Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg

Per E-Mail
Freie und Hansestadt Hamburg
Behörde für Inneres und Sport

Nachrichtlich
Justizbehörde
Finanzbehörde
Senatskanzlei
Behörde für Wissenschaft, Forschung und Gleichstellung

Ludwig-Erhard-Str. 22, 7. OG
20459 Hamburg
Telefon: 040 - 428 54 - 40 50 Zentrale - 40 40
Telefax: 040 - 428 54 - 40 00
[redacted]
Referat G (Demokratie, Inneres, Grundversorgung, Informationsfreiheit)
E-Mail*: [redacted]@datenschutz.hamburg.de

Az.: G / 11.01-06/4

Hamburg, den 24.6.2019

Stellungnahme zum Senatsdrucksachenentwurf zur „Änderung polizeirechtlicher Vorschriften“

Sehr geehrte Damen und Herren,
sehr [redacted]

haben Sie vielen Dank für die Gelegenheit, zum Entwurf eines Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften aus datenschutzrechtlicher Sicht Stellung zu nehmen.

Erlauben Sie mir eine kurze Vorbemerkung: Die Drucksache hat mit 130 Seiten einen erheblichen Umfang und behandelt komplexe datenschutzrechtliche Fragestellungen, bei denen es nicht nur zu überprüfen gilt, ob die europarechtlichen Vorgaben der Richtlinie (EU) 2016/680 (JI-Richtlinie) eingehalten werden, sondern auch darum, ob verschiedene Judikate des Bundesverfassungsgerichts umgesetzt wurden.

Die äußerst kurze Fristsetzung zur Stellungnahme bis zum 24. Juni 2019 gibt eine Bearbeitungszeit von 7 Werktagen vor. Angesichts der Bedeutung sowie Komplexität der Regelungen ist dies zu bedauern. Insbesondere sei daran erinnert, dass die JI-Richtlinie bereits vor mehr als drei Jahren erlassen wurde und uns bis heute durch die Behörde für Inneres und Sport keine Informationen über die geplante Novellierung der polizeirechtlichen Vorschriften erreichten. Eine datenschutzrechtliche Stellungnahme in dieser kurzen Zeit kann daher nur die grundsätzlichen Aspekte beleuchten, die durch die geplanten Regelungen aufgeworfen werden. Insoweit bleibt ausdrücklich vorbehalten, dass einzelne Fragstellungen zu einem späteren Termin aufgegriffen und weitere Argumente nachgereicht werden.

Nach 3.2. Abs. 2 der Beteiligungsrichtlinie ist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) an allen Rechtssetzungsvorhaben zu beteiligen, die Belange des Datenschutzes berühren. Die Beteiligung erfolgt nach 3.2. Abs. 3 der Beteiligungsrichtlinie zu demselben Zeitpunkt und in derselben Form, in der Senatsämter und Fachbehörden an den Rechtsetzungsvorhaben beteiligt werden. Danach ist dem HmbBfDI die Einräumung einer angemessenen Abstimmungsfrist einzuräumen (vgl. § 16 Absatz 1 Satz 3 der Geschäftsordnung des Senats). Es wird darum gebeten, derartige Vorgaben zukünftig zu berücksichtigen.

Auf dieser Basis nimmt der HmbBfDI wie folgt Stellung:

A. Art. 1 – Gesetz über die Datenverarbeitung der Polizei (PolDVG-E)

I. § 1 PolDVG-E - Anwendungsbereich

Bezüglich der in § 1 PolDVG-E normierten Reichweite des Gesetzes auf alle Bereiche der Gefahrenabwehr bestehen erhebliche Bedenken, weil angenommen werden muss, dass dadurch in europarechtswidriger Weise auch der Bereich der Gefahrenabwehr geregelt wird, der in den Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) und damit des Hamburgischen Datenschutzgesetzes (HmbDSG) fällt.

Der Gesetzesentwurf dient ganz überwiegend dazu, das PolDVG an die JI-Richtlinie anzupassen. Aus dem Zusammenspiel von Art. 2 Abs. 2 lit. d) DSGVO und § 2 Abs. 4 HmbDSG sowie Art. 1 Abs. 1 JI-Richtlinie folgt, dass die JI-Richtlinie nur in den Bereichen anwendbar ist, in denen die Anwendbarkeit der DSGVO ausgeschlossen ist. Ausgeschlossen ist die Anwendbarkeit der DSGVO (und des HmbDSG, das die Vorschriften der DSGVO ergänzt) aber nur bei der Verarbeitung von personenbezogenen 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*“. Daraus folgt, dass nur der Bereich der straftatbezogenen Gefahrenabwehr in den Anwendungsbereich der JI-Richtlinie fällt. Die allgemeine Gefahrenabwehr – auch wenn sie durch die in Art. 1 Abs. 1 der JI-Richtlinie genannten zuständigen Behörden vorgenommen wird – fällt in den Bereich der DSGVO bzw. des HmbDSG (so ausdrücklich: Erwägungsgrund Nr. 12 der JI-Richtlinie; ebenso: *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, § 1, Rn. 22 ff.). Durch die Ausweitung des PolDVG (als Umsetzung der JI-Richtlinie) auf den gesamten Bereich der Gefahrenabwehr – auch der nicht straftatbezogenen Gefahrenabwehr (z.B. im

Bereich des Katastrophenschutzes und des Schutzes suizidaler Personen sowie beim Schutz vor ungewollter Obdachlosigkeit) – wird somit der Anwendungsbereich der DSGVO sowie des HmbDSG europarechtswidrig eingeschränkt.

II. Grundproblematik der Einwilligung/§ 4 PolDVG-E Verarbeitung besonderer Kategorien personenbezogener Daten

Der Entwurf enthält an unterschiedlichen Stellen die Möglichkeit, in die Verarbeitung personenbezogener Daten einzuwilligen. Es ist zweifelhaft, ob dies im Anwendungsbereich der JI-Richtlinie überhaupt möglich ist. Zunächst ist festzustellen, dass die JI-Richtlinie keine ausdrücklichen Regelungen zur Einwilligung enthält. Vielmehr regelt Art. 8 JI-Richtlinie, dass die Mitgliedstaaten vorzusehen haben, dass eine Verarbeitung personenbezogener Daten nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Art. 1 Abs. 1 JI-Richtlinie genannten Zwecken wahrgenommen wird. Die Mitgliedstaaten haben also spezifische Vorschriften zu schaffen, auf deren Grundlage die Verarbeitung personenbezogener Daten erfolgen kann. Vor diesem Hintergrund dürfte für eine Verarbeitung personenbezogener Daten auf Grundlage einer Einwilligung im Anwendungsbereich der JI-Richtlinie gerade kein Raum bleiben. Vielmehr dürfte in dem Verzicht der Regelung einer Einwilligung als Grundlage für die Verarbeitung personenbezogener Daten „eine bewusste Entscheidung des Richtliniengebers“ (so auch *Petri*, ZD 2018, 389) zu sehen sein. Diese Überlegung wird auf folgende, grundsätzliche Erwägungen gestützt:

