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
Beteiligte Behörden und Ämter

Ludwig-Erhard-Str. 22, 7. OG
20459 Hamburg
Telefon: 040 - 428 54 - 40 50 Zentrale - 40 40
Telefax: 040 - 428 54 - 40 00
Ansprechpartnerin: [redacted]

E-Mail*: [redacted]@datenschutz.hamburg.de

Az.: 12.01-09 u.a.

Hamburg, den 22.07.2019

Stellungnahme zum Senatsdrucksachenentwurf „Novellierung Hamburgisches Verfassungsschutzgesetz u.a.“

Sehr geehrte Damen und Herren,

haben Sie vielen Dank für die Gelegenheit, zum vorbezeichneten Entwurf aus datenschutzrechtlicher Perspektive Stellung zu nehmen.

Erlauben Sie mir eine kurze Vorbemerkung: Die Drucksache hat einen erheblichen Umfang und behandelt komplexe datenschutzrechtliche Fragestellungen, bei denen es insbesondere auch zu überprüfen gilt, ob verschiedene Judikate des Bundesverfassungsgerichts (BVerfG) umgesetzt wurden.

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). Wir bitten darum, derartige Vorgaben zukünftig stärker zu berücksichtigen.

Die kurze Fristsetzung zur Stellungnahme bis zum 22. Juli 2019 gibt eine Bearbeitungszeit von 10 Werktagen vor. Angesichts der Bedeutung sowie Komplexität der Regelungen ist dies zu bedauern. Dass diese Frist gleichzeitig in die Ferienpause des Sommers fällt, in der auch Mitarbeiterinnen und Mitarbeiter des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit urlaubsbedingt abwesend sind, stellt eine weitere Erschwernis für eine seriöse fristgerechte Stellungnahme dar. Folglich kann die vorliegende datenschutzrechtliche Stellungnahme daher nur die grundsätzlichen Aspekte beleuchten, die durch die geplanten Regelungen aufgeworfen werden. **Insoweit bleibt ausdrücklich vorbehalten, einzelne Fragstellungen zu einem späteren Zeitpunkt aufzugreifen und weitere Argumente gegebenenfalls im Gesetzgebungsverfahren nachzureichen.**

Auf dieser Basis nimmt der HmbBfDI zum vierten Gesetz zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzrechts - wie folgt - Stellung:

I. Befugnisse, § 7 Abs. 1 des Sechstes Gesetz zur Änderung des Hamburgischen Verfassungsschutzgesetz (im Folgenden: HmbVerfSchG-E)

Entsprechend der Regelung in § 8 Abs. 1 Satz. 1 BVerfSchG wird in § 7 Abs. 1 S. 1 HmbVerfSchG-E die Zulässigkeit der Verarbeitung von personenbezogenen Daten aufgrund von Einwilligung neu geregelt.

Es ist zweifelhaft, ob eine Einwilligung überhaupt eine taugliche Rechtsgrundlage für die Verarbeitung durch Nachrichtendienste darstellen kann. Erfordernis einer wirksamen Einwilligung ist, 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. dazu DSGVO EG 43 zur Datenschutzgrundverordnung). Staatliche Stellen sollten im Bereich der Eingriffsverwaltung daher grundsätzlich nur auf Grundlage spezifisch geschaffener Rechtssätze tätig werden. Allgemein 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 Konstrukt einer Einwilligung sollte im Falle der Verarbeitung personenbezogener Daten daher durch öffentliche Stellen nur restriktiv genutzt werden.

II. Nachrichtendienstliche Mittel, § 8 HmbVerfSchG-E

Datenschutzrechtlich bedenklich ist zunächst, dass keine grundsätzliche nachträgliche Mitteilungspflicht zugunsten des Betroffenen bei der Erhebung durch nachrichtendienstliche Mittel vorgesehen wird. Lediglich bei Maßnahmen nach § 8 Abs. 3 ff. (Maßnahmen im Schutzbereich des Art. 13 Grundgesetz (GG) u.Ä.) und 12 HmbVerfSchG-E ist dies unter Verweis auf § 7a Abs. 7 HmbVerfSchG-E und § 12 Artikel 10-Gesetz vorgesehen. Für Maßnahmen wie das verdeckte Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter Einsatz technischer Mittel außerhalb von Wohnungen, Bildaufzeichnungen oder verdeckt eingesetzten Personen gilt dies aber nicht.

Heimliche Überwachungsmaßnahmen haben nach Rechtsprechung des Bundesverfassungsgerichts in aller Regel aber ein erhebliches Eingriffsgewicht in das Grundrecht auf informationelle Selbstbestimmung (BVerfG, Urteil v. 20.04.2016 – 1 BvR 966/06 Rn. 92 ff.). Es ist der Begründung zum Gesetz daher insoweit zuzustimmen, als daraufhin gewiesen wird, dass das in Rede stehende Urteil zwar ausschließlich Befugnisse des Bundeskriminalamtes untersucht, das Urteil aber allgemeine Vorgaben zu heimlichen Überwachungsmaßnahmen enthält, die zum Teil auf das Recht der Nachrichtendienste zu übertragen sind (S. 52 der Mitteilung des Senats an die Bürgerschaft). Daher gehört zu den Anforderungen an eine verhältnismäßige Ausgestaltung von heimlich durchgeführten Überwachungsmaßnahmen u.a. die gesetzliche Anordnung von Benachrichtigungsmaßnahmen, weshalb der Betroffene also grundsätzlich nachträglich in Kenntnis zu setzen ist (BVerfG, Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 134 ff.). Zwar können gerade im Bereich der Nachrichtendienste Geheimhaltungsinteressen im Einzelfall dem entgegenstehen, ein grundsätzlicher Verzicht dürfte aber nicht geboten sein.

