Polizei

SAARLAND

Landespolizeipräsidium

Dienst-gebäude:	Mainzer Straße 134 - 136 66121 Saarbrücken
Bearbeitung:	Thomas Dossow/Marko Groß
Tel.:	0681 962 – 8060/8030
Fax:	0681 962 - 8005
E-Mail:	LPP-Polizei2020@polizei.slpol.de
Az:	LPP-PS1-99.00/80.00-219/2018
Datum:	25.10.2019

Ministerium für Inneres, Bauen und Sport
Referat D 4
Mainzer Straße 136
66121 Saarbrücken

Externe Anhörung zum Entwurf eines Gesetzes zur Neuregelung der polizeilichen Datenverarbeitung im Saarland
Stellungnahme des Landespolizeipräsidiums

a) E-Mail des MIBS, Referat D 4, vom 03.09.2019
b) 06. Sitzung des Bund-Länder-Lenkungsausschuss „Polizei 2020“ am 15.10.2019

Mit Bezug a) wurde der überarbeitete Entwurf eines Gesetzes zur Neuregelung der polizeilichen Datenverarbeitung im Saarland sowie die dazugehörige Gesetzesbegründung zur Kenntnisnahme und Gelegenheit zur Stellungnahme übersandt.
Bevor ich auf die, meiner Einschätzung nach, für die polizeiliche Datenverarbeitung essentiellen Regelungen und aus hiesiger Sicht möglichen Lösungsansätze eingehe, möchte ich an dieser Stelle meinen ausdrücklichen Dank für die gute und konstruktive Zusammenarbeit bei der Erarbeitung dieses Gesetzeswerkes zum Ausdruck bringen.

1) § 23 Abs. 4 SPolDVG-E (Speicherung personenbezogener Daten zur vorbeugenden Bekämpfung von Straftaten)

Das unter dem Namen „Polizei 2020“ verfolgte Vorhaben der deutschen Polizei, ein gemeinsames Datenhaus zu etablieren, genießt nicht nur bei den Sicherheitsbehörden hohe Priorität (vgl. Koalitionsvertrag der Bundesregierung, 2018, Zeile 5785; 207. IMK, TOP 14.7). Dabei geht es vordergründig darum, dass zur polizeilichen Aufgabenwahrnehmung alle relevanten Informationen in einem fachlichen, technischen und organisatorischen Gesamtsystem für die Polizeien in Bund und Ländern nutzbar sind. Mit dem initialen fachlichen Bebauungsplan, welcher in der 06. Sitzung des BLLA (Bezug b)) Gegenstand war, wird das Datenhaus der deutschen Polizei in einem Zielbild und in einer Transformationsphase konkretisiert. Wesentlich für die mit dem Datenhaus verbundene Zielerreichung im Sinne der Saarbrücker Agenda ist

unter anderem die Erkennung und Darstellung der Verbundrelevanz mittels Qualifizierungsdienst. Damit der Qualifizierungsdienst im Sinne einer effektiven Aufgabenwahrnehmung bundesweit zum sachgerechten Einsatz gebracht werden kann, ist die frühestmögliche Bereitstellung der relevanten personenbezogenen Daten (pbD) im Datenhaus von jedem Teilnehmer zwingend.
Die Bereitstellung und somit die Speicherung der Daten stellt einen eigenen Rechtseingriff dar und bedarf einer gesetzlichen Grundlage. Da die Daten sowohl präventiv- als auch repressivpolizeilichen Zwecken dienen sollen, handelt es sich um eine sog. „Mischdatei" i. S. d. § 483 Abs. 3 StPO, so dass sich die Datenverarbeitung nach den Bestimmungen des jeweiligen Polizeigesetzes – im Saarland zukünftig nach dem SPolDVG-E – richtet.

Bezweckt die Speicherung und Verwendung von Daten die schnellere Aufklärung von zukünftigen Straftaten oder die Aufklärung von in der Vergangenheit begangenen Straftaten, die zum Zeitpunkt der Verarbeitung noch nicht bekannt sind, unterfällt dies dem Zweck der Strafverfolgungsvorsorge. Diese erfolgt in zeitlicher Hinsicht präventiv, betrifft aber gegenständlich das repressiv ausgerichtete Strafverfahren und unterfällt der konkurrierenden Gesetzgebung nach Art. 74 Abs. 1 GG (BVerfGE 113, 348 - Vorbeugende/vorsorgende TKÜ gegen Straftaten). Eine Datenverarbeitung, die das Ziel verfolgt, durch Sammlung und Verdichtung von Informationen den Eintritt einer Gefahr in Form der Begehung von Straftaten zu verhindern, unterfällt der Straftatenverhütung. Diese ist gem. v. g. Entscheidung des BVerfG ausschließlich präventiver Natur und unterliegt der ausschließlichen Gesetzgebung der Länder.

