Gesetz zur Neuregelung der polizeilichen Datenverarbeitung im Saarland
Schwerpunkte der Stellungnahme im Rahmen der parlamentarischen Anhörung

Im Rahmen der heutigen Expertenanhörung hat die Landesbeauftragte für Datenschutz zum Entwurf eines Gesetzes zur Neuregelung der polizeilichen Datenverarbeitung im Saarland (SPolDVG-E) Stellung genommen. Im Mittelpunkt der Kritik standen dabei die folgenden Regelungsbereiche des Gesetzentwurfs:

1 Drohende Gefahr

Der Gesetzentwurf erweitert die Eingriffsbefugnisse der Polizei für mittels heimlicher Überwachungsmaßnahmen durchgeführte Vorfeldmaßnahmen, also bevor eine konkrete Gefahr für ein polizeilich geschütztes Rechtsgut erkennbar wird. Während in den neueren Polizeigesetzen anderer Bundesländer hierfür oft der Begriff der drohenden Gefahr verwendet wird, vermeidet der vorliegende Gesetzentwurf diese Begrifflichkeit. Es ist jedoch erkennbar, dass der Gesetzentwurf die Ausführungen des BVerfG im Urteil vom 20. April 2016 - 1 BvR 966/09 (abrufbar unter http://www.bverfg.de/e/rs20160420_1bvr096609.html) – zu den Eingriffsvoraussetzungen bei einer drohenden Gefahr für sich geltend machen will. Da jedoch die diesbezüglichen Vorgaben des BVerfG nur teilweise übernommen werden, führen die Formulierungen im vorliegenden Gesetzentwurf zu erheblichen Auslegungsunsicherheiten, die eine Änderung der Vorschrift dringend erfordern.

Das BVerfG lässt im vorgenannten Urteil (BVerfG, Urteil vom 20. April 2016, - 1 BvR 966/09, Rn. 109 ff.) die Erhebung von Daten durch heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität im Vorfeld konkreter Gefährdungen – das BVerfG spricht in diesem Zusammenhang von einer „*hinreichend konkretisierten Gefahr*" teilweise auch von einer „*drohenden Gefahr*" – nur unter besonderen Voraussetzungen und nur zum Schutz „*besonders gewichtiger Rechtsgüter*" zu. In diesen Konstellationen können die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert werden, allerdings müssen zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen.

Für dieses Konzept einer „*hinreichend konkretisierten Gefahr*" formuliert das Gericht zwei Voraussetzungen, die kumulativ vorliegen müssen: Bestimmte Tatsachen müssen (1.) „*zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen*", (2.) „*zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann*". In

Bezug auf die erste Voraussetzung (also darauf, dass bestimmte Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen) kann nach dem Urteil (nur) *„[i]n Bezug auf terroristische Straftaten"* verzichtet werden – und zwar nur dann, wenn *„das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird"*. (BVerfG, Urteil vom 20. April 2016, - 1 BvR 966/09, Rn. 112)

Diesen Anforderungen wird der vorliegende Gesetzentwurf, insbesondere in § 31 Abs. 1 SPolDVG-E nicht vollumfänglich gerecht. So reduziert der Entwurf die Anforderungen an die Gefahrenprognose in § 31 Abs. 1 Satz 1 SPolDVG-E in verfassungsrechtlich fragwürdiger Weise (a.), die Kriterien für die Bestimmung des Adressatenkreises bei Maßnahmen nach § 31 Abs. 1 SPolG bleiben unklar (b.) und schließlich dient die Eingriffsbefugnis des § 31 Abs. 1 Satz 1 SPolDVG-E nicht ausschließlich dem Schutz *„besonders gewichtiger Rechtsgüter"* (c.).

a.) Verfassungsrechtliche Bedenken bestehen zunächst – und nicht begrenzt auf die Vorschriften des § 31 SPolDVG-E – mit Blick auf die verwendeten Begrifflichkeiten. Wie oben ausgeführt, verlangt das BVerfG in den Konstellationen einer hinreichend konkretisierten Gefahr als erste Voraussetzung, dass bestimmte Tatsachen *„den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen"*. § 31 Abs. 1 Satz 1 SPolDVG-E scheint diese Formulierung auf den ersten Blick zu übernehmen, modifiziert sie dann aber in einem entscheidenden Tatbestandsmerkmal: Anstatt dass *„bestimmte Tatsachen den **Schluss** auf ein (...) [bestimmtes] Geschehen zulassen müssen"*, lässt der Gesetzentwurf bereits die **Annahme** für ein solches Geschehen ausreichen. Hierbei handelt es sich nicht lediglich um eine sprachliche Alternative oder gar um eine synonyme Formulierung zu der vom BVerfG verwendeten Begrifflichkeit, sondern um eine andere Qualität der Prognose. Denn während es sich bei einer Annahme letztlich um eine Spekulation handelt, verlangt das BVerfG, dass bestimmte Tatsachen den Schluss, also die Konklusion, die logisch zwingende Folge auf ein bestimmtes hinreichend konkretisiertes Geschehen zulassen. Der Besuch eines von der Polizei als linksextrem eingeschätzten Studentenkreises begründet vielleicht die Annahme, dass diese Person sich an linksextremistischen Straftaten beteiligen möchte, zwingend ist dieser Schluss aber nicht.

   Entsprechend hat das BVerfG die im damaligen § 20l Abs. 1 Satz 1 Nr. 2 BKAG a.F. enthaltene Befugnis zur Telekommunikationsüberwachung von *„Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass die terroristische Straftaten vorbereiten"* als konturenarm und damit als zu unbestimmt und unverhältnismäßig beurteilt:

   > *„Mit der Verfassung nicht zu vereinbaren ist demgegenüber die nicht näher eingeschränkte Erstreckung der Telekommunikationsüberwachung nach § 20l Abs. 1 Nr. 2 BKAG auf Personen, bei denen bestimmte Tatsachen die **Annahme** rechtfertigen, dass sie terroristische Straftaten vorbereiten. Die Vorschrift, die über die Abwehr einer konkreten*

Gefahr hinaus die Eingriffsmöglichkeiten mit dem Ziel der Straftatenverhütung vorverlagert, verstößt in ihrer konturenarmen offenen Fassung gegen den Bestimmtheitsgrundsatz und ist unverhältnismäßig weit." (BVerfG, Urteil vom 20. April 2016, - 1 BvR 966/09, Rn. 232)

b.) Auslegungsschwierigkeiten und -unklarheiten bestehen auch im Hinblick auf die Bestimmung des Kreises von Personen, die von Maßnahmen nach § 31 Abs. 1 SPolDVG-E betroffen sein können. Das BVerfG erlaubt – wie oben ausgeführt – Maßnahmen im Kontext einer hinreichend konkretisierten Gefahr nur gegen solche Personen, bei denen bestimmte Tatsachen den Schluss zulassen, dass diese Personen beteiligt sind, um sicherzustellen, dass entsprechende Überwachungsmaßnahmen auf bestimmte Person beschränkt werden.