Zudem wird angeraten, bei dem Einsatz von nachrichtendienstlichen Mitteln detaillierte Protokollierungsregeln aufzunehmen. Das Bundesverfassungsgericht führt nämlich ebenfalls aus, dass – gerade weil eine Transparenz der Datenerhebung und –verarbeitung sowie die Ermöglichung individuellen Rechtsschutzes für heimliche Überwachungsmaßnahmen nur sehr eingeschränkt sichergestellt werden kann – der Gewährung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung zukommt. Diese aufsichtliche Kontrolle ist wiederrum jedoch nur hinreichend möglich, wenn eine Protokollierung durchgeführt wird (BVerfG, Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 134 ff.).

Darüber hinaus erscheint sehr zweifelhaft, ob die Norm die Anforderungen an den Bestimmtheitsgrundsatz erfüllt, wenn nachrichtendienstliche Mittel lediglich in einer

Dienstvorschrift und nicht im Gesetz ausgeführt werden gem. § 8 Abs. 2 Satz 2 HmbVerfSchG-E.

III. Vertrauensleute, § 8a HmbVerfSchG-E

Grundsätzlich begrüßt wird zunächst die Aufnahme einer eigenständigen gesetzlichen Regelung zum Einsatz von sog. Vertrauensleute.

Der Entwurf betont wiederholt die Ausrichtung an den Regelungen des BVerfSchG auch für den Einsatz menschlicher Quellen zur verdeckten Informationsgewinnung (S. 66, 67 der Mitteilung an den Senat). Hierunter fällt neben dem Einsatz von Vertrauensleuten nach § 8a Abs. 1 aber auch der Einsatz von Mitarbeitern des Landesamtes für Verfassungsschutz gem. § 8 Abs. 2 Satz 1 Nummer 1. Es fehlen jedoch klare Definitionen sowie eine rechtliche Systematik wie in § 9a und 9b BVerfSchG auf Bundesebene. Insbesondere sind bei den Bestimmungen über verdeckt eingesetzte hauptamtliche Mitarbeiter des Landesamtes für Verfassungsschutz die Zulässigkeitskriterien aus § 9a Abs. 2 BVerfSchG im Entwurf nicht enthalten. Zudem dürfte es sich hier um eine heimliche und daher besonders eingriffsintensive Maßnahme handeln. Eine nachträgliche Mitteilung an den Betroffenen ist daher geboten (vgl. unter II.).

IV. Verarbeitung personenbezogener Daten in Akten und Dateisystemen, § 9 Abs. 2 und Abs. 3 HmbVerfSchG-E, § 18 Novellierung des Hamburgischen Sicherheitsüberprüfungs- und Geheimschutzgesetz (Im Folgenden: HmbSÜG-E)

Nicht nachvollziehbar erscheint zunächst die Heraufsetzung der Prüfungsfrist von vier Jahren ab der Speicherung auf fünf Jahre nach der letzten relevanten Speicherung nach § 9 Abs. 2 HmbVerfSchG-E. Um den Schutz des Persönlichkeitsrechts der Betroffenen in seiner Ausformung des Rechts auf informationelle Selbstbestimmung zu gewährleisten, muss eine das Grundrecht einschränkende Regelung den Grundsatz der Verhältnismäßigkeit achten. Personenbezogene Daten dürfen demnach nicht länger gespeichert werden, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dabei wird sich bei der nun erfolgten Heraufsetzung an der Regelung des Bundes orientiert. Der in der Begründung für die Heraufsetzung dazu lediglich aufgeführte „*Mehraufwand*“ durch die Erstreckung der Erforderlichkeitsprüfung auf Akten dürfte dabei aber eine sachfremde Erwägung darstellen (S. 69 der Mitteilung des Senats).

Zweifelhaft erscheint, ob § 9 Abs. 3 HmbVerfSchG-E den Besonderheiten im Zusammenhang mit der elektronischen Aktenführung hinreichend Rechnung trägt. Begrüßt wird zunächst die Aufnahme des Absatzes 3 Satz 2, wonach klargestellt wird, dass die Regelungen über die Verarbeitung von (schriftlichen) Akten auch auf die elektronischen Akten Anwendung findet und eben nicht die Dateiregelungen. Darüber hinaus ist der Begründung zum Entwurf insoweit zuzustimmen, dass – auch wenn die in elektronischer Form geführte Akte wie eine herkömmliche Papierakte zu behandeln ist – dennoch eine größere datenschutzrechtliche Gefährdung von elektronischen Akten und damit automatisiert verarbeiteten personenbezogenen Daten vorliegt (S. 70 d. Mitteilung des Senats). Die elektronische Aktenführung eröffnet gegenüber der herkömmlichen schriftlichen Aktenführung nämlich ganz neue Nutzungsmöglichkeiten. Eine elektronisch geführte Akte vereinfacht nicht nur Arbeitsabläufe, sondern ermöglicht es (theoretisch), personenbezogene Daten aus Akten zu recherchieren, zu verknüpfen, auszuwerten und abzugleichen. 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 aber 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).