Beschriebene Strafverfolgungsvorsorge und Straftatenverhütung sind im SPolDVG-E unter der vorbeugenden Bekämpfung von Straftaten zusammengefasst. Die Speicherung, Veränderung und Nutzung der Daten für diese Zwecke bzw. den Zweck der vorbeugenden Bekämpfung von Straftaten findet sich in § 23 Abs. 4 und 5 SPolDVG-E wieder. Wesentliches Unterscheidungsmerkmal zwischen § 23 Abs. 4 und Abs. 5 SPolDVG-E sind die betroffenen Personenkategorien. Abs. 4 umfasst die Personenkategorie des Tatverdächtigen sowie Verurteilten. Abs. 5 hingegen umfasst die Anlassperson, die Kontakt- und Begleitperson, das potentielle Opfer, den Zeugen, den Hinweisgeber und die sonstige Auskunftsperson. Während bei einem Tatverdächtigen oder Verurteilten (Abs. 4) die pbD zwangsläufig aus Strafverfahren stammen, können im Gegensatz zum aktuellen § 30 Abs. 4 SPolG nach § 23 Abs. 5 SPolDVG-E auch bei den dort beschriebenen Personenkategorien die Daten aus Strafverfahren stammen. Die Speicherung und Verwendung der Daten der beschriebenen Gruppen – Ausnahme die Anlassperson – bedarf hierbei einer Prüfung der Erforderlichkeit nach einem Jahr und darf insgesamt drei Jahre nicht überschreiten. Einer Wiederholungs- bzw. Negativprognose bedarf es hingegen nicht. Dieser bedarf es im Gegensatz hierzu nach den Bestimmungen des § 23 Abs. 4 SPolDVG-E, so dass Verurteilte und Tatverdächtige gegenüber Opfer, Zeugen etc. tendenziell privilegiert werden, auch wenn die pbD von Verurteilten und Tatverdächtigen im Gegensatz zu den Personen aus Abs. 5 grundsätzlich bis zu 10 Jahren gespeichert werden können und es keiner Prüfung der Notwendigkeit der Speicherung nach einem Jahr bedarf.

Die künftige Neustrukturierung des polizeilichen Informationsverbundes (Stichworte „Polizei 2020“ und „Saarbrücker Agenda“) sowie eine moderne und effektive landesinterne polizeilichen Datenverarbeitung (Stichwort „Analysesysteme zur operativen und strategischen Auswertung“) machen eine möglichst frühzeitige Datenbereitstellung erforderlich. Diese wird jedoch aufgrund der Notwendigkeit der Erstellung der Wiederholungs- bzw. Negativprognose für die Personenkategorie des Verurteilten oder Verdächtigen erheblich erschwert, da häufig erst zu einem späteren Zeitpunkt, wenn ausreichend Personenerkenntnisse vorliegen, eine substantiierte kriminalistisch-kriminologische Prognose einer negativen Legalbewährung möglich ist. Wohl auch deshalb, haben die Polizeigesetze z.B. der Länder Bayern, Berlin, Brandenburg, Sachsen-Anhalt, Sachsen, Thüringen, Nordrhein-Westfalen, Rheinland-Pfalz und Hessen von der Notwendigkeit der Erstellung einer Wiederholungs- bzw. Negativprognose für Verurteilte und Tatverdächtige Abstand genommen.

Lösungsansatz: Befristeter Verzicht auf die Notwendigkeit der Erstellung einer Wiederholungs- bzw. Negativprognose für die Personenkategorie des Verurteilten und des Tatverdächtigen

Formulierungsvorschlag für einen neugefassten § 23 Abs. 4 SPolDVG:

„Die Vollzugspolizei kann personenbezogene Daten

1. *die sie im Rahmen von Strafermittlungsverfahren über Personen gewonnen hat, die verdächtig sind, eine mit Strafe bedrohte Tat begangen zu haben oder*
2. *von Personen, die wegen einer solchen verurteilt wurden,*

speichern, verändern sowie verwenden, soweit das zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Die suchfähig gespeicherten personenbezogenen Daten sind zu löschen