Es ist das Erfordernis einer wirksamen Einwilligung, dass diese freiwillig erfolgt. Die Freiwilligkeit einer Erklärung steht jedoch immer dann in Frage, wenn zwischen den Akteuren ein Ungleichgewicht der Machtverhältnisse besteht. Handelt es sich bei dem Verantwortlichen um eine Behörde, sollte davon ausgegangen werden, dass eine Einwilligung grundsätzlich keine gültige Rechtsgrundlage liefern kann (vgl. zur DSGVO EG 43 zur Datenschutzgrundverordnung). Dies gilt gerade im Falle der Vollzugspolizei, an die sich wesentliche Teile des Entwurfs richten. Staatliche Stellen sollten im Bereich der Eingriffsverwaltung daher grundsätzlich nur auf Grundlage spezifisch geschaffener Rechtssätze tätig werden. Das Konstrukt einer Einwilligung sollte im Falle der Verarbeitung personenbezogener Daten durch öffentliche Stellen nur restriktiv genutzt werden.

Vor allem aber darf eine Einwilligung nicht als Auffangtatbestand für Sachverhalte herangezogen werden, in denen Unklarheit über die staatlichen Befugnisse besteht. Für den Bürger muss Klarheit darüber herrschen, auf welcher Grundlage in seine Grundrechte eingegriffen wird. Der Verantwortliche muss zuvor festgelegt haben, auf Grundlage welchen

Tatbestands personenbezogene Daten verarbeitet werden. Die Einwilligung sollte hier nicht zu einer allgemeinen Auffangbefugnis für fehlende oder unklare Eingriffsregelungen ausgestaltet werden.

Das Konzept der Einwilligung ist der JI-Richtlinie nicht grundsätzlich fremd. In Erwägungsgrund 35 heißt es: “Die Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie sollte nur dann als rechtmäßig gelten, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die eine zuständige Behörde im öffentlichen Interesse auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten 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, ausführt. Diese Tätigkeiten sollten sich auf die Wahrung lebenswichtiger Interessen der betroffenen Person erstrecken. 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. Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung.“

Nach Erwägungsgrund 37 Satz 6 JI-Richtlinie sollte die Einwilligung allein daher keine rechtliche Grundlage für die Verarbeitung besonders sensibler personenbezogener Daten darstellen. Vor diesem Hintergrund hält der HmbBfDI die Schaffung spezifischer Gesetze für die Verarbeitung besonderer Kategorien personenbezogener Daten für erforderlich. Hierfür spricht nicht zuletzt auch der Wortlaut des Art. 10 JI-Richtlinie, der verlangt, dass die Verarbeitung solcher Daten unbedingt erforderlich sein muss. Es ist unklar, inwieweit eine Verarbeitung personenbezogener Daten, die unbedingt erforderlich ist, einer Einwilligung bedürfen sollte, und wenn sie es ist, warum hierfür kein spezifisches Gesetz geschaffen werden können sollte.

Vor diesem Hintergrund bestehen insbesondere Bedenken gegen die Verarbeitung besonderer Kategorien personenbezogener Daten auf Grundlage einer Einwilligung (vgl. § 4

Abs. 1 Nr. 3 PolDVG-E). Derartige Daten genießen aufgrund der Erkenntnisse, die sich aus ihnen über die persönlichen Lebensverhältnisse der betroffenen Personen ziehen lassen, einen besonderen Schutz.

III. § 9 PolDVG-E – Automatisierte Entscheidungen

§ 9 PolDVG-E normiert die Zulässigkeit automatisierter Einzelfallentscheidungen, wenn diese in besonderen Rechtsvorschriften vorgesehen ist. Die Vorschrift bleibt dabei insofern hinter dem Wortlaut des Art. 11 Abs. 1 JI-Richtlinie zurück, wonach hierzu erlassene Regelungen geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen bieten müssen, zumindest aber das Recht auf persönliches Eingreifen. In § 9 Abs. 1 PolDVG-E sollten entsprechende Anforderungen aufgenommen werden. Die Bezugnahme auf geeignete Maßnahmen zum Schutz von Rechtsgütern, die § 9 Abs. 2 PolDVG-E mit Blick auf besondere Kategorien personenbezogener Daten vorsieht, reicht hier nicht aus.

IV. § 18 PolDVG-E – Datenverarbeitungen im öffentlichen Raum und an besonders gefährdeten Orten

§ 18 PolDVG-E regelt Datenverarbeitungen durch Bild- und/oder Tonübertragungen/-aufzeichnungen, trifft jedoch keinerlei spezifische Regelungen zur Information betroffener Personen im Hinblick auf derartige Maßnahmen. Art. 13 JI-Richtlinie regelt die von den Mitgliedstaaten vorzusehenden Informationspflichten. Erwägungsgrund 39 der JI-Richtlinie lässt sich hierzu entnehmen, dass diese Informationen leicht zugänglich sein sollen. Um diesen Anforderungen gerecht zu werden, dürfte es für den Fall einer Videoüberwachung einer entsprechenden Ausweisung in Form einer Hinweisbeschilderung bedürfen (vgl. hierzu auch *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, Rn. 181).

Betroffene Personen, die sich im öffentlichen Raum einer Videoüberwachung ausgesetzt sehen, haben regelmäßig keine Kenntnis von der Identität des Verantwortlichen und können daher auch nicht ohne weiteres herausfinden, gegenüber wem sie ihre Rechte geltend machen müssen. Es ist daher unwahrscheinlich, dass sich betroffene Personen, etwa über Webseiten der Polizei, in geeigneter Weise über die Verarbeitung ihrer personenbezogenen Daten und ihre Rechte informieren können. Der HmbBfDI empfiehlt daher die Aufnahme einer spezifischen Vorschrift zur Information betroffener Person im Hinblick auf Maßnahmen der Videoüberwachung. Die allgemeine Regelung des § 64 PolDVG-E dürfte den spezifischen Anforderungen an Informationspflichten im Hinblick auf eine Videoüberwachung nicht gerecht werden.