Im Hinblick auf den Adressatenkreis verweisen die § 31 Abs. 1 Satz 1 und Satz 2 SPolDVG-E auf den Personenkreis nach § 17 Abs. 2 Nr. 1 und 2 SPolDVG-E. Dabei bleibt unklar, ob die Vorschrift des § 17 Abs. 2 Nr. 1 und 2 SPolDVG-E eine einfachgesetzliche Ausgestaltung der vom BVerfG formulierten Anforderungen darstellt, oder ob hier andere, geringere Anforderungen normiert werden. Für letztes spricht insbesondere, dass das BVerfG verlangt, dass tatsächliche Anhaltspunkte für eine Beteiligung der betroffenen Person vorliegen, während der Gesetzentwurf es bereits ausreichen lässt, dass die überwachten Personen Kenntnis von der Planung oder Vorbereitung haben oder aus der Verwertung der Tat Vorteile ziehen können. Es ist zweifelhaft, ob dies für eine Beteiligung, wie sie das BVerfG voraussetzt, ausreicht.

c.) Problematisch ist schließlich, dass die Eingriffsbefugnis des § 31 Abs. 1 Satz 1 SPolDVG-E nicht auf den Schutz „*besonders gewichtiger Rechtsgüter*" begrenzt ist. Zu diesen besonders gewichtigen Rechtsgütern gehören „*Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes*", aber auch eine „*gemeine Gefahr" oder eine „Gefahr für Güter der Allgemeinheit, die die Existenz der Menschen berühren*" (BVerfG, Urteil vom 20. April 2016, - 1 BvR 966/09, Rn. 108).

Dem wird die Vorschrift des § 31 Abs. 1 Satz 1 SPolDVG-E nicht gerecht, wenn sie die verdeckte Erhebung personenbezogener Daten bereits zur vorbeugenden Bekämpfung von Verbrechen oder anderen gewerbsmäßig, gewohnheitsmäßig oder bandenmäßig begangenen Straftaten gestattet. So ist bei § 31 Abs. 1 Satz 1 Nr. 2 SPolDVG-E Anknüpfungspunkt für eine polizeiliche Maßnahme schon nicht ein bestimmtes zu schützendes Rechtsgut, sondern die Art und Weise der Tatausführung und der Tatmodalitäten, ob also die Tat gewerbsmäßig, gewohnheitsmäßig oder bandenmäßig begangen wird. Bei § 31 Abs. 1 Satz 1 Nr. 1 SPolDVG-E knüpft die polizeiliche Befugnis ganz allgemein an die vorbeugende Bekämpfung von Verbrechen, und damit an alle Straftaten, die im Mindestmaß mit einem Jahr Freiheitsstrafe bedroht sind (§ 12 StGB), an. Damit ist die Vorschrift nicht auf den Schutz von „*besonders gewichtigen Rechtsgütern*" beschränkt, sondern kann bspw. auch in Fällen der vorbeugenden

Bekämpfung von Gefahren für Sach- und Vermögenswerte herangezogen werden. Der Schutz von Sach- und Vermögenswerten stellt hingegen nach Auffassung des BVerfG auch bei bedeutsamen Sachwerten kein hinreichend gewichtiges Rechtsgut für die Durchführung der genannten Überwachungsmaßnahmen im Vorfeld einer konkreten Gefahr, sprich bei einer drohenden Gefahr, dar.

> *„Einen uneingeschränkten Sachwertschutz hat das Bundesverfassungsgericht demgegenüber nicht als ausreichend gewichtig für solche Maßnahmen angesehen." (BVerfG, Urteil vom 20. April 2016, - 1 BvR 966/09, Rn. 108).*

Da die Vorschrift mithin den Umfang der geschützten Rechtsgüter sehr weit zieht, spricht dies dafür, dass die vom BVerfG aufgestellten engen verfassungsrechtlichen Vorgaben für das Vorliegen einer drohenden Gefahr nicht eingehalten sind, was für eine Verfassungswidrigkeit der Norm spricht.

Letztlich zeigen die obigen Ausführungen, dass jedenfalls mit Blick auf die Eingriffsbefugnisse in § 31 Abs. 1 SPolDVG-E, den Verweis auf § 17 Abs. 2 Nr. 1 und Nr. 2 SPolDVG-E und die in beiden Vorschriften verwendeten Begrifflichkeiten noch ein erheblicher Klärungs- und Präzisierungsbedarf besteht. Die Auflösung dieser Unklarheiten sollte vor dem Hintergrund der Konsequenzen, die solche Eingriffsbefugnisse auf die Grundrechte der Bürgerinnen und Bürger haben, nicht erst den Verwaltungsgerichten überlassen werden, sondern im Gesetzgebungsverfahren konkretisiert werden.

2 Benachrichtigungspflichten

Für problematisch halten wir die in § 10 Abs. 5 und 6 SPolDVG-E geregelte Benachrichtigungspflicht, weil sie insbesondere die Entscheidung darüber, welche Personen letztlich über durchgeführte verdeckte Eingriffsmaßnahmen unterrichtet werden, weitgehend in das Belieben der Polizei stellt. Zwar verweist die Gesetzbegründung darauf, dass sich die Absätze 5 und 6 an den einschlägigen Bestimmungen des § 101 Abs. 5, 6 StPO und § 74 BKAG orientieren. Ein Blick in die erwähnten Vorschriften zeigt jedoch, dass der Regelungsumfang im vorliegenden Gesetzentwurf weit hinter den zitierten Vorschriften der StPO und des BKAG zurückbleibt.