Konsequenterweise muss daher die Rechtsgrundlage für das Führen von Akten an diese Besonderheiten im Zusammenhang mit der elektronischen Aktenführung angepasst werden. Es ist aber zu bezweifeln, dass zur *„Kompensation der im Vergleich zur Papierakte größeren datenschutzrechtlichen Gefährdung von in elektronischen Akten (…) verarbeiteten personenbezogenen Daten“*, sowohl die Regelungen in den Absätze 1 und 2, sowie des Minderjährigenschutz nach § 10 ausreichen (Mitteilung des Senats S. 70). So stellt zwar § 9 Abs. 1 klar, dass eine Abfrage von personenbezogenen Daten Dritter auch aus elektronischen Akten grundsätzlich nicht zulässig ist (vgl. § 13 Abs. 4 Satz 3 BVerfSchG), eine Eingrenzung des durch die elektronische Aktenführung möglich gemachten automatisierten Abgleichs dürfte von dieser Regelung jedoch nicht erfasst sein (anders: § 13 Abs. 4 Satz 4 BVerfSchG). Insbesondere wird aber - um die Kontrolle der Einhaltung der Nutzungsbeschränkungen der elektronischen Akten verfahrensmäßig zu sichern (Begründung zu § 13 BVerfSchG, Drs. 18/4654 S. 31) - angeraten, Protokollierungspflichten für Zwecke der Datenschutzkontrolle nach dem Vorbild des § 13 Abs. 4 Satz 5 BVerfSchG aufzunehmen. Eine unabhängige Datenschutzkontrolle nach § 23b HmbVerfSchG-E ist nämlich überhaupt nur möglich, wenn die Datenverarbeitung protokolliert wird (BVerfG, Urteil vom 20.04.2019 – 1 BvR 966/06 u.a. Rn. 140 ff.). Entsprechendes ist für § 19 Abs. 9 HmbSÜG-E anzumerken.

V. Verarbeitung von Daten Minderjähriger, § 10 HmbVerfSchG-E

Datenschutzrechtliche Bedenken bestehen insbesondere hinsichtlich der Herabsetzung des Schutzes Minderjähriger. Die vorliegende Vorschrift geht dabei weit über die Bestimmungen im BVerfSchG hinaus:

Das betrifft zunächst das Alter der minderjährigen Betroffenen, deren Daten gespeichert werden dürfen, das auf zwölf Jahre abgesenkt wird, sowie die im Bundesrecht nicht vorgesehene Möglichkeit, persönliche Daten von Minderjährigen jeden Alters aus Gründen des Kindeswohls zu speichern, um sie gegenüber anderen öffentlichen Stellen nach § 14 HmbVerfSchG-E offenzulegen. Schließlich ergibt sich auch eine niederschwelligere Eingriffsbefugnis: Anders als in § 11 BVerfSchG ist nicht die Begehung oder Planung einer qualifizierten Straftat erforderlich, sondern es reicht nach § 10 Abs. 1 Nr. 1 lit. b HmbVerfSchG-E bereits aus, dass die Informationen für die Erforschung oder Bewertung der Bestrebung der Tätigkeit erforderlich sind.

Im Bereich des Schutzes von Minderjährigen werden damit für das Landesamt für Verfassungsschutz erweitere Eingriffskompetenzen, die das Bundesrecht so nicht kennt, geschaffen. Warum hier von den Regelungen des Bundes abgewichen werden soll und ob eine Verhältnismäßigkeit derartiger Regelungsermächtigungen gegenüber in besonderer Weise schutzbedürftigen minderjährigen Personen gegeben ist, erscheint fraglich.

Bislang galt, dass „Jugendsünden“ nicht auf Dauer vorgehalten werden dürfen (vgl. BT-Drs. 11/4306 S. 62) und derartige Speicherungen somit den Minderjährigen nicht in ihrer weiteren Entwicklung behindern oder im Wege stehen (z.B. im Rahmen von Sicherheitsüberprüfungen). Gerade auch die Verarbeitung von Daten aus Gründen des Kindeswohls darf nicht zum Deckmantel werden, die untere Grenze von 12 Jahren für die Datenerhebung noch zu unterschreiten. Hier fehlt insoweit eine Löschverpflichtung, die nach Offenlegung der Daten gegenüber einer anderen öffentlichen Stelle umzusetzen ist.

Bedenken bestehen auch bzgl. der Speicherdauer für Minderjährige. Bei Minderjährigen vor als auch nach Vollendung des 14. Lebensjahres kann die Speicherung über die zwei (vor Vollendung) bzw. 5 (nach Vollendung) bis auf die maximale Speicherdauer nach § 11 Abs. 2 Nr.4 HmbVerfSchG-E erhöht werden, wenn eben Voraussetzungen nach § 4 Abs. 1 HmbVerfSchG-E vorliegen. Dabei ist unklar, ob dann ebenfalls das in § 10 Abs. 1 Nr. 1 normierte zusätzliche Erfordernis der „*erheblichen Bedeutung*“ der Informationen über Minderjährige für Tätigkeiten nach § 4 Abs. 1 gilt oder „nur“ Erkenntnisse nach § 4 Abs. 1 HmbVerfSchG-E vorliegen müssen.

VI. Offenlegung personenbezogener Daten gegenüber ausländischen öffentlichen Stellen, § 16 HmbVerfSchG-E

Der Ausgestaltung der Offenlegung personenbezogener Daten gegenüber ausländischen öffentlichen Stellen unterliegt datenschutzrechtlichen Bedenken.