V. § 21 PolDVG-E – Datenverarbeitung durch den verdeckten Einsatz technischer Mittel

Soweit nach § 21 Abs. 2 Satz 2 PolDVG-E die Anfertigung von Bildaufnahmen und Bildaufzeichnungen sowie Maßnahmen nach § 21 Abs. 1 Satz 2 PolDVG-E nur dem Amtsleitervorbehalt unterliegen, dürfte dies zu Missverständnissen führen. Es wird angeregt – angelehnt an § 45 Abs. 2 Nr. 2 und Nr. 3 i.V.m Abs. 3 Nr. 2 und Nr. 4 BKAG – zumindest klarzustellen, dass, wenn derartige Maßnahmen auch längerfristig i.S.d. § 20 Abs. 1 PolDVG-E durchgeführt werden, auch hier der Richtervorbehalt gilt. Soweit bezüglich § 21 Abs. 2 Satz 2 PolDVG-E in der Gesetzesbegründung ausgeführt wird, dass ein Richtervorbehalt für die Anfertigung von Bildaufnahmen und Bildaufzeichnungen auch zukünftig nicht erforderlich ist, ist dies nach der Rechtsprechung des Bundesverfassungsgerichts nur dann zutreffend, wenn es sich um kurzfristige Observationen handelt. So führt das Gericht aus, dass es nicht zu beanstanden sei,

> „*dass für die Anfertigung von Bildaufnahmen sowie für nur kurze Observationen – auch mittels Bildaufzeichnung oder technischer Peilsender – ein Richtervorbehalt nicht vorgesehen ist*. (…) *Demgegenüber ist eine unabhängige richterliche Kontrolle verfassungsrechtlich aber unverzichtbar, wenn Observationen (…) längerfristig – zumal unter Anfertigungen von Bildaufzeichnungen oder unter Nutzung besonderer technischer Mittel wie Peilsender – durchgeführt werden (…)“.* (BVerfG, Urt. v. 20.4.2019 – 1 BvR 966/09, Rn. 173)

VI. § 30 Abs. 2 Nr. 3 PolDVG-E - Elektronische Aufenthaltsüberwachung

Datenschutzrechtliche Bedenken bestehen hinsichtlich des § 30 Abs. 1 Nr. 3 und Abs. 2 Nr. 3 PolDVG-E, wonach zur Abwehr einer Gefahr für Leib, Leben und Freiheit einer Person die elektronische Aufenthaltsüberwachung angeordnet werden kann und die erhobenen Daten sodann bei Vorliegen jeder Gefahr für Leib, Leben und Freiheit verwendet werden können.

Bei der Befugnis zur elektronischen Überwachung des Aufenthaltsorts von Personen handelt es sich, wie der Gesetzesbegründung zu § 30 PolDVG-E zutreffend zu entnehmen ist, zunächst um eine Maßnahme, die eine besonders intensive Auswirkung auf die Grundrechtsausübung der Betroffenen hat. Zur Eingrenzung des in Betracht kommenden Personenkreises sollte daher auf die vom Bundesverfassungsgericht im Urteil vom 20.4.2016 (1 BvR 966/09) entwickelten Voraussetzungen für gefahrenabwehrrechtliche Maßnahmen zurückgegriffen werden (vgl. BT-Drs 18/11163 zu § 56 BKAG, S. 122 zur elektronischen Aufenthaltsüberwachung). Derartige Maßnahmen dürften daher nur zum Schutz besonders gewichtiger und bedeutsamer Rechtsgüter zulässig sein. Die in § 30 S. 1 Abs. 1 Nr. 1 und Nr. 2 i.V.m. Satz 3 PolDVG-E aufgenommene Begrenzung auf „terroristische Straftaten“ könnte

dem Rechnung tragen, soweit es sich dabei um Straftaten mit dem Gepräge des Terrorismus nach Rechtsprechung des Bundesverfassungsgerichts handelt. Derartige Straftaten zielen auf eine Destabilisierung des Gemeinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung andere Menschen durch Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen den Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Die Bereitstellung von wirksamen Aufklärungsmitteln zu ihrer Abwehr ist ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht (BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 95 ff.).

Es bestehen jedoch erhebliche Bedenken, soweit § 30 Abs. 1 Nr. 3 PolDVG-E im Gegensatz zu Nr. 1 und Nr. 2 bereits jede Gefahr für Leib, Leben und Freiheit einer Person als ausreichend ansieht. Die aus der BT-Drucksache zu § 56 BKAG weitgehend übernommene Begründung zu § 30 Abs. 2 Nr. 3 PolDVG-E ist nachvollziehbar. Danach soll durch die Verwendung der durch Absatz 1 erhobenen Daten auch zur Abwehr einer Gefahr für Leib, Leben und Freiheit einem Vertrauensverlust in die Funktionsfähigkeit der Polizei entgegengetreten werden, wenn entsprechende Daten nicht (weiter) zur Verhinderung von erheblichen Straftaten, insbesondere von schweren Gewaltstraftaten, genutzt werden können (vgl. BT-Drs. 18/11163 zu § 56 BKAG S. 122). Insoweit sollte die Verwendung der nach Absatz 1 gewonnenen Daten dann – nach dem Vorbild des BKAG – aber auch auf die Abwehr von **erheblichen gegenwärtigen** Gefahren beschränkt bleiben (vgl. § 56 Abs. 2 Satz 3 Nr. 4 BKAG).

VII. § 31 Abs. 1 PolDVG-E – Polizeiliche Beobachtung

Die Umsetzung der Vorgaben des Bundesverfassungsgerichts (Urt. v. 20.4.2019 - 1 BvR 699/06 u.a.) im Hinblick auf die Konkretisierung der Tatbestandsvoraussetzungen „*Tatsachen, die die Annahme rechtfertigen*“ jedenfalls in den §§ 20 Abs. 1 Nr. 2 ff. PolDVG-E im Rahmen der Verhütung von Straftaten wird ausdrücklich begrüßt.

Soweit ersichtlich handelt es sich bei der Einfügung der Abschnitte *„(…) die ein wenigstens seiner Art nach konkretes und zeitlich absehbares Geschehen erkennen lassen*“ (u.a. § 20 Abs. 1 Nr. 2 PolDVG-E) bzw. „*individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet*“ (vgl. § 30 Abs. 1 Nr. 2 PolDVG-E) um die Übernahme des Wortlauts aus dem fraglichen Urteil. Nicht ersichtlich ist jedoch, warum derartige Ergänzungen nicht auch Eingang in den § 31 Abs. 1 Nr. 2 PolDVG-E gefunden haben. Auch diese Vorschrift regelt die Rechtfertigung von Eingriffen im Bereich der Verhütung von Straftaten, von denen der Betroffene zunächst keine Kenntnis hat. Bei Maßnahmen im Bereich der Verhütung von Straftaten hat das Bundesverfassungsgericht aber in Bezug auf die hinreichende Bestimmtheit

dieses Tatbestandsmerkmals ganz allgemein Bedenken ausgeführt. Der Gesetzgeber hat demnach die Anforderungen an Tatsachen, die auf die künftige Begehung hindeuten, so bestimmt zu umschreiben, dass das im Bereich der Vorfeldermittlungen besonders hohe Risiko einer Fehlprognose gleichwohl verfassungsrechtlich noch hinnehmbar ist (vgl. auch BVerfG, Urt. v. 27.7.2005 – 1 BvR 668/04, Rn. 119 ff.). Daher sind die vom Gericht aufgestellten Anforderungen an die Konkretisierung für das Merkmal „Tatsachen, die die Annahme rechtfertigen“ auch in dieser Vorschrift vorzunehmen.