Dies gilt insbesondere für den Kreis der Benachrichtigungsempfänger. § 10 Abs. 5 Satz 1 SPolDVG-E sieht eine Regelbenachrichtigung zunächst nur für die Zielpersonen vor, also die Personen, gegen die sich eine verdeckte Maßnahme konkret richtet. Ob und inwieweit andere Personen zu benachrichtigen sind, lässt der Gesetzentwurf im Wesentlichen offen bzw. stellt diese Entscheidung ins Belieben der Polizei. Die Regelung verwendet in § 10 Abs. 5 Satz 4 SPolDVG-E lediglich den Begriff der „sonstigen betroffenen Person" ohne näher zu beschreiben, welcher Personenkreis hiermit konkret gemeint sein soll. Zusätzlich wird die Benachrichtigungspflicht noch dadurch beschränkt, dass diese betroffenen Personen ein besonders schutzwürdiges Interesse an einer Benachrichtigung haben müssen.

Die im Gesetzentwurf zitierten Vorschriften der StPO und des BKAG, an denen sich die Regelung des § 10 Abs. 5 SPolDVG-E orientiert, definieren hingegen (anders als die vorliegende Norm) für jede verdeckte Ermittlungsmaßnahme verbindlich den Kreis der Benachrichtigungsempfänger. Exemplarisch soll dies am Beispiel einer Wohnraumüberwachung nach § 34 SPolDVG-E und dem Einsatz eines verdeckten Ermittlers in einer Wohnung nach § 31 Abs. 2 Nr. 4 SPolDVG-E gezeigt werden. Hier bleibt nach dem saarländischen Regelungsentwurf zweifelhaft, wer bei einer Wohnraumüberwachung, die sich nicht gegen den Wohnungsinhaber (bspw. der Mieter) selbst als Zielperson gerichtet hat und der auch zum Zeitpunkt der Maßnahme nicht in seiner Wohnung war, über diese Maßnahme zu unterrichten ist. Die Regelungen in der StPO und im BKAG sind hier eindeutig und verlangen, dass auch die Personen, deren nicht allgemein zugängliche Wohnung die beauftragte Person, die Vertrauensperson oder der Verdeckte Ermittler betreten hat, bzw. Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten zu benachrichtigen sind (§ 101 Abs. 4 Nr. 5 lit. c und Nr. 9 lit. c StPO bzw. § 74 Abs. 1 Nr. 2 lit. c und Nr. 3 lit. c BKAG).

Entsprechend der vorgenannten Vorschriften halten wir es auch hier für erforderlich, dass im Gesetzestext der Kreis der Benachrichtigungsempfänger für jede verdeckte Ermittlungsmaßnahme verbindlich vorgegeben wird.

3 Aussonderungsprüfristen und Mitziehregel

Erhebliche europarechtliche Bedenken bestehen gegen die in § 26 Abs. 2 Satz 4 SPolDVG-E vorgesehene Mitziehregel. Diese verstößt gegen Art. 5 und Art. 7 Abs. 2 der JI-Richtlinie. Danach hat der Mitgliedstaat angemessene Fristen vorzusehen, nach deren Ablauf eine Überprüfung der Notwendigkeit der weiteren Speicherung personenbezogener Daten vorzunehmen ist. Gemäß Art. 7 Abs. 2 der JI-Richtlinie muss der Gesetzgeber zudem alle angemessenen Maßnahmen vorsehen, damit personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden.

Zwar sieht der Entwurf in § 26 Abs. 2 Satz 2 SPolDVG-E zunächst entsprechende Aussonderungsprüffristen weiterhin vor. Aussonderungsprüffristen sind keine Löschfristen, sondern Zeiträume, nach deren Ablauf geprüft werden muss, ob die jeweiligen gespeicherten Daten noch zulässig gespeichert und weiterhin erforderlich sind.

Die Regelung des § 26 Abs. 2 Satz 4 SPolDVG-E, die auch in der Gesetzesbegründung als sog. Mitziehregel bezeichnet wird, hebelt diesen Prüfmechanismus jedoch aus. Die Neueinfügung der Mitziehregel in § 26 Abs. 2 Satz 4 SPolDVG-E, die bei jedem neuen Speicheranlass für die Daten der betroffenen Person insgesamt einen Neubeginn der Aussonderungsprüffrist anordnet, hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Im Wortsinn werden die alten Datensätze mit dem neu eingefügten Datensatz „mitgezogen" Dies kann im Einzelfall dazu führen, dass es bei Personen, die beispielsweise bereits im jugendlichen Alter von 15 Jahren einmalig straffällig werden (z.B. wegen Cannabiskonsums) und die danach nur einmal im Jahrzehnt auffällig werden, sei es durch einen Geschwindigkeitsverstoß oder eine andere

Bagatelle, bis zu deren Tod nicht ein einziges Mal zu einer einzelfallbezogenen Überprüfung kommt und der Datensatz über das jugendliche Bagatelldelikt zeitlebens mitgeführt wird.

Hierbei ist auch zu berücksichtigen, dass es sich bei polizeilichen Informationssystemen um Verdachtsdateien handelt. Die Behörden speichern in polizeilichen Informationssystemen Daten auch über solche Personen, die bislang nur unter einem Verdacht standen, aber nicht verurteilt wurden. Die Vorschrift betrifft deshalb auch einen Anteil von Personen, die tatsächlich keine Straftaten begangen haben.

Diese Daten sind Grundlage und „Anknüpfungspunkt" neuer Ermittlungen. Wer „polizeibekannt" ist, muss eher damit rechnen, Gegenstand polizeilicher Ermittlungen zu werden. Dies stellt für die betroffene Person eine potentiell erhebliche Belastung dar.

Bislang mildern diese Belastung an der jeweils vorgeworfenen Tat orientierte Aussonderungsprüffristen ab. Ereignisse, die längere Zeit – also in der Regel mehr als 10 Jahre zurückliegen – werden im Regelfall gelöscht. Damit werden den Betroffenen nach der bisherigen Regelung ältere Verdachtsmomente nicht mehr entgegengehalten.