1. *nach Fristablauf von zwei Jahren oder wenn*
2. *die betroffene Person im Strafverfahren rechtskräftig freigesprochen wurde oder*
3. *die Eröffnung des Hauptverfahrens gegen sie unanfechtbar abgelehnt wurde oder*
4. *das Verfahren nicht nur vorläufig eingestellt ist und sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Straftat nicht oder nicht rechtswidrig begangen hat.*

Eine Speicherung über die in Satz 2 Nummer 1 genannte Frist hinaus ist nur zulässig, wenn wegen der Art, Ausführung oder Schwere der Tat oder der Persönlichkeit der betroffenen Person die Gefahr der Wiederholung besteht.“

2) § 21 Abs. 1 S. 1 SPolDVG-E (Rechtsgrundlage für die Vorgangsbearbeitung)

Die in § 21 Abs. 1 S. 1 SPolDVG-E vorzufindende Formulierung, nach der die Polizei personenbezogene Daten speichern, verändern sowie verwenden kann, soweit dies zur Erfüllung ihrer Aufgaben, zur Vorgangsverwaltung oder zur Dokumentation erforderlich ist, löst den derzeit in § 31 SPolG vorzufindenden strengen Zweckbindungsgrundsatz

auf. Hiermit wurde einer der Forderungen seitens des LPP Rechnung getragen, was ich begrüße.

Aufgrund der wiederholt und eindringlich artikulierten fachlichen Bedarfe seitens der hiesigen Fachdienststelle dient das Vorgangsbearbeitungs-/Vorgangsverwaltungssystem POLADIS (VBS POLADIS) derzeit neben der Vorgangsverwaltung und Dokumentation auch und im Besonderen der dem LPP gesetzlich zugeschriebenen Aufgabe der Strafverfolgung und Gefahrenabwehr, indem die gespeicherten Daten mittels der systemimmanenten Suchfunktion in einem landesweiten Lesezugriff zur Verfügung stehen. Der suchfähige Datenumfang orientiert sich hierbei an der dem/der jeweiligen Mitarbeiter*in zugeschriebenen Aufgabe. Hierdurch kann beispielsweise zeitnah nach einem Namen oder einer Telefonnummer, der bzw. die im Zuge eines aktuell betriebenen Strafverfahrens bekannt wurde, gesucht werden. Im Trefferfall können unter Beachtung der gesetzlichen Voraussetzungen die entsprechenden Daten in das aktuelle Strafverfahren eingebracht werden oder evtl. ein neues Strafverfahren eröffnet werden.

Aus den beschriebenen Umständen wird von hier um Klarstellung bzw. erläuternde Darstellung innerhalb der Gesetzesbegründung dahingehend gebeten, dass es sich bei der in § 21 Abs. 1 S. 1 SPolDVG-E vorzufindende Speicherung, Veränderung und Verwendung personenbezogener Daten zur „Aufgabenerfüllung“ um eine Generalklausel handelt, die die gesamte Bandbreite polizeilicher Aufgaben umfasst. Hiervon umfasst ist auch die im Vorfeld konkreter Gefahren liegende vorbeugenden Bekämpfung von Straftaten, sofern die Voraussetzungen spezieller Vorschriften wie z. B. des § 23 Abs. 4 SPolDVG-E (noch) nicht vorliegen (vgl. Bayerischer Verfassungsgerichtshof, Az. Vf. 12-VII/92, 19.10.1994, Schmidtbauer in: beck-online, Polizeiaufgabengesetz, Schmidtbauer/Steiner, 4. Auflage, 2014, Rn.5 Bäuerle in: beck-online, Polizei und Ordnungsrecht Hessen, Möstl/Mühl, 11. Edition, Stand: 10.04.2018, Rn 28). Zum anderen erlaubt die Befugnis auch die Speicherung, Veränderung sowie Verwendung der Daten für Zwecke des (aktuell betriebenen) Strafverfahrens, wenn diese in einer sog. „Mischdatei“ erfolgt, in welcher die dortigen Datenbestände sowohl präventiven als auch repressiven Zwecken dienen (vgl. § 483 Abs. 3 StPO).

Die datenschutzrechtliche Sensibilität der beschriebenen Nutzung des VBS POLADIS als Informationssystem ist dem LPP durchaus bewusst. Diesbezüglich kritische Stimmen, die ausschließlich die „Vorgangsverwaltung“ als Zweck der Datenverarbeitung eines VBS erkennen, sind hier bekannt (vgl. Bäuerle in: beck-online, Polizei und Ordnungsrecht Hessen, Möstl/Mühl, 11. Edition, Stand 10.04.2018, Rn 40 und 40.1). Ebenso die offenbar in selbige Richtung zielende Stellungnahme des Unabhängigen Datenschutzzentrums des Saarlandes (Az. S 2600/970 – vom 22. Juli 2019) im Sachzusammenhang des Löschmoratoriums aufgrund der Vorfälle bei der Universitätsklinik in Homburg/Saar.