VIII. § 34 PolDVG-E Abs. 6 und 7 – Grundsätze der Zweckbindung

Bezüglich § 34 Abs. 6 PolDVG-E wird angeraten klarzustellen, wie sich diese Rechtfertigungsgrundlage zu § 4 PolDVG-E verhält. Durch § 34 Abs. 6 PolDVG wird die Verarbeitung von sog. personenbezogenen Hinweisen geregelt. Aus dem Sinn und Zweck der Norm folgt aber, dass es sich bei den „personengebundenen Hinweisen“ insbesondere auch um Gesundheitsdaten (z.B. Infektionskrankheiten) und damit um besondere Kategorien von Daten nach Art. 10 JI-Richtlinie handeln dürfte. Die Verarbeitung von besonderen Kategorien von personenbezogenen Daten i.S.d. Art. 10 JI-Richtlinie wird nun in § 4 PolDVG-E geregelt. Als Ermächtigung für die Speicherung von personengebundenen Hinweisen, wenn es sich dabei um personenbezogene Daten i.S.d. Art. 10 JI-Richtlinie handelt, käme grundsätzlich § 4 Abs. 1 Nr. 2 PolDVG-E (Zwecke der Eigensicherung) in Betracht. Allerdings müsste dann auch eine unbedingte Erforderlichkeit nach § 4 PolDVG vorliegen. Das Merkmal der unbedingten Erforderlichkeit findet sich allerdings nicht in § 34 Abs. 6 PolDVG-E, sondern lediglich die einfache Erforderlichkeit. Es kann daher nicht zweifelsfrei entnommen werden, ob es sich dabei um eine von § 4 PolDVG-E speziellere Regelung handelt. Sollte dies der Fall sein, wären auch im Rahmen von § 34 Abs. 6 PolDVG-E die Vorgaben des Art. 10 JI-Richtlinie zu beachten, falls unter personenbezogenen Hinweisen auch die besondere Kategorie von personenbezogenen Daten erfolgen soll bzw. ein Verweis auf § 4 PolDVG geboten.

Bezüglich § 34 Abs. 7 PolDVG-E ist anzuraten, das Verhältnis von Satz 1 und Satz 2 näher darzulegen, weil nicht zweifelsfrei entnommen werden kann, auf welche Betroffenen sich das Erforderlichkeitsmerkmal bezieht bzw. ob bei der Erstellung eines Kriminalitätsbildes personenbezogene Daten von einem Tatverdächtigten überhaupt weiterverarbeitet werden. In § 34 Abs. 7 Satz 1 PolDVG-E wird zunächst geregelt, dass bereits vorhandene personenbezogene Daten verarbeitet werden dürfen. Satz 2 weist darauf hin, dass die Daten der dort genannten nicht tatverdächtigen Personen nur verarbeitet werden dürfen, wenn dies erforderlich ist. Aus dem Zusammenspiel der Vorschriften könnte somit geschlossen werden, dass eine Verarbeitung von personenbezogenen Daten eines Tatverdächtigten nach § 34 Abs. 7 Satz 1 PolDVG-E auch ohne das Merkmal der Erforderlichkeit nach Satz 2 zulässig wäre. Dies wäre dann aber ein Verstoß gegen Art. 8 JI-Richtlinie.

IX. § 35 Abs. 3 – Dauer der Datenspeicherung; sog. Mitziehregelung

Datenschutzrechtliche Bedenken bestehen bzgl. der pauschalen sog. Mitziehreglung in § 35 Abs. 3 Satz 2 ff. PolDVG-E und dem Grundsatz der Erforderlichkeit.

Nach Art. 4 Abs. 1 lit e) JI-Richtlinie dürfen personenbezogene Daten nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht. Zudem sieht Art. 5 JI-Richtlinie vor, dass für die Löschung von personenbezogenen Daten oder der regelmäßigen Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen sind. Nicht angezweifelt wird in diesem Zusammenhang, dass grundsätzlich ein legitimes Bedürfnis der Polizei bestehen kann, einen langfristigen Überblick über die kriminellen Aktivitäten eines Betroffenen zu erhalten. Es kann daher im Einzelfall eine Notwendigkeit bestehen, die Laufzeit aller Eintragungen nach dem letzten und demnach am weitesten in der Zukunft liegenden Überprüfungsdatum zu richten. Bei einem pauschalen nachträglichen Hinausschieben des Prüfungsdatums (laut PoldDVG-E im Höchstfall um 20 Jahre (!) bei Erwachsenen) auch bei Delikten im sog. Bagatellbereich oder bei gänzlich fehlendem Sachzusammenhang oder Schweregrad bestehen jedoch erhebliche Zweifel, ob dies für die polizeiliche Aufgabenwahrnehmung notwendig und damit erforderlich i.S.d. JI-Richtlinie erscheint.

Eine polizeiliche Speicherung der Daten kann aus gänzlich unterschiedlichen Gründen erfolgen. Die Nachziehregelung in § 35 Abs. 3 PolDVG-E geht hier von einem unwiderlegbaren Erfordernis der Verlängerung der Speicherdauer aus. Diese Fiktion kann massive stigmatisierende Wirkung für Betroffene haben, da sie kumulativ alle Vorwürfe, die gegen einen Betroffenen innerhalb eines Zeitraum von dann maximal zwanzig Jahren erhoben werden, konserviert, ohne dass hier eine Prüfung der Erforderlichkeit vorgesehen wäre.

X. § 46 PolDVG-E Automatisierte Anwendung der Datenanalyse

Erhebliche datenschutzrechtliche Bedenken bestehen hinsichtlich des § 46 PolDVG-E.

Es ist bereits unklar, was unter die „*automatisierte Anwendung der Datenanalyse*“ fällt und somit letztlich, welche Eingriffe durch diese Norm gerechtfertigt werden sollen. Der Vorgang der „*automatisierten Anwendung der Datenanalyse*“ ist weder im Gesetz legal definiert, noch kann eine genauere Eingrenzung der Gesetzesbegründung entnommen werden. Weder die Art der personenbezogenen Daten, die genutzt werden sollen, noch aus welchen Dateien die Polizei diese ziehen kann, ergeben sich aus der vorliegenden Vorschrift. Auch fehlt dem Gesetz eine Begrenzung im Hinblick auf den zeitlichen Umfang der Maßnahme.