Das wird sich künftig ändern. Eine Überprüfung und Aussonderung nach „angemessenen Fristen" (Art. 5 JI-Richtlinie) findet nach der Neuregelung überhaupt nicht statt, wenn ein Betroffener innerhalb der Aussonderungsprüffrist nochmal auffällig wird. Dabei hat die Polizei schon nach geltendem Recht die Möglichkeit, die personenbezogenen Daten länger aufzubewahren, sofern ein sachlicher Grund die längere Speicherung rechtfertigt. Auch § 26 Abs. 2 Nr. 2 SPolDVG-E sieht diese Möglichkeit weiterhin vor. Die in § 26 Abs. 2 Satz 4 SPolDVG-E vorgesehene Regelung ändert dies nur für die Fälle, in denen ein solcher sachlicher Grund gerade nicht vorliegt. Das ist unverhältnismäßig und verstößt gegen Art. 5 JI-Richtlinie und gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

4 Zweckbindungsgebot

Eng mit den Aussonderungsprüffristen zusammen hängen die Grundsätze zur Gewährleistung der Zweckbindung. Solange personenbezogene Daten gespeichert sind, solange stellt sich die Frage, für welche Zwecke diese Daten verwendet werden dürfen. Denn einmal erfasste Daten über den Betroffenen eröffnen die Möglichkeit, diese Daten in verschiedenen Zusammenhängen erneut zu verwenden. Um diesen Risiken für den Betroffenen zu begegnen, gilt als ein wesentlicher datenschutzrechtlicher Grundsatz das Zweckbindungsgebot. Danach dürfen einmal erhobene Daten grundsätzlich nur für diejenigen konkreten Zwecke gespeichert, verarbeitet oder genutzt werden, für die sie erhoben worden sind. Sollen sie für andere Zwecke verarbeitet werden, bedarf es hierfür einer rechtlichen Grundlage (Zweckänderungsbefugnis).

Die Polizeigesetze der Länder sehen für die polizeiliche Arbeit übereinstimmend drei grundlegende Zweckbestimmungen vor (siehe Abbildung 1).

1. Aufgabenerfüllung einschl. Vorgangsbearbeitung
2. Vorgangsverwaltung und Dokumentation
3. Gefahrenvorsorge bzw. Strafverfolgungsvorsorge

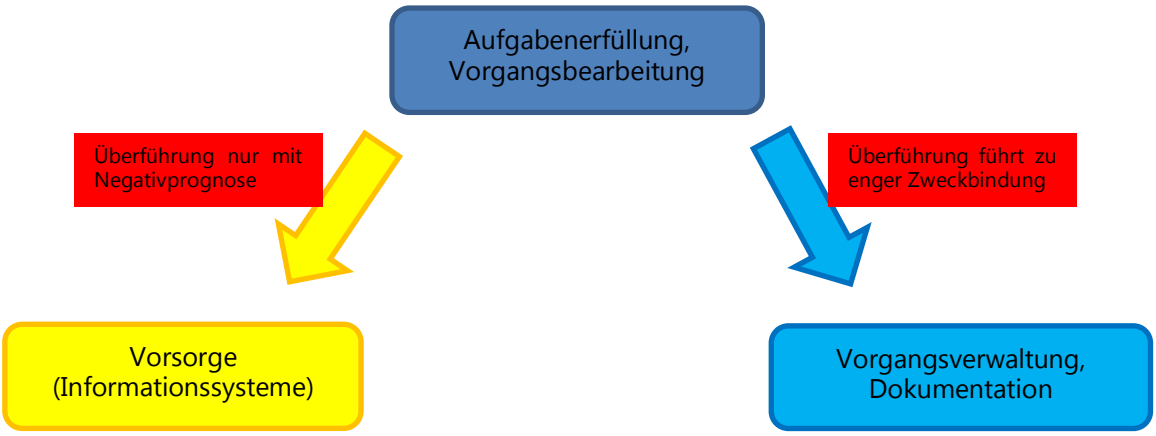

Abbildung 1

Der Zweck der Aufgabenerfüllung erfasst zunächst die Datenverarbeitung, die für die Bearbeitung eines konkreten Ermittlungs- oder Gefahrenabwehrverfahrens erforderlich ist. Die Vorgangsverwaltung und Dokumentation dienen dazu, ein sicheres und rasches Auffinden von Vorgängen (nicht Informationen) sowie eine (bspw. juristische oder parlamentarische) Kontrolle ihrer Bearbeitung zu ermöglichen. Der Zweck der Vorsorge zielt schließlich darauf ab, für die Verfolgung von künftigen Straftaten oder zur Abwehr künftiger Gefahren eine Informationsvorsorge zu treffen. Diese unterschiedlichen Verarbeitungszwecke sind durch technische und organisatorische Maßnahmen strikt voneinander abzugrenzen und trennen.

Da die Zweckbindung im Rahmen der Aufgabenerfüllung einzelfallbezogen ist, sich also auf ein bestimmtes, konkretes Verfahren bezieht, bedarf sowohl die Nutzung personenbezogener Daten in einem anderen Verfahren einer Rechtfertigung ebenso wie die Überführung personenbezogener Daten in eine Vorsorgedatei oder eine Verarbeitung zur Dokumentationszwecken. § 23 Abs. 1 – 3 SPolDVG-E normieren insofern in Anlehnung an die Ausführungen des Bundesverfassungsgerichts zum damaligen Bundeskriminalamtgesetz (BKAG) nunmehr die Voraussetzungen der sog. hypothetischen Datenneuerhebung unter denen personenbezogene Daten aus einem Verfahren in einem anderen Verfahren genutzt werden können.

Im Hinblick auf die Anforderungen zur Überführung personenbezogener Daten in Vorsorgedateien oder Vorgangsverwaltungssysteme hingegen können die Grundsätze der hypothetischen Datenneuerhebung nicht fruchtbar gemacht werden. Das Urteil des Bundesverfassungsgerichts zum BKAG hat an diesen Anforderungen an die Zweckbindung nichts geändert.

Vor diesem Hintergrund sehen wir die im Vergleich zum bisherigen § 30 Abs. 2 SPolG erfolgende Neuregelung in § 23 Abs. 4 SPolDVG-E, mit der die bisher bestehende Pflicht zur Durchführung einer Negativprognose entfallen soll, und insbesondere die Gesetzesbegründung hierzu kritisch. Die Gesetzesbegründung geht offenbar davon aus, dass durch die Regelung des § 23 Abs. 4 SPolDVG-E eine Überführung personenbezogener Daten in Vorsorgedateien auch ohne Negativprognose zulässig sei. Dem muss nachdrücklich widersprochen werden. Wie oben ausgeführt dienen die Vorsorgedateien allein dem Zweck für zukünftige Verfahren eine Informationsvorsorge zu betreiben. Dies setzt die positive Feststellung voraus, dass im Einzelfall eine gewisse Wahrscheinlichkeit dafür besteht, dass der Betroffene eines strafrechtlichen Ermittlungsverfahrens auch zukünftig Straftaten begehen wird. Eine solche Prognose kann sich insbesondere aus der Art, Ausführung oder Schwere der Tat oder der Persönlichkeit der betroffenen Person ergeben (Negativprognose).

