JOHANNES GUTENBERG-UNIVERSITÄT MAINZ

FACHBEREICH 03

Lehrstuhl für Öffentliches Recht und Informationsrecht, insbesondere Datenschutzrecht

Dr. Sebastian J. Golla

Wissenschaftlicher Mitarbeiter

Johannes Gutenberg-Universität Mainz

Jakob-Welder-Weg 9
55128 Mainz

Tel. +49 6131 39-23045

Bürgerschaft der Freien und Hansestadt Hamburg

Innenausschuss

Postfach 100902

20006 Hamburg

Per E-Mail: Manuela.Knieler@bk.hamburg.de

Drittes Gesetz zur Änderung polizeirechtlicher Vorschriften, Drucksache 21/17906

Anhörung am 19. September 2019

Sehr geehrte Damen und Herren,

haben Sie vielen Dank für die Gelegenheit zu einer Stellungnahme und die Einladung zu der Anhörung. Als Anlage leite ich Ihnen meine Stellungnahme zu.

Mit freundlichen Grüßen

Dr. Sebastian J. Golla

Mainz, den 13. September 2019

Stellungnahme zu dem Entwurf des Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften, Drucksache 21/17906

Dr. Sebastian J. Golla

I. Vorbemerkung und Zusammenfassung

Aufgrund des Umfangs des vorgelegten Gesetzesentwurfes und der knappen Zeit zur Stellungnahme konzentriert sich diese Stellungnahme auf ausgewählte Aspekte. Diese betreffen im Wesentlichen die Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (JIRL) sowie die neue Befugnis zum automatisierten Datenabgleich in § 49 PolDVG-E.

Es ist wie folgt zusammenzufassen:

- Die Befugnisse des Hamburgischen Beauftragten für Datenschutz genügen nicht den Anforderungen des Unionsrechts. Die Datenschutzaufsicht ist auch gegenüber der Polizei mit Einwirkungsbefugnissen auszustatten.
- Die neue Befugnis zur Datenanalyse in § 49 PolDVG-E sollte mit begleitenden Verpflichtungen ausgestattet werden, um die Anwendung potentiell riskanter neuer Formen des Datenabgleichs besser einschätzen und kontrollieren zu können.
- Die in dem Entwurf vorgesehenen Möglichkeiten, polizeiliche Datenverarbeitungen auf Einwilligungen zu stützen, erscheinen zu weitgehend. Jedenfalls sollte die Freiwilligkeit von Einwilligungen durch zusätzliche Anforderungen an die Aufklärung der Betroffenen besser abgesichert werden.
- Kleiner Nachbesserungsbedarf besteht bei den Betroffenenrechten. Die Ausnahme vom Recht auf Löschung bei einem unverhältnismäßigen Aufwand hält den Vorgaben der JIRL nicht Stand.

II. Fehlende Befugnisse der Datenschutzaufsicht

Die Befugnisse des Hamburgischen Beauftragten für Datenschutz in § 72 PolDVG-E sind zu schwach ausgestaltet und erfüllen die Anforderungen des Unionsrechts nicht. Nach Art. 47

Abs. 2 JIRL sieht jeder Mitgliedsstaat durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Abhilfebefugnisse verfügt. Dazu können nicht nur Befugnisse zur (Ver-)Warnung gehören (Art. 47 Abs. 2 lit. a JIRL), sondern auch weitgehende Anweisungsrechte einschließlich des Rechtes, Verarbeitungsvorgänge einzuschränken oder zu verbieten (Art. 47 Abs. 2 lit. b und c JIRL).

Art. 47 JIRL erfordert zwar nicht, die in Abs. 2 der Vorschrift genannten Rechte wortlautgetreu umzusetzen. Um den Aufsichtsbehörden die Möglichkeit zu geben, „wirksam" einzuschreiten, dürfte es aber unerlässlich sein, ihnen das Recht zu geben, konkrete Weisungen bezüglich einzelner Datenverarbeitungsvorgänge zu erteilen. Eine funktionsfähige und mit ausreichenden Befugnissen ausgestattete Datenschutzaufsicht ist essentiell, um die Einhaltung und Durchsetzung des Datenschutzrechts zu gewährleisten. Dies ist auch dem Umstand geschuldet, dass die Betroffenen selbst oftmals nicht über die Mittel verfügen oder ausreichende Anreize haben, um Datenschutzverstöße selbst zu verfolgen.