Während die (wohl) vergleichbare Vorschrift des § 6a Antiterrordateigesetz (ATDG) die Nutzung ausdrücklich auf „*einzelfallbezogene Projekte*“ begrenzt, einen zeitlichen Rahmen vorgibt und die Art der zu nutzenden personenbezogenen Daten festlegt, findet sich eine derartige Eingrenzung im vorliegenden Entwurf nicht. Lediglich in der Begründung wird die Feststellung getroffen, dass die „*automatisierte Anwendung zur Datenanalyse im Einzelfall erforderlich sein* (muss)“.

Ob durch diese Norm auch ein Einsatz von Technologien aus dem sog. Big-Data-Bereich zur Datenanalyse gerechtfertigt werden sollen, bleibt zumindest nach dem Wortlaut offen. Mangels Beschreibung und Begrenzung der zu verarbeitenden Datenarten, muss zudem davon ausgegangen werden, dass auch eine Verarbeitung von Lichtbildern und von besonderen Kategorien von Daten gem. Art. 10 JI-Richtlinie erfolgen kann.

Mangels normklarer Vorgaben lässt sich nicht erkennen, inwieweit limitierende Kriterien gegenüber umfassenden Massendatenverarbeitungen bestehen. Entgegen der Gesetzesbegründung, die vermuten lässt, dass davon ausgegangen wird, dass es sich nicht um einen erheblichen Grundrechtseingriff handeln soll („*lediglich die automatisierte Analyse*“ vgl. Begründung zu § 49 PolDVG-E, S. 104), dürfte auch dieser Datenverarbeitungsschritt einen intensiven Eingriff in das Recht auf informationelle Selbstbestimmung darstellen. So könnte § 46 PolDVG-E durchaus auch präventive Auswertungen von Videoaufzeichnungen durch automatisierte Gesichtserkennung ermöglichen, ohne dass damit den rechtsstaatlichen Anforderungen an Bestimmtheit und Verhältnismäßigkeit genügt wird.

Das Recht auf informationelle Selbstbestimmung schützt gerade das Interesse des Einzelnen, dass die mit seinem Verhalten in der Öffentlichkeit verbundenen, personenbezogenen Informationen nicht im Zuge automatischer Informationserhebung zur Speicherung mit der Möglichkeit der Weiterverwendung und Auswertung durch staatliche Stellen erfasst werden (BVerfG, Urt. v. 11.3.2008 – 1 BvR 1254/07, Rn. 67). Im Rahmen der Datenverarbeitung nimmt die Schwere des Eingriffs mit der Möglichkeit der Nutzung der Daten für Folgeeingriffe sowie mit der Möglichkeit der Verknüpfung mit anderen Daten zu, die wiederum Folgemaßnahmen auslösen können (zur Videoüberwachung: BVerfG, Beschl. v. 23.2.2007 – BvR 2368/06, Rn. 52; BVerfG, Urt. v. 11.3.2008 – 1 BvR 2074/05, Rn. 79).

Die Anforderungen an eine hinreichend bestimmte Ermächtigungsgrundlage im Sinne einer verfassungsgemäßen Schranke, die diese Art von Eingriffen zu rechtfertigen vermag, erfüllt diese Vorschrift daher nicht. Mangels hinreichender Bestimmtheit kann ein Betroffener anhand der Voraussetzung die Rechtslage nicht erkennen und sein Verhalten danach ausrichten (vgl. dazu: BVerfG, Urt. v. 12.4.2005 – 2 BvR 581/01, Rn. 49). Zudem wird die Entscheidung über

die Grenzen der Freiheit des Bürgers durch eine derart unbestimmte Formulierung einseitig in das Ermessen der Verwaltung gestellt (vgl. dazu: BVerfG, Urt. v. 27.7.2005 – 1 BvR 668/04, Rn. 118).

Zu den gesetzlich zu regelnden Mindestvoraussetzungen in einem solchen Fall zählen dabei nicht nur die – wie die zwar vorliegend in Abs. 1 geregelten – Anlassstraftaten für einen derartigen Einsatz, sondern auch Art und Umfang der personenbezogenen Daten sowie die Begrenzung des Zeitraums für einen derartigen Einsatz. Es bestehen zudem Zweifel, ob die vorliegende Vorschrift Anforderungen an prozedurale Vorgaben erfüllt. Verfahrensrechtliche Vorgaben wie ein Richtervorbehalt oder die Kontrolle entsprechender Datenbanken durch unabhängige Stellen sind erforderlich, um eine Kompensation der Rechte Betroffener, denen die Verarbeitung ihrer Daten regelmäßig nicht bekannt sein wird, vorzunehmen (vgl. zur Kompensationsfunktion der aufsichtlichen Kontrolle für schwach ausgestalteten Individualrechtsschutz BVerfG, Urt. v. 24.4.2013 – 1 BvR 1215/07, Rn. 213 ff.). Im Hinblick auf die mögliche Schwere des Eingriffes bestehen zunächst Bedenken bzgl. des Amtsleitervorbehalts in Absatz 3. Bei intensiven Eingriffen in die Grundrechte der Betroffenen – insbesondere dann, wenn der Betroffene eine eigene Kontrolle mangels Kenntnis nicht vornehmen kann – bedarf es grundsätzlich einer vorherigen Kontrolle durch eine unabhängige Stelle, z.B. in Form einer richterlichen Anordnung. Selbst bei Zulässigkeit eines Amtsleitervorbehalts wäre nicht nachvollziehbar, warum keine formellen Anforderungen an die Anordnung normiert werden (anders vgl. § 6a Abs. 7 ATDG) bzw. im Rahmen des § 46 Abs. 3 PolDVG-E nicht ebenfalls auf den § 20 Abs. 2 PolDVG-E verwiesen wird. Für polizeiliche Maßnahmen, die ohne Kenntnis des Betroffenen durchgeführt werden und daher grundsätzlich nur nachträglich auf ihre Rechtmäßigkeit überprüft werden können, dürfte bereits aus Art. 19 Abs. 4 GG die Erforderlichkeit einer nachprüfbaren, aktenkundigen Anordnung folgen. Nach dem Ausgeführten über die Eingriffsintensität derartiger Maßnahmen wird zudem die Aufnahme des § 46 PolDVG-E in den § 61 PolDVG-E (Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen) angeraten.