Die Pflicht zur Durchführung einer solchen Negativprognose folgt bereits aus dem Erforderlichkeitsgrundsatz und der Unschuldsvermutung. Ein Kernanliegen des Datenschutzes ist es, die Unschuldsvermutung auch in polizeilichen Dateien zur Geltung zu bringen. Entsprechend ergibt sich auch in den Bundesländern, in denen eine Negativprognose nicht ausdrücklich normiert ist (die Gesetzesbegründung erwähnt unter anderem Rheinland-Pfalz), eine entsprechende Feststellungspflicht implizit aus dem dort normierten Tatbestandsmerkmal der Erforderlichkeit, mit der Folge, dass in diesen Bundesländern bei der Beurteilung der Erforderlichkeit der Speicherung eine Prognoseentscheidung im Hinblick auf eine Wiederholungsgefahr getroffen werden muss (vgl. Baunack, in: De Clerck/Schmidt, Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz, 28. Erg. Oktober 2018, § 33 S. 10).

Bei der Überführung personenbezogener Daten in Vorsorgedateien sind auch die Folgen für die Betroffenen zu berücksichtigen. Eine Überführung personenbezogener Daten in Vorsorgedateien führt in der Regel dazu, dass die Daten dieser Personen in bund- und länderübergreifenden Systemen auch den Polizeien der anderen Bundesländer und dem BKA zur Verfügung gestellt werden. Auch § 44 Satz 3 Nr. 2 SPolDVG-E sieht eine solche Übermittlungsbefugnis ausdrücklich vor. Das Erfordernis einer Negativprognose gewährleistet dabei, dass eine Bereitstellung personenbezogener Daten nur auf Grund einer hinreichenden Tatsachen- und Ermittlungsgrundlage erfolgt, was im Regelfall erst gegen Ende des Ermittlungs- oder des Strafverfahrens der Fall ist. Dies führt auch die Gesetzesbegründung richtig aus, wenn dort formuliert ist, dass „*häufig erst zu einem späteren Zeitpunkt ausreichende Erkenntnisse vorliegen, die eine substantiierte Prognose einer Legalbewährung ermöglichen*".

Ziel und Konsequenz der gesetzlichen Neuregelung in § 23 Abs. 4 SPolDVG-E und der Begründung hierzu ist es damit, personenbezogene Daten von Verdächtigen bereits zu einem Zeitpunkt bund- und länderübergreifend bereitzustellen, zu dem eine Teilnahme oder Täterschaft noch überhaupt nicht plausibel ist. Wie bereits ausgeführt, handelt es sich bei polizeilichen Dateien um Verdachtsspeicherungen. Die Vorschrift hat zur Folge, dass bei jeder Anzeige, sei sie berechtigt oder unberechtigt, und ohne weitere Ermittlungen der Polizei der jeweilige Betroffene in den bundesweiten Informationssystemen als Täter- oder Teilnehmer einer Straftat geführt

werden wird. Das kehrt die Unschuldsvermutung gegen die sonst geltenden Prinzipien um und widerspricht der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und des Bundesverfassungsgerichts.

§ 23 Abs. 4 SPolDVG-E widerspricht schließlich auch den Vorgaben der JI-Richtlinie. Artikel 6 Buchst. a der JI-Richtlinie fordert eine Differenzierung bei den Voraussetzungen der Speicherungen bzw. den Rechtsfolgen zwischen Verdächtigen, Verurteilten, Opfern und anderen Parteien. Demgegenüber behandelt der Gesetzentwurf im Hinblick auf die Speicherung personenbezogener Daten in Vorsorgedateien solche Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben wie bereits verurteilte Straftäter.

5 Zugriff auf informationstechnische Systeme

§ 35 Abs. 2 SPolDVG-E erlaubt zur Ermöglichung der Aufzeichnung von zu überwachender Telekommunikation, bevor diese verschlüsselt wird, den Zugriff auf informationstechnische Systeme einer verdächtigen Person (sog. Quellen-TKÜ). Diese Zugriffe auf informationstechnische Systeme der Betroffenen stellen einen Eingriff in das aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitete Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar. Der Zugriff erfolgt dabei regelmäßig über die Ausnutzung von Sicherheitslücken in der vom Verdächtigen verwendeten Hard- und Software.

Diese Möglichkeit zur Nutzung von Sicherheitslücken führt jedoch zu Fehlanreizen bei den Sicherheitsbehörden dahingehend, dass diese dazu verleitet werden, ihnen bekannte Sicherheitslücken nicht dem Hersteller zu melden, sondern für einen möglichen zukünftigen Bedarf zu „horten". Dies führt zu einer Schwächung des IT-Sicherheitsniveaus insgesamt (in der Wirtschaft, in der Verwaltung und bei Privaten), da dem Hersteller nicht gemeldete Sicherheitslücken auch von Kriminellen genutzt werden können. Aus dem Grundrecht auf Gewährleistung Vertraulichkeit und Integrität informationstechnischer Systeme folgt aber eine staatliche Schutzpflicht, diesen Fehlanreizen entgegenzuwirken. Dies kann nur dadurch erreicht werden, dass der Zugriff auf informationstechnische Systeme nur mittels solcher Sicherheitslücken erfolgen darf, die dem Hersteller der Hard- bzw. Software bereits bekannt sind.