Für die Notwendigkeit, konkrete Rechte der Aufsichtsbehörden zur Einwirkung auf Datenverarbeitungsvorgänge vorzusehen, spricht auch Art. 46 Abs. 1 lit. a JIRL, wonach jeder Mitgliedstaat vorsieht, „dass jede Aufsichtsbehörde in seinem Hoheitsgebiet die Anwendung der nach dieser Richtlinie erlassenen Vorschriften sowie deren Durchführungsvorschriften überwacht und durchsetzt". Eine Durchsetzung im engeren Sinne ist ohne verbindliche Einwirkungsbefugnisse nicht vorstellbar. Auch die Art. 29-Datenschutzgruppe hat sich auf die Auffassung gestellt, dass wirksame Abhilfebefugnisse im Sinne von Art. 47 Abs. 2 JIRL „verbindliche Befugnisse der Datenschutzaufsichtsbehörden, um bestimmte korrigierende Maßnahmen anzumahnen, zu verhängen oder anzuordnen und verbindliche Entscheidungen gegenüber Verantwortlichen zu erlassen"[1] erfordern.

§ 72 Abs. 1 PolDVG-E beschränkt den Hamburgischen Beauftragten für Datenschutz als Aufsichtsbehörde hingegen darauf, Datenschutzverstöße zu beanstanden und gerichtlich feststellen zu lassen. So werden der Datenschutzaufsicht im polizeilichen Bereich die Zähne

[1] Art.-29-Datenschutzgruppe, Stellungnahme zu einigen grundlegenden Fragestellungen der Richtlinie Justiz/Inneres, EU 2016/680, WP 258, angenommen am 29. November 2017, S.30.

gezogen. Die Beanstandung selbst hat noch keine Sanktionswirkung und führt lediglich dazu, dass der Adressat dazu verpflichtet wird, sich mit ihrem Gegenstand zu befassen. Eine echte Einwirkungsmöglichkeit hat der Datenschutzbeauftragte damit nicht. Es fehlt an wirksamen Abhilfebefugnissen im Sinne von Art. 47 Abs. 2 JIRL und damit an einer ausreichenden Umsetzung der Vorschrift.

Im Übrigen ist die Begründung des Entwurfs für das Fehlen wirksamer Abhilfebefugnisse nicht überzeugend. Dass die Datenverarbeitungsvorgänge bei der Polizei von einer hohen „Sensibilität und Komplexität“[2] sind, gilt auch für die daraus folgenden Risiken für die Datensubjekte. Es bedarf gerade deshalb wirksamer Kontrollmöglichkeiten und einer entsprechenden Ausstattung der Datenschutzaufsicht für diese Arbeiten.

§ 72 PolDVG-E ist um verbindliche Einwirkungsbefugnisse zu ergänzen. Hierfür könnten Art. 58 Abs. 2 lit. a – f DSGVO für entsprechend anwendbar erklärt werden. Ähnlich § 64 Abs. 4 LDSG Schleswig-Holstein könnte § 72 PolDVG-E um einen entsprechenden Absatz ergänzt werden.[3]

> *§ 72 PolDVG-E ist um einen Abs. 4 zu ergänzen, der lautet: „Artikel 58 Absatz 2 Buchstabe a bis f der Verordnung (EU) 2016/679 gilt entsprechend.“*

III. Neue Befugnis zur Datenanalyse

Leichter Nachbesserungsbedarf besteht bezüglich der neuen Befugnis zum Einsatz automatisierter Anwendungen zur Datenanalyse in § 49 PolDVG-E. Diese Befugnis soll komplexe Analysen bei der Polizei vorhandener Daten mit modernen technischen Hilfsmitteln ermöglichen.[4] Sie erinnert bis in die Details ihres Wortlauts stark an § 25a HSOG, mit dem erstmals eine Befugnis für komplexe Datenabgleiche im Polizeirecht der Länder geschaffen wurde. Als erster Ansatz zur Regelung einer sich etablierenden polizeilichen Praxis wurde diese

---

[2] Drs. 21/17906, S. 81.