XI. § 48 PolDVG-E Zuverlässigkeitsüberprüfung

§ 48 PolDVG-E regelt die sog. Zuverlässigkeitsprüfung. Nach § 48 Satz 1 Nr. 1 PolDVG-E soll die Verarbeitung personenbezogener Daten im Zusammenhang derartiger Zuverlässigkeitsüberprüfungen zulässig sein, soweit sie mit Zustimmung der betroffenen Person erfolgt. Der Begriff der Zustimmung ist dem Datenschutzrecht fremd und ist auch in anderen Rechtsgebieten begrifflich vorgeprägt (vgl. §§ 183 f. BGB). Der Gesetzesbegründung lässt sich hierzu entnehmen, dass statt des bisher verwendeten Begriffs der Einwilligung an dieser Stelle von der erforderlichen Zustimmung gesprochen würde, da es bei letzterer gerade

nicht auf die Beurteilung der Freiwilligkeit ankommen solle (S. 105 der Begründung). Hiermit wird praktisch ein Rechtsinstitut sui generis für die Verarbeitung personenbezogener Daten geschaffen, dessen Voraussetzungen und Geltungsumfang vollkommen unklar sind. Dies begegnet erheblichen datenschutzrechtlichen Bedenken. Das Datenschutzrecht dient dem Schutz des Rechts auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG) und dem Grundrecht auf Datenschutz (Art. 8 EU-Grundrechtecharta). Von einer Selbstbestimmung kann jedoch dann keine Rede sein, wenn ein Eingriff in diese Grundrechte nicht auf Grundlage einer jedenfalls freiwilligen Entscheidung erfolgt. Fehlt es an einer solchen freiwilligen Entscheidung für einen Grundrechtseingriff, bedarf es zur Legitimation eines Eingriffs eines Gesetzes. Art. 8 Abs. 2 EU-Grundrechtecharta regelt daher:

> *„Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden.“*

Das Konstrukt einer „unfreiwilligen“ Zustimmung ist im Zusammenhang mit der Verarbeitung personenbezogener Daten folglich nicht vorgesehen.

XII. § 66 Abs. 2 und 3 PolDVG-E – Verweigerung der Auskunft

Durch § 66 Abs. 2 und 3 PolDVG-E wird die Auskunftserteilung an den Betroffenen beschränkt. Die Regelungen entsprechen zum Teil § 18 Abs. 2 und 3 HmbDSG a.F. Es bestehen aber Zweifel an der richtlinienkonformen Ausgestaltung der Absätze 2 und 3 PolDVG-E:

Nach Art. 15 JI-Richtlinie sind Ausnahmen für die Erteilung einer Auskunft zu den in Buchstabe a bis e bezeichneten Zwecken vorgesehen. Die Regelungen des § 66 Abs. 2 PolDVG-E beziehen sich nicht auf einen dieser bezeichneten Zwecke. Die in Absatz 2 genannten Zwecke finden keine Erwähnung in Art. 15 JI-Richtlinie. Aus der Gesetzesbegründung folgt auch kein Bezug auf die JI-Richtlinie, sondern alleine ein Hinweis darauf, dass die Regelung § 18 Abs. 2 HmbDSG entspricht. Eine Orientierung an den Vorgaben der Richtlinie wäre aber geboten gewesen (vgl. dazu *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, § 1, Rn. 193 zu § 57 BDSG).

Laut Begründung nimmt auch § 66 Abs. 3 PolDVG-E den Rechtsgedanken des § 18 HmbDSG a.F. auf, wonach bei einem unverhältnismäßigen Aufwand von einer Auskunftserteilung abgesehen werden kann, wenn der Betroffene keine Angaben macht, die das Auffinden der Daten ermöglichen. Wie in der Gesetzesbegründung zutreffend ausgeführt wird, dürfte dies gerade im Hinblick auf nicht suchfähig gespeicherte Daten bei einer Organisationseinheit wie der Polizei zu einem unverhältnismäßigen Verwaltungsaufwand führen, wenn z.B. auch nicht

suchfähig gespeicherte Daten – ohne vorherigen Hinweis – nach dem Gesetz zu beauskunften wären. Dies führt aber nicht dazu, dass die Bearbeitung des Auskunftsbegehrens von der Polizei stets davon abhängig gemacht werden darf, dass das Begehren näher konkretisiert wird. Eine derartige Einschränkung des Rechts auf Auskunft kann der JI-Richtlinie nicht entnommen werden. Es wird daher eine Klarstellung angeregt, wonach eine vollständige Auskunftserteilung über alle durch die Polizei nach § 1 verarbeiteten Daten nicht verlangt werden kann, wenn das Auffinden einzelner Daten einen unverhältnismäßigen Aufwand bedeuten würde. In seiner jetzigen Fassung ist § 66 Abs. 3 PolDVG-E europarechtswidrig.

XIII. § 69 PolDVG-E – Befugnisse

Nach § 69 Abs. 1 hat der HmbBfDI im Gegensatz zu den Regelungen der DSGVO nicht das Recht, Anordnungen gegenüber der Polizei zu treffen. Er kann lediglich seine eigene (!) Beanstandung gerichtlich überprüfen lassen. Die hierzu vorgetragenen Begründungen vermögen ausnahmslos nicht zu überzeugen.

Soweit die Gesetzesbegründung ausführt, dass dies für die Bereiche der Straftatenverhütung und der Gefahrenabwehr einschlägig sei, ist dies unzutreffend und europarechtswidrig. Die JI-Richtlinie gilt ausschließlich für den Bereich der straftatenverhütenden Gefahrenabwehr (s. dazu oben unter A. I.).

Die Begründung erklärt, dass sich eine Anordnungsbefugnis nicht mit der „*Sensibilität und Komplexität der entsprechenden Verarbeitungen*“ in Einklang bringen ließe. Gründe für diese Behauptung werden nicht vorgebracht. Die Befürchtung, dass entsprechende Anordnungen die Aufgabenwahrnehmung der Polizei konterkarieren, ist vorliegend unsubstantiiert, da weder eine sofortige Vollziehung noch eine Durchsetzung der Anordnung durch die Verwaltungsvollstreckung möglich ist.

Nach der Gesetzesbegründung ist der Ausschluss dieser Befugnisse nicht ausreichend und könne den Bedürfnissen der Polizei nicht genügen, denn bereits die mit der Anordnung verbundene Rechtsunsicherheit lasse befürchten, dass die Datenverarbeitung für die Dauer der Überprüfung ebenfalls unterbliebe.

M.a.W: Bereits das Existieren einer Anordnungskompetenz des HmbBfDI erzeuge eine Selbstblockade bei der Polizei, die Befugnisse zur Aufgabe der Gefahrenabwehr tatsächlich wahrzunehmen.