6 Abgleich personenbezogener Daten

Für problematisch erachten wir auch die Befugnis zum Abgleich personenbezogener Daten in § 28 Abs. 1 SPolDVG-E mit allen Dateisystemen, die die Polizei selbst führt oder für die sie eine Berechtigung zum Abruf hat. Diese umfassende Befugnis lässt die Vorgaben des BVerfG im Urteil zum BKA-Gesetz (BVerfG, Urteil vom 20. April 2016, - 1 BvR 966/09) zur Zweckbindung gänzlich unberücksichtigt. In der grundsätzlichen Möglichkeit zum Datenabgleich realisiert sich gerade das Risiko, vor dem das Recht auf informationelle Selbstbestimmung schützen will: Die Verknüpfung unterschiedlicher Datenbestände sowie die Erweiterung des Kreises der Kenntnishabenden und dadurch die Gefahr für den Betroffenen, Ziel von Vorverurteilungen, Stigmatisierungen und polizeilichen Folgemaßnahmen zu werden. Entsprechend sieht das Gericht in einem solchen Abgleich einen

eigenständigen Grundrechtseingriff, der im Sinne des Verhältnismäßigkeitsgrundsatzes geeignet und erforderlich sein muss. Vor diesem Hintergrund muss bei einer polizeilichen Inanspruchnahme auch der Abgleich personenbezogener Daten von diesem Zweck her seine Begrenzung finden. Dies zugrunde gelegt bedarf die Vorschrift des § 28 Abs.1 SPolDVG-E aus verfassungsrechtlicher Sicht daher einer Präzisierung in Form der Festlegung von Zweckvorgaben und Eingriffsschwellen.

Insbesondere bedarf es einer Orientierung am Erforderlichkeitsgrundsatz, um eine auf den Einzelfall bezogene verfassungskonforme Normanwendung gewährleisten zu können. So ist es bspw. unverhältnismäßig, im Rahmen einer allgemeinen Verkehrskontrolle den kontrollierenden Beamten die Art, Zahl und den Umfang bisher gegen den Fahrer geführter Ermittlungsverfahren zu offenbaren (§ 28 Abs. 1 Satz 1 SPolDVG-E). Ebenso unverhältnismäßig ist es etwa, jeden Anzeigeerstatter oder Hinweisgeber einem Abgleich mit den Fahndungsbeständen zu unterziehen (§ 28 Abs. 1 Satz 3 SPolDVG-E). Die beiden vorgenannten Beispielfälle wären derzeit unzweifelhaft von der Formulierung des § 28 Abs. 1 SPolDVG-E gedeckt. Eine verfassungskonforme Ausgestaltung, die auch der Vielzahl der unterschiedlichen denkbaren Situationen gerecht wird, kann hier am besten mit der Normierung eines Erforderlichkeitsmaßstabs begegnet werden.

7 Zuverlässigkeitsüberprüfungen

Im Kontext des vorgenannten Abgleichs personenbezogener Daten wird auch eine Möglichkeit zur Durchführung von sog. Zuverlässigkeitsüberprüfungen neu ins Gesetz aufgenommen. Mit der Überprüfung der Zuverlässigkeit von Personen durch einen Abgleich mit polizeilichen Dateien soll festgestellt werden, ob sicherheitsrelevante Erkenntnisse gegen diese Personen vorliegen.

Solche Überprüfungen sind datenschutzrechtlich problematisch, da sie tief in das Grundrecht auf informationelle Selbstbestimmung des Betroffenen eingreifen, ohne dass, wie sonst im Polizeirecht üblich, diese Person einen konkreten Anlass hierfür bietet oder eine konkrete Gefahr existiert. Sie berühren zudem auch eine Vielzahl von anderen Grundrechten. Strebt der Betroffene etwa eine Tätigkeit in einer Behörde mit Vollzugsaufgaben an (§ 28 Abs. 3 Nr. 1lit. a SPolDVG-E) und wird er bei Verweigerung der Einwilligung vom weiteren Bewerbungsverfahren ausgeschlossen werden, so ist dies am Maßstab des Art. 33 Abs. 2 GG zu messen. Im Falle eines privilegierten Zugangs eines Pressevertreters zu der Veranstaltung einer Behörde ist die Durchführung der Zuverlässigkeitsüberprüfung am Maßstab der Pressefreiheit nach Art. 5 Abs. 2 Satz 2 GG zu bewerten. Zudem spielt auch die Berufsausübungsfreiheit eine Rolle, wenn einem Dienstleister (bspw. Reinigungsunternehmen) die Tätigkeit innerhalb einer Behörde mit Vollzugsaufgaben versagt wird, weil ein Mitarbeiter des Reinigungsunternehmens die Einwilligung verweigert. Letztlich sind auch die Rechte des Verteidigers zu berücksichtigen, der seinen Mandaten in der JVA besuchen möchte und sich hierfür nach § 28 Abs. 3 Nr. 5 SPolDVG-E einer Zuverlässigkeitsüberprüfung unterziehen muss.

All diese Einschränkungen können vor dem Hintergrund der sie berührenden Grundrechte hier nur deshalb verfassungskonform sein, weil sie von einer Einwilligung der betroffenen Personen in die Durchführung der Überprüfung abhängig sind. Wirksam kann eine solche Einwilligung indes nur dann sein, wenn sie freiwillig erfolgt. Freiwilligkeit liegt nur aber vor, wenn der Betroffene bei einer Verweigerung der Einwilligung nicht mit Nachteilen rechnen muss. Eine solche Freiwilligkeit wäre daher nicht gegeben, wenn dem Betroffenen bspw. bei Verweigerung der Einwilligung der privilegierte Zugang verwehrt würde. Wir halten es deshalb für wichtig in der Gesetzesbegründung nochmal zu verdeutlichen, dass die Verweigerung der Einwilligung ohne negative Folgen für den Betroffenen bleiben muss. Will man dies anders regeln, will man also dem Betroffenen bei einer Verweigerung der Einwilligung die gewünschte Privilegierung versagen, so sollte anstatt des datenschutzrechtlich konnotierten Begriffs der Einwilligung, der Begriff der Zustimmung verwendet werden.

Was die Vorschrift im Übrigen anbelangt, schlagen wir vor, das Verhältnis der Zuverlässigkeitsüberprüfung zu anderen Sicherheitsüberprüfungen, insbesondere solchen nach dem Saarländischen Sicherheitsüberprüfungsgesetz klarzustellen. Insbesondere wenn es um die Tätigkeit in einer Behörde mit Vollzugsaufgabe geht, sieht schon heute das Sicherheitsüberprüfungsgesetz eine Sicherheitsüberprüfung mit klaren rechtlichen Vorgaben vor, sodass eine zusätzliche Zuverlässigkeitsüberprüfung durch die Polizei hier nicht notwendig ist. Zudem regen wir an, die Durchführung einer Zuverlässigkeitsüberprüfung bei einer beratenden oder unterstützenden Tätigkeit für eine Behörde darauf einzuschränken, dass dies im begründeten Einzelfall erforderlich ist. Andernfalls ist die Vorschrift viel zu weit und erfasst alle externen Personen, die in irgendeiner Weise für eine saarländische Kommunal- oder Landesbehörde tätig werden.