[3] Vgl. dazu LfDI Hamburg, Schriftliche Anhörung des Innen- und Rechtsausschusses des schleswig-holsteinischen Landtags zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, S. 6 ff.

[4] Vgl. Drs. 21/17906, S. 70 f.

von den Sachverständigen im hessischen Gesetzgebungsverfahren überwiegend positiv aufgenommen.[5]

Der Regelungsansatz erscheint auch hier grundsätzlich sinnvoll, weil er mehr Rechtsklarheit und sauberere Lösungen verspricht als Ansätze, neue komplexe Analyseverfahren auf bestehende Befugnisse zu stützen. Die allgemeinen Befugnisse zum Datenabgleich in den Polizeigesetzen wie auch in der StPO fußen noch auf der Annahme, dass die Auswertung von Daten im Vergleich zu ihrer Erhebung nur einen geringfügigen zusätzlichen Eingriff begründet. Spätestens mit den aktuellen Möglichkeiten zur Verknüpfung und Analyse großer Datenmengen bis hin zum Einsatz von Verfahren maschinellen Lernens ist diese Annahme nicht mehr haltbar. Auch auf die Generalklauseln zur Datenverarbeitung ließen sich entsprechende Analysemethoden kaum stützen.

Zu begrüßen ist, dass § 49 Abs. 1 PolDVG-E eine erhöhte Eingriffsschwelle definiert, um automatisierte Analysen durchzuführen. Optimierungsbedarf besteht bei der prozeduralen Einkleidung und der Sicherung der Grundvoraussetzungen zum Einsatz solcher Verfahren.

Erstens wäre es wünschenswert, den Einsatz der Analyseverfahren ausdrücklich von einem erhöhten Standard der Qualität der einbezogenen Daten abhängig zu machen. Komplexe Verknüpfungen lassen sich nicht herstellen und Analysen sind wenig erfolgversprechend, wenn das zu Grunde liegende Datenmaterial nicht ausreichend verifiziert wird. Deswegen sollten für die in die Auswertung nach § 49 PolDVG-E einbezogenen Daten strenge Maßstäbe der Datenqualität gelten, die im Vergleich zu dem in § 3 Nr. 4 PolDVG-E beschriebenen Grundsatz der Datenqualität genauer zu definieren sind.

[5] *Hornung*, in: Ausschussvorlage des Innenausschusses des Hessischen Landtags 19/63 Teil 3, S. 372 (382 f.); *Löffelmann*, in: Ausschussvorlage des Innenausschusses des Hessischen Landtags 19/63 Teil 1, S. 87 (106 f.); mit Einschränkungen auch LfD Hessen, in: Ausschussvorlage des Innenausschusses des Hessischen Landtags 19/63 Teil 1, S. 127 (138); anders *Federrath*, in: Stenografischer Bericht der 86. Sitzung des Innenausschusses des Hessischen Landtags vom 8. Februar 2018, S. 70 mit Verweis auf die unzureichende Erforschung der automatisierten Datenanalyse.

Zweitens sollte für den Einsatz neuer Plattformen, die komplexe Analysen nach § 49 PolDVG-E ermöglichen, stets eine Datenschutzfolgeabschätzung nach § 57 PolDVG-E erfolgen. Dies könnte klarstellend in § 49 Abs. 3 PolDVG-E verankert werden.

Drittens sollte aufgrund des neuartigen Charakters der Befugnis zumindest vorerst eine jährliche Berichtspflicht über Maßnahmen nach § 49 PolDVG-E gegenüber der Bürgerschaft vorgesehen werden. § 75 PolDVG-E sollte entsprechend ergänzt werden. Die Öffentlichkeit über das Parlament über derartige Maßnahmen und ihr Gesamtaufkommen zu informieren, ist angesichts des enormen gesamtgesellschaftlichen Interesses an dieser technologischen und rechtlichen Entwicklung sinnvoll.

IV. Die Einwilligung als Verarbeitungsgrund

Der Entwurf sieht weitreichende Möglichkeiten vor, personenbezogene Daten zur Erfüllung polizeilicher Zwecke auf Grundlage einer Einwilligung zu verarbeiten (§ 11 Nr. 8 PolDVG-E). Dieses Regelungskonzept begegnet grundsätzlichen Bedenken im Hinblick auf seine Vereinbarkeit mit der JIRL. Vorzugswürdig wäre es, die Einwilligung nicht allgemein als Verarbeitungsgrund zu regeln, sondern nur für spezifische Situationen.