Ein Blick auf die Realität lässt hier freilich genau den umgekehrten Schluss zu: Im Hinblick auf das beim VG Hamburg anhängige Videmo-Verfahren (17 K 203/19) ist zu konstatieren, dass die Polizei sehr wohl mit einer Verarbeitung fortfährt, die vom HmbBfDI untersagt wurde. Während des laufenden Gerichtsverfahrens ist dies zulässig, die Argumente in der Gesetzesbegründung sind unzutreffend und realitätsfern. Aus der Perspektive des HmbBfDI stellt sich die Situation hingegen so dar, dass das derzeitige Recht der aufschiebenden Wirkung der Anfechtungsklage eine rechtswidrige Datenverarbeitung bis zum Erlass eines letztinstanzlichen Urteils – möglicherweise über Jahre hinweg - ermöglicht. Dies führt in der Praxis zu einer langandauernden Verletzung der Rechte und Freiheiten einer Vielzahl von betroffenen Personen. Der Ausschluss der sofortigen Vollziehbarkeit wird daher – jedenfalls mit Blick auf den Geltungsbereich der DSGVO – im Schrifttum als europarechtswidrig angesehen (vgl. *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, 2. Auflage 2018, § 20 BDSG, Rn. 12 ff).

Im Übrigen suggeriert die Gesetzesbegründung, dass die bisherige Rechtslage, nach der dem HmbBfDI die Befugnis einer Anordnung zustand, die polizeiliche Aufgabenwahrnehmung unangemessen erschwere. Davon kann keineswegs die Rede sein. Der HmbBfDI hat im Bereich der Regelung des § 6 UsmsAAG seit Geltung der JI-Richtlinie lediglich eine Anordnung erlassen. Diese bezieht sich auf den Einsatz automatisierter Gesichtserkennung, deren Zulässigkeit rechtsstaatlich umstritten ist.

Der Verweis auf die Wirksamkeit der Beanstandung einer Datenverarbeitung durch den HmbBfDI geht zudem aus rechtlicher Sicht fehl. Es kann als anerkannt gelten, dass die Beanstandung keine rechtlichen Folgen hat (siehe nur VG Stuttgart, Urt. v. 21.2.2019 – 14 K 17293/17, Rn. 25: „*Von Rechts wegen ist der Adressat der Beanstandung – mangels unmittelbarer Rechtswirkung – allerdings nicht verpflichtet, der Beanstandung Folge zu leisten*…*Aus der Sicht des Landesbeauftragten für die Informationsfreiheit mag die Erwartung bestehen, dass auf Grund der Beanstandung Abhilfe geschaffen wird; zwingend ist das allerdings nicht. Die informationspflichtige Stelle als Adressatin der Beanstandung kann ganz oder teilweise einlenken, sie kann sich dem Anliegen des Landesbeauftragten für die Informationsfreiheit aber auch verschließen, ohne dass dieser hiergegen einschreiten kann.*“; ebenso *Maatsch/Schnabel*, HmbTG, 2015, § 14, Rn. 50 f.; *Schoch*, IFG, 2. Aufl. 2016, § 12, Rn. 83; alle zur Informationsfreiheit mit entsprechenden Nachweisen zum Datenschutzrecht). Die Beanstandung ist derart wirkungslos, dass gegen sie gar nicht geklagt werden kann. Die Rechtsprechung lässt dies an der fehlenden Klagebefugnis oder dem Feststellungsinteresse scheitern (vgl. OVG SH, Beschl. v. 16.9.1991 – 1 L 18/91; SächsOVG, RDV 2011, 249 f.). Auch wenn sich die Begründungen unterscheiden, so besteht doch eine auffällige

Übereinstimmung in der Hinsicht, dass bislang alle Klagen gegen Beanstandungen bereits auf der Zulässigkeitsebene scheiterten.

Die Gesetzesbegründung ist daher unzutreffend. Es ist auch fraglich, ob die gesetzliche Regelung in der avisierten Form überhaupt möglich ist. Nach der Vorstellung der Gesetzesbegründung soll es dem HmbBfDI möglich sein, ein gerichtliches Verfahren im Hinblick auf die eigene Beanstandung einzuleiten. Woraus sich eine entsprechende Klagebefugnis ergeben soll, bleibt unklar. Nach der Rechtsprechung ist die Klagebefugnis aber auch für die Feststellungsklage nach § 43 VwGO erforderlich (vgl. *Pietzcker*, in: Schoch/Schneider/Bier, VwGO, Stand: 36. EL Februar 2019, § 43, Rn. 29 mit zahlr. Nw. aus der verwaltungsgerichtlichen Rspr.). Die landesrechtliche Anordnung des Vorliegens eines Feststellungsinteresses, Rechtsschutzbedürfnisses und einer Klagebefugnis begegnet kompetenzrechtlichen Bedenken.

Die Argumente der BIS werden auch nicht konsequent durchgehalten: Im Gegensatz zu § 69 PolDVG-E sieht § 58 Abs. 4 PolDVG-E ausdrücklich vor, dass der HmbBfDI von der Polizei die zu Unrecht unterlassene Benachrichtigung Betroffener von Datenschutzverstößen **verlangen** kann. Hierunter ist eine rechtlich verbindliche Anordnung zu verstehen, welche die Gesetzesbegründung in § 69 PolDVG-E für unvereinbar mit den Bedürfnissen der Polizei hält. Trotzdem wurde sie in § 58 Abs. 4 PolDVG-E eingeräumt. Die Gesetzesbegründung verhält sich dazu nicht.

Abschließend ist darauf hinzuweisen, dass der Entwurf zu § 69 PolDVG-E nicht nur rechtspolitisch verfehlt und unzutreffend begründet, sondern auch europarechtswidrig ist und der Gesetzgeber sich damit vollkommen unnötig der Gefahr einer Verurteilung durch den EuGH im Rahmen eines Vertragsverletzungsverfahrens wegen unzureichender Umsetzung der JI-Richtlinie aussetzt. Art. 47 Abs. 2 JI-Richtlinie verlangt vom Gesetzgeber des Mitgliedstaats,

„*dass jede Aufsichtsbehörde über wirksame Abhilfebefugnisse wie etwa die beispielhaft genannten folgenden verfügt, die es ihr gestatten,*

> *…*
>
> *b) den Verantwortlichen oder den Auftragsverarbeiter **anzuweisen**, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die **Anordnung** der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung gemäß Artikel 16;*

> *c) eine* ***vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen***."

Das Recht, Gerichte anzurufen, ist in Art 47 Abs. 5 JI-Richtlinie ausdrücklich und damit abweichend geregelt. Es ist keine Umsetzung der Forderungen aus Absatz 2. Ferner kann aus dem Vorliegen von Regelbeispielen nicht geschlossen werden, dass die Richtlinie umgesetzt wurde, wenn nicht einmal die Regelbeispiele erfüllt werden.
§ 69 PolDVG-E ist damit in seiner jetzigen Form unzureichend und europarechtswidrig. Auf Seiten des HmbBfDI bestehen keine wesentlichen Zweifel daran, dass der EuGH zu demselben Ergebnis kommen würde.