Eine Übermittlung von Daten in Drittstaaten ist nach der Rechtsprechung sowohl des EuGH, des EGMR und des Bundesverfassungsgerichts nur zulässig, wenn durch den dortigen Umgang mit den übermittelten Daten nicht die Garantien des menschenrechtlichen Schutzes personenbezogener Daten im Empfängerstaat unterlaufen werden (vgl. EuGH, Urteil v. 06.10. 2015 - C-362/14, Schrems/Digital Rights Ireland, NJW 2015, S. 3151 (3155); vgl. auch Art. 8 EMRK; dazu EGMR [GK], Zakharov v. Russland, Urteil v. 04.12.2015, Nr. 47143/06, §§ 227 ff.). Zwar ist für die ausländische Rechtsordnung auf der Empfängerseite keine institutionelle und verfahrensrechtliche Sicherung der Grundrechte nach deutschem Vorbild zu fordern. Dennoch hält es das Bundesverfassungsgericht für geboten, dass ein angemessenes materielles datenschutzrechtliches Niveaus für den Umgang mit den übermittelten Daten im Empfängerstaat vorhanden ist, wozu ausdrücklich gefordert wird, dass im Empfängerstaat die Grenzen durch Zweckbindung und Löschungspflichten sowie grundlegende Anforderungen an Kontrolle und Datensicherheit wenigstens grundsätzlich Beachtung finden (BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 334 ff.). Der EuGH stellt auf die innerstaatlichen Rechtsvorschriften und die internationalen Verpflichtungen des Empfängerstaats sowie ihre Umsetzung in der täglichen Anwendungspraxis ab (vgl. ähnlich EuGH, Urteil vom 06.10. 2015 - C-362/14, Schrems/Digital Rights Ireland, NJW 2015, S. 3151 (3155)).

Nach Auffassung des Bundesverfassungsgerichts hat der nationale Gesetzgeber daher Sorge zu tragen, dass der Schutz der Europäischen Menschenrechtskonvention und der anderen internationalen Menschenrechtsverträge (vgl. Art. 1 Abs. 2 GG) durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen nicht ausgehöhlt wird. Er kann diesbezüglich auch eine generalisierende tatsächliche Einschätzung der Sach- und Rechtslage der Empfängerstaaten vorsehen, aber auch die Abgabe von Einzelgarantien kann hier ausreichen (vgl. hierzu näher BVerfG Urteil v. 20.04.2016 – a.a.O., Rn. 339).

Dass eine Offenlegung nach § 16 Satz 3 bzw. § 21 des Entwurfs zu unterbleiben hat, wenn auswärtige Belange der Bundesrepublik oder überwiegende schutzwürdige Interessen der

betroffenen Person entgegenstehen, reicht nicht, um von einer gesetzlichen Pflicht zur Überprüfung des Datenschutzniveaus des Empfängerstaates abzusehen. Ausdrücklich weist das Bundesverfassungsgericht darauf hin, dass die Vergewisserung über das geforderte Schutzniveau keine Entscheidung ist, die der freien politischen Willensbildung deutscher Stellen unterliegt, sondern durch die Datenschutzbeauftragten überprüfbar und einer gerichtlichen Kontrolle zugänglich sein muss (BVerfG Urteil v. 20.04.2016 – a.a.O., Rn. 339). Davon kann allerdings keine Rede sein, wenn eine gesetzliche Regelunge hierzu und damit jegliche verfahrensleitende Bestimmungen zur Offenlegung der Daten an Drittstaaten fehlt und derartige Offenlegungen zu Zwecken der Nachprüfung darüber hinaus nicht zu dokumentieren sind (anders: § 16 Abs. 3 Satz 3 BVerfSchG). Insoweit wird die Entwurfsregelung dem grundrechtlichen Schutzgehalt des informationellen Selbstbestimmungsrechts nicht gerecht.

VII. Offenlegung personenbezogener Daten gegenüber Stellen außerhalb des öffentlichen Bereichs, § 17 HmbVerfSchG-E

Es bestehen grundsätzliche datenschutzrechtliche Bedenken gegen die Ermächtigungsgrundlage zur Offenlegung von personenbezogenen Daten gegenüber Stellen außerhalb des öffentlichen Bereichs. Sowohl nach der (noch) geltenden Fassung, als auch im Bund nach § 19 Abs. 4 Satz 1 BVerfSchG wird ein grundsätzliches Verbot der Offenlegung personenbezogener Daten an nichtöffentliche Stellen mit Erlaubnisvorbehalt normiert (Mitteilung d. Senats S. 80).

Inwiefern es nunmehr eine Abkehr von diesem Grundsatz bedarf, ist nicht ersichtlich und kann auch der Begründung nicht zweifelsfrei entnommen werden. Nach § 4 HmbVerfSchG-E ist Aufgabe des Landesamtes für Verfassungsschutz allein die Sammlung und Auswertung von Informationen. Es handelt sich nicht um eine operative Aufgabenwahrnehmung. Nachrichtendienste arbeiten grundsätzlich verdeckt und sind auf Beobachtung und Aufklärung im Vorfeld beschränkt (BVerfG, Urteil 24.04.2013 -1 BvR 1215/07, Rn. 122). Grundsätzliche Ausführungen zur Öffentlichkeitsarbeit des Verfassungsschutzes (Herausgabe von Publikationen, Broschüren und Flyern etc.) in der Begründung zum Gesetz vermögen nicht zweifelsfrei klarzustellen, inwieweit die gesetzlich festgelegten Aufgaben des Nachrichtendienstes überhaupt durch **die Offenlegung** von personenbezogenen Daten **gegenüber Privaten** wahrgenommen werden können. Zudem sei darauf hingewiesen, dass die äußerst sensiblen Informationen – wenn sie an private Stellen übermittelt werden – sich im Hinblick auf Speicherung und anderweitiger Nutzung außerhalb des Wirkungs- und Kontrollbereichs des Landesamts für Verfassungsschutz befinden. Eine Stigmatisierung der Betroffenen im privaten Bereich ist daher zu befürchten.