Ob und inwieweit sich die Verarbeitung personenbezogener Daten im Anwendungsbereich der JIRL auf eine Einwilligung stützen lässt, ist nicht abschließend geklärt.[6] Art. 8 JIRL, der die Rahmenbedingungen für die Rechtmäßigkeit der Verarbeitung im Anwendungsbereich der JIRL festlegt, erwähnt die Möglichkeit einer Einwilligung überhaupt nicht. Dass die Einwilligung als Verarbeitungsgrund nicht vollständig ausgeschlossen ist, legt ErwGr 35 JIRL nahe, der von der Möglichkeit einer Einwilligung spricht. Allerdings stellt ErwGr 35 die Situationen, in denen eine Einwilligung nicht erteilt werden kann, in den Vordergrund und erweckt den Eindruck, dass die Einwilligung als Grundlage der Verarbeitung in weiten Bereichen ausgeschlossen ist.[7] Die

[6] Vgl. *Golla/Skobel*, GSZ 2019, 140 ff.; *Kramer*, in: Auernhammer, BDSG, 6. Aufl. 2018, § 51 Rn. 4 („Die Einwilligung in die Datenverarbeitung ist dem Recht der Strafverfolgung und Gefahrenabwehr grundsätzlich wesensfremd."); *Schwichtenberg*, DuD 2016, 605 (606).

[7] *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, Rn. 154.

Einwilligung soll ausdrücklich dann „keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen“, wenn „die zuständigen Behörden natürliche Personen auffordern oder anweisen, ihren Anordnungen nachzukommen“ (ErwGr 35 Satz 3 und 4 JIRL). Bei der Aufforderung, einer rechtlichen Verpflichtung nachzukommen, bestehe keine Wahlfreiheit und daher kein Spielraum für eine freiwillige Einwilligung (ErwGr 35 Satz 5 JIRL). Im Falle einer Duldungs- oder Mitwirkungspflicht bei der Datenverarbeitung ist eine Einwilligung damit kategorisch ausgeschlossen.[8]

Nach ErwGr 35 Satz 6 JIRL sollen die Mitgliedstaaten allerdings nicht daran gehindert sein, „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.“ Dieser Hinweis auf die Zulässigkeit der Möglichkeit einer Einwilligung in spezifischen Fällen deutet darauf hin, dass die Einwilligung im Anwendungsbereich der JIRL nur bezüglich spezifischer Fälle und Maßnahmen als Rechtsgrundlage der Datenverarbeitung geregelt werden kann, nicht aber als übergreifender Erlaubnistatbestand.[9] Dies gilt auch für die polizeiliche Datenverarbeitung.

Im Ergebnis dürfen Polizei und Ordnungsbehörden im Anwendungsbereich der JIRL ihren Befugniskreis nicht beliebig durch Einwilligungen erweitern, wenn die Voraussetzungen einer gesetzlichen Grundlage für die Datenerhebung nicht vorliegen.[10] Dies ist für die Erfüllung der polizeilichen Aufgaben aber in der Regel unschädlich, da vorhandene Generalklauseln Datenverarbeitungen bereits in einem äußerst weiten Umfang gestatten und die Behörden damit regelmäßig auch nicht auf eine Einwilligung angewiesen sein werden. Sollten dennoch Fälle verbleiben, in denen es notwendig und sinnvoll erscheint, dass Polizei und Ordnungsbehörden

---

[8] *Schwichtenberg*, DuD 2016, 605 (606).

[9] Ähnlich *Bäcker*, Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, S. 63 (71); vgl. ebenfalls spezifische Regelungen befürwortend *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, Rn. 157.

[10] Vgl. *Bäcker*, Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, S. 63 (71).

ihre Datenverarbeitung auf eine Einwilligung stützen, sollten diese Fälle ermittelt und spezifisch in den einschlägigen Polizei- und Ordnungsgesetzen geregelt werden.