XIV. § 70 PolDVG-E

Die Regelung, dass der HmbBfDI die Einhaltung der Vorgaben der §§ 20 bis 31 und § 47 PolDVG-E spätestens alle zwei Jahre zu überprüfen hat, ist sinnvoll. Der HmbBfDI hat allerdings nicht die personellen Kapazitäten, dieser Verpflichtung nachzukommen. Im Zusammenspiel mit den zahlreichen Verpflichtungen nach der DSGVO sieht sich der HmbBfDI mit der momentanen personellen Ausstattung strukturell überfordert. Weitere Aufgaben ohne die entsprechende personelle Ausstattung würden das Problem noch verschärfen.

Das BVerfG hat wiederholt auf die hohe Bedeutung einer organisatorisch unabhängigen Kontrolle hingewiesen:

> „*Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu und sind solche Kontrollen in angemessenen Abständen - deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf - durchzuführen.* ***Dies ist bei ihrer Ausstattung zu berücksichtigen****.*" (BVerfG, Urt. v. 24.4.2013 – 1 BVR 1215/07, Rn. 217, „Antiterrordatei", Hervorhebung nur hier)

Das Bundesverfassungsgericht sah sich dazu genötigt, diese Forderung wortgleich zu wiederholen (vgl. BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 141, „BKA-Gesetz").

Hierbei handelt es sich um eine eindeutige Forderung des Bundesverfassungsgerichts, die bei der Anordnung von neuen Prüf- und Überwachungspflichten zu beachten ist. Es ist insoweit mit der Unabhängigkeit der Datenschutzaufsichtsbehörden im primären und sekundären Gemeinschaftsrecht, ebenso wie konkret mit der in Art. 60 a HV landesverfassungsrechtlich eingeräumten Unabhängigkeit des HmbBfDI nicht vereinbar, gesetzlich immer mehr Pflichten

zu schaffen, ohne deren Erfüllung durch die Schaffung angemessener personeller Ressourcen zu ermöglichen.

Die an sich sinnvolle Vorgabe ist daher nicht vollziehbar, wenn der HmbBfDI nicht die dringend benötigten personellen Ressourcen bekommt, um diesen Pflichten auch nachzukommen.

XV. §§ 70, 71 PolDVG-E

Der Begriff „Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit“ hat eine Doppelfunktion: Er bezeichnet sowohl die Behörde als auch die Behördenleitung in Person. Im Einzelfall kann es zu Verwirrungen kommen, ob die Behörde oder die Behördenleitung gemeint ist.

§ 69 Abs. 3 PolDVG-E gewährt „*der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit und ihren oder seinen Beauftragten*“ verschiedene Rechte. Die Verwendung des Begriffs „*ihren oder seinen Beauftragten*“ ist gewöhnungsbedürftig, es dürften aber keine Zweifel bestehen, dass insoweit die Beschäftigten des HmbBfDI gemeint sind. Eventuell ist hier ein besonderer „Beauftragungs-Akt“ der Behördenleitung erforderlich.
In diesem Kontext ist es problematisch, dass bei den Kompetenzen und Aufgaben des HmbBfDI in §§ 70, 71 PolDVG-E ausschließlich von „*der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit*“ gesprochen wird. Mit hoher Wahrscheinlichkeit handelt es sich hier lediglich um eine terminologische Ungenauigkeit und die Kompetenzen bzw. Pflichten sollen nicht ausschließlich der Person der Behördenleitung zustehen bzw. auferlegt werden. Eine Klarstellung ist jedoch angezeigt. Das Landesrecht kennt Beispiele, in denen Rechte ausschließlich der Person des HmbBfDI zustehen, zum Beispiel in § 14 Abs. 3 Satz 4 HmbTG („*Stellt der Senat im Einzelfall fest, dass durch eine mit der Einsicht verbundene Bekanntgabe von Informationen die Sicherheit des Bundes oder eines Landes gefährdet ist, dürfen die Rechte nach Absatz 2 nur von der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit persönlich oder von einer oder einem von ihr oder ihm schriftlich besonders damit Beauftragten ausgeübt werden*“).
Auch ist nach § § 2 Abs. 4 Nr. 7 HmbSÜGG ausschließlich die Person des HmbBfDI von einer Sicherheitsüberprüfung ausgenommen, nicht seine oder ihre Beschäftigten. Um Unklarheiten vorzubeugen, wird angeregt, die in § 69 Abs. 3 PolDVG-E und §§ 70, 71 PolDVG-E dieselben Formulierungen zu verwenden und ggf. in der Gesetzesbegründung klarzustellen, ob mit der Verwendung der Bezeichnung „HmbBfDI“ alle Beschäftigten der Behörde gemeint sind oder lediglich die Person der Behördenleitung.

B. Art. 3 – Hamburgisches Gesetz zur Aufsicht über die Anwendung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften (HmbRI (EU) 2016/680 UmsAAG)

Im Hinblick auf die Streichung der Anordnungsbefugnis auch im Bereich der strafverfolgungsrechtlichen Maßnahmen der Polizei im UmsAAG durch Artikel 3 ist auf die bereits zu § 69 PolDVG-E angeführten Argumente zu verweisen. Ferner ist hierzu anzumerken, dass die bereits mit § 6 UmsAAG gemachten Erfahrungen sich nicht dazu eignen, die Darstellung in der Gesetzesbegründung zu bestätigen. Es gab bislang eine einzige Anordnung des HmbBfDI. Diese hat nicht dazu geführt, dass die Polizei die aus ihrer Sicht dringend notwendigen Datenverarbeitungen unterlassen hat. Stattdessen ist ein gerichtliches Verfahren angestrengt worden, in welchem es zeitnah zu einer mündlichen Verhandlung kommen wird. Die gerichtlichen Entscheidungen werden Rechtsklarheit bringen und eine Situation vermeiden, in der es unklar ist, ob die Datenverarbeitungen der Polizei zulässig sind. Dies ist aus rechtsstaatlicher Sicht uneingeschränkt zu begrüßen.

Aus rechtspolitischer Sicht sei angemerkt, dass die avisierte Gesetzesänderung den missverständlichen – und unzutreffenden – Eindruck hinterlassen könnte, dass die Polizei vor einer rechtsverbindlichen Überprüfung ihres Handelns bewahrt bleiben soll. Hierfür besteht nach der festen Überzeugung des HmbBfDI kein Bedürfnis.

C. Informationsfreiheitsrechtliche Bedenken

Gegen den vorgelegten Entwurf bestehen keine informationsfreiheitsrechtlichen Bedenken.

Mit freundlichen Grüßen

[redacted]