insgesamt könnte außerdem klarer gefasst werden, für welche Behörden die Regelungen zu Zwecken des § 40 HDSIG-E/ Richtlinie (EU) Nr. 2016/680 im Einzelfall anwendbar sind. Die Formulierung in der Gesetzesbegründung lässt an dieser Stelle Interpretationsspielraum (S. 136): *„wenn die Behörden die Datenverarbeitung zum Zwecke der auf die Verhütung von Straftaten oder Ordnungswidrigkeiten bezogenen Gefahrenabwehr vornehmen und eine solche gesetzliche Aufgabenzuweisung besteht*.“ In diesem Sinne könnte dann ebenso eine klare Abgrenzung zum Anwendungsbereich des OWIG erfolgen.

[70] Siehe hierzu den Begriff der Anonymisierung in § 2 Absatz 4 HDSIG-E.