§ 11 Nr. 8 PolDVG-E sollte daher gestrichen und die Möglichkeit der Verarbeitung personenbezogener Daten auf Grundlage einer Einwilligung auf spezifische Fälle beschränkt werden.

Jedenfalls sollten die Voraussetzungen, die für die Erteilung einer Einwilligung gelten, angepasst werden. Auch bei einer spezifischen Regelung der Situationen, in denen eine Einwilligung als Verarbeitungsgrund zulässig ist, könnte § 5 PolDVG-E weiterhin die allgemeinen Bedingungen der Einwilligung regeln. Hierfür müsste dieser aber zusätzliche Vorkehrungen enthalten, um die Freiwilligkeit der Einwilligung sicherzustellen. Diese ist bei der Erteilung einer Einwilligung gegenüber der Polizei regelmäßig problematisch. Betroffene werden hier oftmals den Eindruck haben, dass sie keine echte freie Entscheidung über die Erteilung einer Einwilligung treffen können. Um dem entgegen zu wirken, sollten Betroffene zumindest stets über die Freiwilligkeit und die Folgen der Verweigerung einer Einwilligung belehrt werden. Dass dies nach § 5 Abs. 1 Satz 4 PolDVG-E bislang nur ausnahmsweise erfolgen soll, ist unzureichend.

§ 5 Abs. 1 Satz 4 PolDVG-E sollte wie folgt gefasst werden: „Die betroffene Person ist über die Freiwilligkeit der Einwilligung sowie die Folgen ihrer Verweigerung zu belehren."

Im Zusammenhang mit § 51 Satz 1 Nr. 1 PolDVG-E ergibt es schließlich wenig Sinn, zur Rechtfertigung einer Datenverarbeitung zum Zwecke der Zuverlässigkeitsüberprüfung auf die „Zustimmung" einer Person abzustellen, die inhaltlich geringeren Anforderungen genügen soll als eine Einwilligung. So soll es nach der Entwurfsbegründung bei der Zustimmung „gerade nicht auf die Beurteilung der Freiwilligkeit im Sinne des § 5 Absatz 1 ankommen"[11]. Diese Abstufung zwischen den Voraussetzungen von Einwilligung und Zustimmung ergibt sich nicht aus den maßgeblichen unionsrechtlichen Vorgaben der JIRL. Zwar spricht Erwägungsgrund 35 Satz 6 JIRL vom Zustimmen in eine Datenverarbeitung, legt dabei aber keine geringeren inhaltlichen Anforderungen als der Begriff der Einwilligung nahe. Aus dem systematischen und

[11] Drs. 21/17906, S. 71.

entstehungsgeschichtlichen Zusammenhang ist der Erwägungsgrund so zu verstehen, dass er Situationen beschreibt, in denen die Möglichkeit einer rechtfertigenden Einwilligung (im Sinne der DSGVO) zwar abgelehnt wird, für Spezialfälle jedoch die Möglichkeit vorgesehen ist, eine Zustimmung als Bestandteil einer Ermächtigungsgrundlage für eine Datenverarbeitung vorzusehen. Anders als die Einwilligung müsste die Zustimmung damit als Merkmal einer Rechtsvorschrift geregelt werden. Nicht gewollt war eine Absenkung der Anforderungen im Vergleich zu einer Einwilligung nach dem Leitbild der DSGVO.[12] Des Weiteren ergibt sich nicht aus der Begründung des Gesetzesentwurfes und ist inhaltlich auch im Übrigen nicht nachvollziehbar, warum im Rahmen der Zuverlässigkeitsüberprüfung eine „pro forma"-Zustimmung, die nicht freiwillig sein muss, als Grundlage der Datenverarbeitung ausreichen sollte. Es erschiene auch ausreichend, die Datenverarbeitung in den relevanten Fällen aus hinreichenden sachlichen Gründen (vgl. § 51 Satz 1 Nr. 2 PolDVG-E) gesetzlich zu gestatten und die Befugnis nicht künstlich auszuweiten.

In § 51 Satz 1 Nr. 1 PolDVG-E sollte der Begriff „Zustimmung" gestrichen und durch den Begriff „Einwilligung" ersetzt werden.

V. Betroffenenrechte

Im Zusammenhang mit den datenschutzrechtlichen Betroffenenrechten besteht kleinerer Nachbesserungsbedarf.