Für rechtsstaatlich äußerst problematisch halten wir zudem, dass das Verfahren zur Durchführung der Zuverlässigkeitsüberprüfung derzeit keine Anhörung des Betroffenen vorsieht. Zwar erteilt der Betroffene zunächst seine „Einwilligung“. Das Ergebnis der Zuverlässigkeitsüberprüfung kann der Betroffene aber nicht vorhersehen. Dies insbesondere deshalb, weil der Betroffene bspw. wegen möglicher verdeckter Maßnahmen gegen ihn oder wegen Unkenntnis über die Löschung seiner Daten bzw. ganz allgemein, weil er Art, Umfang und Qualität, sprich Aktualität und Richtigkeit der bei der Polizei gespeicherten personenbezogenen Daten, die Eingang in die Bewertung finden, nicht abschätzen und voraussehen kann.

Im Falle eines negativen Ausgangs der Zuverlässigkeitsüberprüfung, wenn also Sicherheitsbedenken bestehen, wird der Betroffene weder vorher angehört noch hat er sonst eine Möglichkeit, seinen Standpunkt und eventuell entlastende Angaben in das Verfahren einzubringen. Er wird teilweise noch nicht einmal darüber informiert, woraus sich die Sicherheitsbedenken in seiner Person ergeben. Der Betroffene wird damit zum reinen Objekt einer staatlichen Maßnahme gemacht. Aus rechtsstaatlicher Sicht ist es daher dringend geboten, in § 28 SPolDVG-E bei negativem Ausgang einer Zuverlässigkeitsüberprüfung eine Pflicht zur vorherigen Anhörung des Betroffenen vorzusehen, um diesem noch die Gelegenheit zu geben, sich persönlich zu den für die Entscheidung erheblichen Tatsachen zu äußern, wie dies auch in § 16 Abs. 7 Saarländisches Sicherheitsüberprüfungsgesetz richtigerweise vorgesehen ist.

8 Schutz von Berufsgeheimnisträgern

Die Notwendigkeit von Anpassungen ergibt sich auch aus dem Urteil des BVerfG vom vorvergangenen Dienstag zu den Befugnissen des Bundesnachrichtendienstes. Nicht zuletzt die dortigen Ausführungen des Gerichts lassen Bedenken aufkommen, ob die in § 41 SPolDVG-E vorgesehenen Regelungen zum Schutz von Berufsgeheimnisträgern verfassungskonform sind.

Die schwer verständlichen Regelungen in § 41 Abs. 4 und 5 schaffen zwei Klassen von Berufsgeheimnisträgern. Die eine Gruppe von Berufsgeheimnisträgern (Abs. 4), zu denen Geistliche, Parlamentarier, Strafverteidiger und Rechtsanwälte gehören und für die ein absoluter Schutz gelten soll. Und die zweite Gruppe von Berufsgeheimnisträgern (Abs. 5), zu denen unter anderem auch Ärzte gehören, für die nur ein relativer Schutz geltend soll. Zu dieser zweiten Gruppe, bei der verdeckte polizeiliche Maßnahmen nach einer Einzelfallabwägung („*im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen*") prinzipiell zulässig sind, gehören auch Journalisten. Gerade diese unterschiedliche Handhabung von Rechtsanwälten auf der einen Seite und Journalisten auf der anderen Seite dürfte so nicht zulässig sein.

Zwar lässt das BVerfG eine unterschiedliche Handhabung in Bezug auf Kategorien von Berufsgeheimnisträgern grundsätzlich zu. Anders als der vorliegende Entwurf verlangt aber das BVerfG, dass zum Schutz der Kommunikationsbeziehungen von Journalisten und ihren Informanten die gleichen Maßstäbe zu gelten haben wie für Rechtsanwälte und ihre Mandanten, mit der Folge, dass die Journalisten im vorliegenden Gesetzentwurf der ersten Gruppe (Abs. 4) zuzuordnen wären, für die ein absoluter Schutz gilt.

9 Bild- und Tonaufzeichnungen

Änderungen der gesetzlichen Vorgaben soll es auch bei der Befugnis zur offenen Anfertigung von Bild- und Tonaufzeichnungen geben, insbesondere für stationäre Videoüberwachungen und beim Einsatz der Bodycam.

So wird der bereits im öffentlichen Raum zulässige Einsatz von Bodycams nun auch auf den Bereich von Wohnungen erweitert. § 32 Abs. 3 Satz 2 SPolDVG-E sieht hierzu vor, dass zum Schutz der eingesetzten Polizeivollzugsbeamten eine offene Anfertigung von Bild- und Tonaufzeichnungen in Wohnung zulässig ist, sofern dies zur Abwehr einer dringenden Gefahr für Leib oder Leben erforderlich ist. Wir begrüßen, dass im Vergleich zu früheren Entwürfen dieser Norm nunmehr als Voraussetzung für einen Einsatz in Wohnungen eine dringende Gefahr für Leib oder Leben als Eingriffsschwelle nominiert wird, da wir dies vor dem Hintergrund des Art. 13 Abs. 5 GG für zwingend erforderlich halten, um die Vorschrift verfassungskonform auszugestalten.

Für den Bereich der Videoüberwachung öffentlich zugänglicher Orte wird in § 32 Abs. 2 Nr. 1 SPolDVG-E eine Klarstellung dahingehend aufgenommen, dass eine Videoüberwachung nur an solchen Orten zulässig ist, an

denen wiederholt Straftaten der Straßenkriminalität begangen worden sind. Wir begrüßen auch diese Klarstellung, die insbesondere die Errichtung stationärer Videoüberwachungsanlage nur an bekannten Kriminalitätsbrennpunkten zulässt.