VIII. Offenlegung personenbezogener Daten gegenüber der Öffentlichkeit, § 18 HmbVerfSchG-E

Bezüglich der neu aufgenommenen Norm stellt sich zunächst die Frage der Erforderlichkeit einer solchen Regelung. Nicht dargelegt wird, ob in der Vergangenheit ein praktisches Bedürfnis dafür bestand bzw. sich zu dieser Art der Offenlegung ergeben hat. Angeraten wird jedenfalls die Aufnahme der „zwingenden Erforderlichkeit" im Gesetzeswortlaut, um der durch die Veröffentlichung zu erwartenden erhebliche Eingriffstiefe gerecht zu werden.

IX. Offenlegung personenbezogener Daten gegenüber dem Landesamt für Verfassungsschutz, § 19 HmbVerfSchG-E

Grundsätzlich zu begrüßen ist die Bestrebung „*im Sinne der Datensparsamkeit nicht erforderliche Offenlegungen*" von personenbezogenen Daten gegenüber dem Landesamt für Verfassungsschutz durch Einfügung des § 19 Abs. 2 Satz 2 HmbVerfSchG-E zu vermeiden (S. 82 der Mitteilung des Senats). Empfohlen wird allerdings eine deutlichere Gestaltung der Norm dahingehend, dass dies zum einen nicht als zusätzliche/eigene Verpflichtung zur Übermittlung von personenbezogenen Daten verstanden werden soll und zum anderen, dass die Nennung von personenbezogenen Daten grundsätzlich zur Klärung nicht erforderlich sein dürfte.

X. Übermittlung von personenbezogenen Daten Minderjähriger, § 22 HmbVerfSchG-E

Bezüglich der Herabsetzung des Schutzes von Minderjährigen - sowohl im Hinblick auf die Altersgrenze als auch der weiteren Voraussetzungen - bei Verarbeitung personenbezogener Daten durch das Landesamt für Verfassungsschutz wird auf die Ausführungen zu § 10 HmbVerfSchG-E verwiesen.

Im Hinblick auf die Schutzbedürftigkeit von Minderjährigen vor und nach Vollendung des 14. Lebensjahres sollte von einer Offenlegungsbefugnis generell auch gegenüber privaten Stellen nach § 17 HmbVerfSchG-E abgesehen werden. Auch hier vermag die Begründung (S. 84 der Mitteilung des Senats) durch Nennung von „*sachgerecht*(e) *Mitarbeit an Präventionsprojekten und Deradikalisierungsprogrammen*" nicht zu überzeugen, inwiefern die Übermittlung von personenbezogenen Daten Minderjähriger an private Stellen dafür erforderlich erscheint. Zudem dürfte Präventionsprojekten immanent sein, dass eine Gefährdung durch eine konkrete

Person gerade nicht vorliegt. Der angemessene Ausgleich zwischen dem Schutz der Minderjährigen und dem öffentlichen Sicherheitsbedürfnis ist nicht ersichtlich.

XI. Auskunftserteilung, § 23 HmbVerfSchG-E

Der datenschutzrechtliche Auskunftsanspruch trägt dem in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG enthaltenen Grundrecht auf informationelle Selbstbestimmung Rechnung und bildet die Voraussetzung für die Ausübung von weiteren Rechten, wie z.B. Berichtigung, Sperrung und Löschung sowie die Basis für gegebenenfalls gerichtlichen Rechtsschutz. Wäre der Bürger gehindert, Kenntnis davon zu erlangen, wer wo über seine personenbezogenen Daten in welcher Weise und zu welchem Zweck verfügt, so wäre sein Rechtsschutz verfassungsrechtlich unzureichend (BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83 u.a., Rn. 209). Es erscheint zunächst zweifelhaft, ob die nun neu eingefügte Abhängigkeit der Auskunft von Hinweisen auf einen konkreten Sachverhalt und Darlegung eines besonderen Interesses nach dem Vorbild der Regelung im Bund im Hinblick der dargelegten Bedeutung des Auskunftsrechts gerecht wird. Zudem überrascht diese Eingrenzung. Eine Notwendigkeit für eine derartige Beschränkung des Auskunftsrechts ohne Ermessen ist nicht in der Begründung dargelegt worden und auch nicht ersichtlich. Dies erscheint auch im Hinblick auf die ausführlich normierten Versagungsgründe in Absatz 2 zweifelhaft. Die Versagungsgründe tragen dem Bedürfnis der Geheimhaltung im Einzelfall Rechnung.

XII. Stellung, Aufgaben und Befugnisse der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit im Anwendungsbereich des HmbVerfSchG-E und HmbSÜG-E, §§ 23 Abs. 4, 23b Abs. 3 Satz 3 HmbVerfSchG-E und § 36a Abs. 3 Satz 3 HmbSÜG-E

§ 23 HmbVerfSchG-E regelt die Auskunftserteilung an die betroffene Person durch das Landesamt für Verfassungsschutz. § 23b HmbVerfSchG-E und § 36a HmbSÜG-E haben die Gestaltung der unabhängigen Datenschutzkontrolle zum Gegenstand.