1. Absehen von einer Löschung wegen unverhältnismäßigen Aufwands

Der Entwurf sieht eine zu weite Ausnahme vom Recht auf Löschung vor, die von den Vorgaben der JIRL nicht mehr gedeckt ist. Nach §§ 70 Abs. 2 i.V.m. 59 Abs. 4 Nr. 4 PolDVG-E[13] soll es

---

[12] *Golla/Skobel*, GSZ 2019, 140 (142 f.).

[13] Die Möglichkeiten, die Datenverarbeitung statt einer Löschung nach § 59 Abs. 4 PolDVG-E einzuschränken, sollen ausweislich der Entwurfsbegründung auch im Zusammenhang mit § 70 Abs. 2 PolDVG-E gelten; Drs. 21/17906, S. 79.

zulässig sein, von der Löschung abzusehen, wenn „eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist“.

Dies ist nicht vom Umsetzungsspielraum der JIRL gedeckt. Art. 16 Abs. 3 JIRL beschränkt die Möglichkeit, eine Einschränkung der Verarbeitung statt einer Löschung vorzusehen, im Wesentlichen auf zwei Fälle:

- Die betroffene Person bestreitet die Richtigkeit der personenbezogenen Daten und die Richtigkeit oder Unrichtigkeit kann nicht festgestellt werden (Art. 16 Abs. 3 lit. a).
- Die personenbezogenen Daten müssen für Beweiszwecke weiter aufbewahrt werden (Art. 16 Abs. 3 lit. b).

Den Fall, dass eine Löschung nur mit unverhältnismäßigem Aufwand möglich ist, nennt Art. 16 Abs. 3 JIRL hingegen nicht als mögliche Ausnahme. Die Regelung ist so zu verstehen, dass ein ökonomischer oder administrativer Aufwand nicht vorgebracht werden kann, um das Löschungsrecht einzuschränken.[14]

§ 59 Abs. 4 Nr. 4 PolDVG-E ist daher zu streichen.

2. Endgültiges Absehen von Benachrichtigungen

Eine weitere problematische Regelung enthält § 68 Abs. 3 PolDVG-E. Dieser regelt die Zurückstellung von Benachrichtigungen unter der Voraussetzung der richterlichen Zustimmung. Nach § 68 Abs. 3 Satz 6 PolDVG-E ist fünf Jahre nach Beendigung der Maßnahme mit gerichtlicher Zustimmung ein endgültiges Absehen von der Benachrichtigung möglich, „wenn die Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden, die Voraussetzungen für eine Löschung sowohl bei der Polizei als auch bei den Empfängern von Datenübermittlungen vorliegen und die Daten gelöscht wurden.“ Die Regelung lehnt sich an § 74 Abs. 3 Satz 5 BKAG an und entspricht in ihren

[14] Vgl. *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 1244; *Schwichtenberg*, in: Kühling/Buchner, BDSG, 2. Aufl. 2018, BDSG § 58 Rn. 7.

Vorgaben dem Urteil des BVerfG zum BKAG.[15] Es ist dennoch zweifelhaft, ob das endgültige Absehen von einer Benachrichtigung unter den genannten Voraussetzungen in allen Fällen verhältnismäßig ist.

Historische Erfahrungen zeigen, dass von heimlichen Überwachungsmaßnahmen betroffene Personen auch eine lange Zeit nach Ende der Maßnahme noch ein erhebliches Interesse haben können, von entsprechenden Maßnahmen zu erfahren. Dass die „Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden“, lässt sich nur schwer prognostizieren. Auch wenn es um den Schutz von Beteiligten oder bedeutsamen Rechtsgütern gibt, können Veränderungen der Sachlage (zB das Ableben der zu schützenden Personen) dazu führen, dass die Voraussetzungen für eine Benachrichtigung letztlich eintreten. Es besteht zwar auch ein Interesse daran, Justiz und Behörden bei der Nachprüfung dieser Voraussetzungen zu entlasten. Dem könnte aber auch zB durch längere Prüfintervalle und einer Erhöhung der Höchstfrist zur Zurückstellung der Benachrichtigung Rechnung getragen werden.

[15] BVerfGE 141, 220 (320).