Sofern allerdings der v. g. Bewertung gefolgt wird und somit der Zweck der Datenverarbeitung innerhalb eines VBS ausschließlich in der „Vorgangsverwaltung“ und nicht in der „Aufgabenerfüllung“ erkannt wird, ist die Nutzung des VBS als Informationssystem mehr als fraglich. Die entsprechenden Suchfunktionalitäten

müssten voraussichtlich auf die jeweiligen Organisationseinheiten beschränkt werden. Eine umfängliche Suche wäre lediglich in den „Vorsorgedateien“ wie z. B. POLIS möglich. Zudem würde eine solche Bewertung die Teilnahme am „Datenhaus der Polizei“ gefährden. Im Datenhaus soll perspektivisch eine einmalige Datenhaltung erfolgen und Datenzugriffe mittels Qualifizierungsservices (z.B. Verbundrelevanz) sowie Rechte-/Rollenkonzept über verschiedene Sichten auf die Daten ermöglicht werden.

Selbstverständlich bedarf es infolge der Verwendung der Daten zur Aufgabenerledigung auch der Beachtung der Grundsätze der Zweckbindung – ggf. der hypothetischen Datenneuerhebung sowie der hierzu notwendigen Kennzeichnung – der Daten. Auf diesen Umstand wurde bereits grundsätzlich in der Gesetzesbegründung zu § 22 Kennzeichnung SPolDVG-E hingewiesen.

Lösungsansatz: Berücksichtigung der vorstehenden Erläuterungen in der Gesetzesbegründung zu § 21 Abs. 1 S. 1 SPolDVG-E.

3) § 21 Abs. 1 Satz 1 vs. § 23 Abs. 2 SPolDVG-E (Rechtsgrundlage für die Auswertung/Analyse)

Mit Beschluss des AK II zu TOP 38 (Anschlagsgeschehen mit rechtsextremistischen Hintergrund am 09.10.19 in Halle (Saale) und Landsberg OT Wiedersdorf) wurde eine „priorisierte Ertüchtigung der polizeilichen […] Datensysteme hinsichtlich ihrer Analysefähigkeit“ empfohlen. Solche Analysemaßnahmen sollten rechtssicher durchgeführt werden können.

Fraglich scheint, ob das SPolDVG-E für diese Zwecke über ausreichende Rechtgrundlagen verfügt. Es bedarf einer Befugnisnorm, die es erlaubt, personenbezogene Daten unterschiedlicher Betroffenkreise auf gemeinsame Strukturen, Handlungsmuster, Personengruppen sowie zeitliche, sachliche und situative Zusammenhänge zu analysieren. Die bisherige Trennung der Daten in unterschiedliche Dateien, wie z. B. POLIS, POADIS, KRISTAL-SL, steht diesem Erfordernis entgegen.

Es bedarf der Klarstellung, ob die in der Generalklausel des § 21 Abs. 1 Satz 1 SPolDVG-E erlaubte „Verwendung“ von Daten zur notwendigen Analyse berechtigt und wie sich hierbei das Verhältnis zu den in § 23 SPolDVG-E aufgeführten Grundsätzen der Zweckbindung darstellt. Gleichzeitig sollte erläutert werden, inwiefern die beabsichtigten Analysezwecke von der in § 21 Abs. 1 Satz 1 SPolDVG aufgeführten Aufgabenerfüllung umfasst sind und wie sich diese zur Zweckbindung verhalten. Hierbei ist beachtlich, dass Hessen bereits mit § 25a HSOG eine bereichsspezifische Norm zur Datenanalyse geschaffen hat und Hamburg dies mit § 49 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG HH) beabsichtigt.

Die Gesetzesbegründungen zu beiden v. g. Normen heben hervor, dass die neugeschaffene Norm keine Befugnisnorm zur Erhebung neuer personenbezogener Daten, sondern lediglich die automatisierte Analyse bereits rechtmäßig erlangter Daten darstellt. Aufgrund der Eingriffsintensität begrenzen beide Normen die Analyse auf die

vorbeugende Bekämpfung von den in § 100a Abs. 2 der StPO genannten Straftaten oder sofern dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist. Zudem steht die Durchführung entsprechender Analysen unter dem Vorbehalt der Behördenleitung.