§ 23b Abs. 1 HmbVerfSchG-E und § 36a Abs. 1 HmbSÜG-E sehen lediglich vor, dass sich Betroffene an den HmbBfDI wenden können und dieser beim Landesamt für Verfassungsschutz die Einhaltung der Vorschriften für den Datenschutz kontrolliert (§ 23b Abs. 2 Satz 1 HmbVerfSchG-E, § 36a Abs. 2 Satz 1 HmbSÜG-E). Eigene Befugnisse des HmbBfDI, die über die in § 23b Abs. 2 Satz 2 HmbVerfSchG-E aufgeführte Möglichkeit, die Öffentlichkeit im Rahmen seiner Zuständigkeit zu informieren, hinausgehen, sind nicht vorgesehen. Insbesondere besteht weder die gemäß § 25 Hamburgisches Datenschutzgesetz (HmbDSG) a.F. vorgesehene Möglichkeit der Beanstandung bei Rechtsverstößen, noch die Möglichkeit

weitere aufsichtsbehördliche Maßnahmen nach Art. 58 DSGVO zu ergreifen, da Art. 58 DSGVO durch § 23c Satz 1 HmbVerfSchG-E für unanwendbar erklärt wird. Das ist ein Rückfall nicht nur hinter die neuen EU-Standards der DSGVO wie auch der EU-JI-Richtlinie, sondern gegenüber dem seit Jahrzehnten geltenden Konzept einer völlig unabhängigen Kontrollstelle auch mit Blick auf das Landesamt für Verfassungsschutz.

Darüber hinaus sind gemäß der §§ 23 Abs. 4, 23b Abs. 3 Satz 3 HmbVerfSchG-E und § 36a Abs. 3 Satz 3 HmbSÜG-E die verbleibenden Befugnisse des HmbBfDI ausgeschlossen, wenn festgestellt wird, dass durch die Auskunft an den HmbBfDI „die Sicherheit des Bundes oder eines Landes gefährdet würde“. Diese Feststellung hat durch den Präses der BIS (§ 23 Abs. 4 HmbVerfSchG-E) bzw. den Senat (§ 23b Abs. 3 Satz 3 HmbVerfSchG-E) bzw. die Leitung des Landesamt für Verfassungsschutz (§ 36a Abs. 3 Satz 3 HmbSÜG-E) zu erfolgen. Die Regelung entspricht § 15 BVerfSchG und § 16 Abs. 3 Satz 4 HmbDSG.

Soweit § 16 Abs. 2 Satz 4 HmbDSG im Anwendungsbereich der DSGVO die Befugnisse der Aufsichtsbehörde beschneidet, bestehen Bedenken gegen die Europarechtskonformität der Norm. Die Feststellung, dass die Sicherheit des Bundes oder des Landes bedroht sei, ist wohl nicht gerichtlich überprüfbar. Der HmbBfDI kann insoweit keine eigenen Rechte geltend machen, die Überprüfung durch den HmbBfDI dürfte auch kein einklagbares Recht der betroffenen Person sein.

Es bestehen erhebliche Zweifel an der Verfassungsmäßigkeit einer solchen Einschränkung. Das Bundesverfassungsgericht hat wiederholt die herausgehobene Bedeutung der unabhängigen aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz betont (vgl. BVerfG, Urt. v. 24.4.2013 – 1 BVR 1215/07, Rn. 217; ebenso BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 141). Gerade in einem Bereich, in dem das Recht der Betroffenen aus Gründen des öffentlichen Interesses stark eingeschränkt wird, kommt der aufsichtlichen Kontrolle durch die Datenschutzbehörden eine Kompensationsfunktion zu. Die Befugnisse des Landesamts für Verfassungsschutz bestehen weit überwiegend in der verdeckten Datenerhebung. Hier ist die aufsichtliche Kontrolle nicht nur ein wünschenswerter Ausgleich zu erheblichen, verdeckten Grundrechtseingriffen, sondern in weiten Teilen ein verfassungsrechtliches Erfordernis, das Grundrechtseingriffe überhaupt erst angemessen und damit verfassungsgemäß machen kann. Das BVerfG hat dazu ausgeführt: „*Weil eine Transparenz der Datenerhebung und -verarbeitung sowie die Ermöglichung individuellen Rechtsschutzes für heimliche Überwachungsmaßnahmen nur sehr eingeschränkt sichergestellt werden können, kommt der Gewährleistung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung zu. Der Verhältnismäßigkeitsgrundsatz stellt für tief in die Privatsphäre reichende Überwachungsmaßnahmen deshalb an eine wirksame Ausgestaltung*

dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen (vgl. BVerfGE 133, 277 <369 Rn. 214>).“ – (BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 140.)

Die Beschränkung der Befugnisse des HmbBfDI steht einer wirksamen Kontrolle jedoch entgegen. Eine derartige Beschränkung hat daher mittelbare Auswirkungen auf die Frage der Rechtmäßigkeit der Eingriffsbefugnisse.

Unabhängig von der Frage der Verfassungsmäßigkeit ist darauf zu verweisen, dass Hamburg in anderen Gesetzen anders verfährt. Es erscheint daher sinnvoll, im HmbVerfSchG-E und HmbSÜG-E den gleichen Weg zu gehen wie im Hamburgischen Transparenzgesetz und der vom Parlament gewählten Person des HmbBfDI ein besonderes Vertrauen entgegenzubringen. Hierfür spricht schon der Umstand, dass der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit wie die Mitglieder der Bürgerschaft, der Präsident des Hamburgischen Verfassungsgerichts und der Erste Bürgermeister nach § 2 Abs. 4 Nr. 7 HmbSÜG-E von der Sicherheitsüberprüfung ausgenommen ist.