Als solche Kriminalitätsbrennpunkte werden derzeit von Seiten des Ministeriums insbesondere die Bereiche am Hauptbahnhof und an der Johanneskirche angesehen. Was man hierbei jedoch nicht unberücksichtigt lassen darf ist, dass die Errichtung einer stationären Videoüberwachung auf der Grundlage des erwähnten § 32 Abs. 2 Nr. 1 SPolDVG-E auch zu Verdrängungs- und Verlagerungseffekten führt, mit der Folge, dass ab einem bestimmten Zeitpunkt nicht mehr von einem Kriminalitätsbrennpunkt ausgegangen werden kann und die Voraussetzungen des § 32 Abs. 2 Nr. 1 SPolDVG-E entfallen. Es bedarf daher aus hiesiger Sicht einer regelmäßigen Evaluierung der Kriminalitätslage an den bestehenden Anlagen und einer Überprüfung, ob die Voraussetzungen des § 32 Abs. 2 Nr. 1 SPolDVG-E noch fortbestehen. Um dies rechtssicher und für die Polizei auch praktikabel zu handhaben, schlagen wir daher vor, eine Frist, nach deren Ablauf eine Evaluierung und Prüfung erfolgen muss, gesetzlich vorzusehen. Eine solche Evaluierungsfrist, die wir in einer Größenordnung von allen zwei Jahren für sinnvoll halten, hätte auch für die Polizei den Vorteil, dass bei Entfallen der Tatbestandsvoraussetzungen vor Ablauf dieser Frist die Videoüberwachung vorerst bis zum Ablauf der Evaluierungsfrist rechtskonform weiterbetrieben werden könnte. Dies gibt Planungssicherheit und verhindert, dass aufgrund nur vorübergehender Verlagerungseffekte die Anlage bereits kurz nach Inbetriebnahme wieder entfernt werden muss.

10 Befugnisse der Aufsichtsbehörde

Für offensichtlich europarechtswidrig und für mit dem Unabhängigkeitspostulat der Aufsichtsbehörde unvereinbar halten wir die Regelung zur Ausübung der Abhilfebefugnisse durch die Aufsichtsbehörde. § 6 SPolDVG-E sieht dazu vor, dass bei Verstößen der Polizei gegen datenschutzrechtliche Vorschriften und nach vorheriger fruchtloser Beanstandung dieser Verstöße die Aufsichtsbehörde eine Beschränkung oder eine Untersagung des Verfahrens nur verhängen, sprich anordnen darf, wenn die zuständige Fach- und Rechtsaufsicht – für die Vollzugspolizei das Ministerium für Inneres, Bauen und Sport – hiermit einverstanden ist.

Was bereits absurd klingt, weil schon nicht erkennbar ist, wie nach einem fruchtlosen Ablauf eines unter Beteiligung der Fach- und Rechtsaufsicht durchgeführten Beanstandungsverfahrens noch ein Einvernehmen zu erreichen sein soll, ist auch zweifellos europarechtswidrig.

Die JI-Richtlinie sieht in Art. 42 Abs. 1 vor, dass die Mitgliedstaaten gewährleisten müssen, dass die Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig handelt. Hierzu gehört nach Art. 47 Abs. 2 JI-Richtlinie, dass die Aufsichtsbehörde über wirksame, sprich effektive Befugnisse verfügt, die es ihr gestatten unter anderem eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots zu verhängen. Das schließt selbstverständlich nicht aus, dass gegen diese Maßnahmen der Aufsichtsbehörde auch ein Rechtsweg zu den Verwaltungsgerichten eröffnet ist.

Europarechtswidrig ist es aber, die Wahrnehmung aufsichtsbehördlicher Befugnisse von der Zustimmung oder dem Einvernehmen einer anderen Behörde abhängig zu machen.

Richtig ist die Intention der Regelung, nämlich die Fach- und Rechtsaufsichtsbehörde in das datenschutzrechtliche Aufsichtsverfahren einzubinden und dieser die Möglichkeit zur Stellungnahme zu eröffnen, bevor eine behördliche Anordnung ergeht. Dies wird im vorliegenden Gesetzentwurf bereits durch das vorgeschaltete Beanstandungsverfahren sichergestellt. Durch die gleichwohl zusätzlich vorgesehene Zustimmungsbedürftigkeit wird der kontrollierten Stelle und der ihr vorgesetzten Behörde aber ein entscheidender Einfluss auf die von der Aufsichtsbehörde zu ergreifenden Maßnahmen eingeräumt, der mit dem Erfordernis der Unabhängigkeit nicht vereinbar ist. Bereits im Jahr 2010 hat der EuGH zum Erfordernis der „*völligen Unabhängigkeit*" (Art. 42 Abs. 1 JI-Richtlinie) festgestellt, dass hierbei gewährleistet sein muss, dass die Aufsichtsbehörde *„ihre Aufgaben* ***ohne äußere Einflussnahme*** *[wahrnehmen kann]. Diese Unabhängigkeit schließt nicht nur* ***jegliche Einflussnahme seitens der kontrollierten Stellen*** *aus, sondern auch jede Anordnung und* ***jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar,*** *durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen."* (EuGH, Urteil vom 9.3.2010, Az. C-518/07).

Aus diesen Ausführungen des EuGH lässt sich nur schlussfolgern, dass das in § 6 SPolDVG-E vorgesehene Erfordernis zur Herstellung des Einvernehmens europarechtswidrig und ersatzlos zu streichen ist. Es existieren im Übrigen auch bundesweit keine vergleichbaren Einschränkungen der aufsichtsbehördlichen Befugnisse. Nur beispielhaft erwähnt sei hier der § 69 Abs. 2 BKAG. Nachvollziehbar ist die Befürchtung des Ministeriums, dass eine mögliche Untersagung eines Verfahrens für die Aufgabenwahrnehmung der Polizei erhebliche Konsequenzen haben kann. Diesen Bedenken muss hier aber mit den Mitteln des Verwaltungsverfahrensrechts begegnet werden. So ist es unzweifelhaft und unstrittig - und wird auch durch § 6 Abs. 3 SPolDVG-E ausdrücklich klargestellt -, dass die Polizei gegen eine Untersagungsanordnung der Aufsichtsbehörde Klage einreichen könnte, die aufschiebende Wirkung hätte, mit der Folge, dass bis zur endgültigen gerichtlichen Entscheidung in der Sache, die Polizei das Verfahren weiterbetreiben könnte und damit aus operativer Sicht keine negativen Folgen zu befürchten hätte.

Vor diesem Hintergrund lässt der hier vom Ministerium vorgesehene Regelungsvorschlag eher die Vermutung zu, dass man im Falle von datenschutzrechtlichen Verstößen eine gerichtliche Klärung datenschutzrechtlich fragwürdiger Verfahren zulasten einer zahnlosen Datenschutzaufsichtsbehörde von vornherein vermeiden will. Dies ist mit europarechtlichen Vorgaben schlichtweg unvereinbar.

Saarbrücken, den 28. Mai 2020