§ 14 Abs. 3 Satz 4 HmbTG sieht vor: „*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*“.

Die Regelung im HmbTG entspricht der Stellung und der Bedeutung des HmbBfDI und gilt in der rechtswissenschaftlichen Literatur als vorbildlich (*Schnabel*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 24. Edition 2018, § 12 IFG, Rn. 44 im Vergleich zum Bundesrecht).

Wird die in §§ 23 Abs. 4, 23b Abs. 3 Satz 3 HmbVerfSchG-E und § 36a Abs. 3 Satz 3 HmbSÜG-E vorgesehene Regel Gesetz, so wäre dies in verschiedener Hinsicht bedenklich: Die Rechtslage wäre zersplittert. Der HmbBfDI wäre im Transparenzbereich mit stärkeren Rechten ausgestattet als im HmbVerfSchG und im HmbSÜG-E. Die Frage, ob er die entscheidungserheblichen Unterlagen einsehen dürfte oder nicht, hinge davon ab, ob der Zugang nach dem Datenschutz- oder dem Transparenzrecht begehrt wird. Eine Angleichung der beiden Rechtsgebiete sollte auf dem Niveau des Transparenzrechts erfolgen, in dem Hamburg eine bundesweite Vorreiterrolle einnimmt.

XIII. Abhilfebefugnisse des HmbBfDI

Diese Bedenken werden dadurch erhärtet, dass das HmbVerfSchG-E und HmbSÜG-E bei Verstößen des Landesamts für Verfassungsschutz gegen Datenschutzbestimmungen keine Abhilfebefugnisse des HmbBfDI vorsieht.

Im Anwendungsbereich der DSGVO ergeben sich die Befugnisse der Aufsichtsbehörde unmittelbar aus Artikel 58 DSGVO. Art. 58 Abs. 2 stattet die Aufsichtsbehörde mit verschiedenen Abhilfebefugnissen aus. Diese ermöglichen der Aufsichtsbehörde ein direktes Einschreiten gegenüber der Aufsicht unterworfenen Regelungsadressaten. Das Spektrum der Abhilfebefugnisse reicht von einer Warnung bis zu einer verbindlichen Anweisung gegenüber einem Verantwortlichen, datenschutzrechtlich gebotene Handlungen vorzunehmen. Dies halten wir aus verfassungsrechtlichen und rechtspolitischen Gründen auch in diesem Bereich für geboten.

Offenbar soll das Landesamt für Verfassungsschutz – anders als Polizei und Staatsanwaltschaft – von einer gerichtlichen Klärung offener Rechtsfragen durch eine unabhängige Datenschutzaufsicht frei gehalten werden. Aus rechtsstaatlichen Gründen und zur Stärkung des Schutzes von Grundrechten Betroffener ist dies zu bedauern. Beim Recht der Nachrichtendienste handelt es sich bislang um ein im Wesentlichen rechtsprechungsfreies Recht. Eine gerichtliche Klärung könnte erheblich zur Stärkung der Legitimation des Landesamts für Verfassungsschutz beitragen. Das gilt auch für Verwarnungen oder Rügen bzw. Warnungen, die im Rahmen der allgemeinen EU- Datenschutzregelungen als Standardabhilfebefugnisse bestehen. Dass der Gesetzentwurf hier keine Bestimmungen vorsieht stelle eine verfassungsrechtlich zweifelhafte Privilegierung des Landesamts für Verfassungsschutz dar.

Im Verfassungsschutzbereich geht dem Gesetzgeber anscheinend selbst die Beanstandung, die eine formelle Rüge von Verwaltungshandelns ermöglicht, zu weit. Nach der nun vorgesehenen Regelung hätte der HmbBfDI keinerlei Kompetenzen mehr. Nicht einmal die Beanstandung soll möglich sein. Dabei ist die Beanstandung nicht mehr als ein rechtlicher Hinweis an die Behördenleitung sowie die gesetzlich geregelte Möglichkeit, die gleiche Rechtsmeinung auch dem Senat als Ganzem vorzutragen. Es besteht kein Anlass, dem HmbBfDI im Verfassungsschutzbereich wirksame Abhilfebefugnisse vorzuenthalten. Selbst im Bundesrecht hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit aufgrund der Verweisung in § 27 BVerfSchG auf § 16 Abs. 2 Bundesdatenschutzgesetz (BDSG) die Möglichkeit, eine Beanstandung auszusprechen. Die Rechtslage im Bundesrecht

ist alles andere als ein Garant für den effektiven Schutz von Bürgerrechten. Sie auch noch zu unterschreiten, sollte für den hamburgischen Gesetzgeber eine rote Linie darstellen.

Insgesamt ergibt sich: Ein Zurückdrängen der aufsichtsbehördlichen Kompetenzen der unabhängigen Kontrollstelle zum Schutz personenbezogener Daten ist weder mit grundgesetzlichen Verfahrensgarantien des Bundesrechts vereinbar, noch mit der Bestimmung nach Art. 60a Abs. 1 und Abs. 2 der Verfassung der Freien und Hansestadt Hamburg (HmbVerf), wonach die Einhaltung der Vorschriften über den Datenschutz von einer unabhängigen Stelle überwacht wird. Diese landesverfassungsrechtliche Garantie gilt auch gegenüber dem Landesamt für Verfassungsschutz.

XIV. Anwendung des allgemeinen Datenschutzrechts, § 23c HmbVerfSchG-E

Regelungszweck der Norm ist ausweislich der Gesetzesbegründung der Ausschluss der Anwendbarkeit der DSGVO sowie des HmbDSG für den Regelungsbereich des HmbVerfSchG-E.

Das HmbDSG und die DSGVO sind gemäß § 2 Abs. 1 u. 6 HmbDSG grundsätzlich auf hamburgische Behörden anwendbar, durch § 23c Satz 1 HmbVerfSchG-E werden sie ausgeschlossen. Die Verweisungsnorm des § 23c Satz 2 HmbVerfSchG soll sodann bestimmte Teile des HmbDSG und des BDSG wieder zur Anwendung bringen. Diese Form der Regelungstechnik ist grundsätzlich nicht zu beanstanden. Die konkrete Ausgestaltung in § 23c Satz 2 HmbVerfSchG ist allerdings in ihrer jetzigen Form unübersichtlich und schwer verständlich formuliert. Dies hat zur Folge, dass die Reglung intransparent wirkt.

Dies liegt insbesondere daran, dass die Platzierung der für § 9 HmbDSG geltenden Einschränkung „außerhalb des Einsatzes nachrichtendienstlicher Mittel“ in § 23c Satz 2 HmbVerfSchG-E der Verständlichkeit des Satzes abträglich ist. Dass die Einschränkung nur für § 9 HmbDSG gelten soll, ist aufgrund der Satzstruktur nicht leicht verständlich. Dies könnte zu Fehlinterpretationen führen und erweckt den Eindruck der Undurchsichtigkeit in Bezug auf das anwendbare Recht. Weiterhin erschließt sich der Regelungszweck des Verweises auf § 19 Abs. 2 Satz 1 HmbDSG nicht. Zum einen enthält § 19 Abs. 2 Satz 1 HmbDSG eine im Vergleich zu § 23b Satz 2 HmbVerfSchG-E nahezu inhaltsgleiche Regelung, wobei § 23b Satz 2 HmbVerfSchG-E die speziellere Norm darstellt und daher § 19 Abs. 2 Satz 1 HmbDSG verdrängen dürfte. Somit ist fraglich, welchen Hintergrund der Verweis auf § 19 Abs. 2 Satz 1 HmbDSG hat. Aus der Gesetzesbegründung ergibt sich dies nicht. Zudem beinhaltet § 19 Abs. 2 Satz 1 HmbDSG einen Verweis auf § 2 Abs. 1 HmbDSG, welcher gerade durch § 23c Satz HmbVerfSchG-E für unanwendbar erklärt wird. Dementsprechend wäre nur eine sinngemäße

Anwendung der Norm in der Weise denkbar, dass der Verweis auf § 2 Abs. 1 HmbDSG durch den Verweis aus § 23b Satz 2 HmbVerfSchG-E ersetzt wird. Eine Klarstellung des Zwecks des Verweises und des Verhältnisses der §§ 19 Abs. 2 S. 1 HmbDSG und 23b HmbVerfSchG-E wäre daher schon aus Gründen der Rechtsklarheit sinnvoll. Gleiches gilt für die Verweisung in § 36 Abs. 1 Satz 1 HmbSÜG-E.

Soweit § 23c des Entwurfs auf § 22 Absatz 2 und § 23 HmbDSG verweist, die besondere Pflichten des bzw. der HmbDSB nach Beendigung des Amtsverhältnisses betreffen, geht dies regelungssystematisch ins Leere: Die Amtsverschwiegenheit gilt bereits nach dieser Bestimmung für alle mit dem Amt verbundenen Tätigkeiten. Sie bezieht sich daher auch auf Informationen, die der HmbBfDI im Zuge seiner Kontrollverantwortung über das Landesamt für Verfassungsschutz erlangt hat. Darüber hinaus bleibt die Verweisung auf die Beschränkung von Tätigkeiten nach Beendigung des Amtsverhältnisses in § 23 Abs. 1 HmbDSG in der Ausrichtung unklar. Das Ergreifen einer beruflichen Betätigung nach der Amtszeit durch die Amtsinhaberin oder den Amtsinhaber unterliegt einer besonderen Prüfung. Diese Vorschrift greift in das Grundrecht der Berufswahlfreiheit nach Art. 12 Abs. 1 GG ein. Sie ordnet für die bzw. für den Amtsinhaber eine Karenzzeit für „alle mit den Aufgaben des früheren Amts nicht zu vereinbarenden Tätigkeiten an“, wie sie entsprechend für Senatsmitglieder nach dem Hamburgischen Senatsgesetz gilt. Die Kontrolle des Hamburgischen Landesamts für Verfassungsschutz findet im Rahmen der allgemeinen Aufgabenwahrnehmung der bzw. des HmbBfDI statt. Sie kann hier keine weitergehende Beschränkungen und Verpflichtungen als die bereits bestehenden begründen.

XIV. Redaktionelle Hinweise

Der korrekte Titel des HmbBfDI lautet gem. sechster Abschnitt §§ 19 ff. HmbDSG „Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit“. Die jeweiligen bestimmten Artikel vor den Aufgabengebieten „~~den~~ Datenschutz“ und „~~die~~ Informationsfreiheit“ sind zu streichen.

Mit freundlichen Grüßen

[redacted]