Lösungsansatz: Klarstellung der Rechtsgrundlage für die Auswertung/Analyse im SPolDVG sowie deren Verhältnis zu § 23 SPolDVG-E.

4) § 54 Abs. 1 Satz 1 SPolDVG-E (Datenschutz-Folgenabschätzung; Risiko der Datenverarbeitung)

Art. 27 der JI-Richtlinie 2016/680 führt für die Datenverarbeitung, die zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit durchgeführt wird, das Konzept der Datenschutz-Folgeabschätzung (DSFA) ein. Das SPolDVG-E berücksichtigt dies in § 54.
Das Konzept der DSFA basiert auf dem Grundsatz des risikobasierten Datenschutzes und verlangt von dem Verantwortlichen eine eigenverantwortliche und detaillierte Risikoanalyse der eigenen Datenverarbeitung (vgl. u. a. Baumgartner in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Auflage 2018, Rn. 1, beck-online-kommentar). Der risikobasierte Ansatz verpflichtet den Verantwortlichen zu spezifischen Maßnahmen und Vorkehrungen entsprechend dem jeweiligen Risiko der jeweiligen konkreten Datenverarbeitung. Im Gegensatz zu pauschalen und undifferenzierten Verpflichtungen soll hierdurch ein effektives Datenschutzsystem entstehen. Es ist ein dem Risiko angemessenes Schutzniveau zu gewährleisten und zu diesem Zweck sind geeignete technische und organisatorische Maßnahmen zu ergreifen. Der Risikobegriff findet sich dementsprechend sowohl in Art. 27 Abs. 1 der JI-Richtlinie 2016/680 als auch in den Erwägungsgründen 58 und 60.

Der derzeitige § 54 Abs. 1 Satz 1 SPolDVG-E wird nach hiesiger Bewertung dem durch den europäischen Gesetzgeber geforderten risikobasierten Ansatz nicht in Gänze gerecht oder birgt doch zumindest durch die aktuelle Wortwahl das Risiko von Missverständnissen, indem Satz 1 lautet: „Hat eine Form der Verarbeitung [...] voraussichtlich eine erhebliche Gefahr...“. Es wird der Gefahrenbegriff der „erheblichen Gefahr“ aufgeführt, der ohne jeden Zweifel mit der Abwehr von Gefahren für die öffentliche Sicherheit konnotiert ist, statt den seitens der JI-Richtlinie 2016/680 geforderten Risikobegriff zu wählen.

Die beschriebenen Anforderungen der JI-Richtlinie 2016/680 und im Besonderen zukünftige Fragestellungen, die bei der Durchführung einer DSFA auftauchen werden, begründen nach hiesiger Bewertung den Anpassungsbedarf der Norm. Verbleibt es bei der derzeitigen Formulierung, erschwert dies den Rückgriff auf einschlägige Werke zur DSFA, wie z. B. des „White Paper Datenschutz-Folgenabschätzung - Ein Werkzeug für einen besseren Datenschutz“ des Forums für Privatheit“, das Kurzpapier Nr. 5 zur DSFA

der Datenschutzkonferenz aus dem Jahre 2017 oder auf entsprechende Kommentare zum Thema. Vorbezeichnete Veröffentlichungen sowie andere hier bekannte Papiere sprechen vom „Risiko“ und nicht von einer „Gefahr“.
Dem LPP ist bekannt, dass der Bundesgesetzgeber die in § 54 SPolDVG-E vorzufindende Wortwahl auch in § 67 Bundesdatenschutzgesetz (BDSG) gewählt hat. Allerdings hat der Kooperationspartner Rheinland-Pfalz in § 56 Abs. 1 seines Landesdatenschutzgesetzes (LDSG) das „hohe Risiko“ erwähnt, so dass mit Blick auf die IT-Kooperation eine mögliche Vergleichbarkeit der entsprechenden Landesnormen angestrebt werden sollte.

Lösungsansatz: Den in § 54 Abs. 1 Satz 1 aufgeführten Begriff der „erheblichen Gefahr“ ersetzen durch „hohes Risiko“.

5) § 6 Abs. 2 Nr. 3 SPolDVG-E (Befugnisse der Aufsichtsbehörde – hier: Beschränkung und Verbot der Verarbeitung)

Die Vorschrift des § 6 SPolDVG-E setzt laut Gesetzesbegründung Art. 47 der JI-Richtlinie 2016/680 um und orientiert sich an § 16 BDSG.
§ 16 Abs. 2 BDSG beschränkt hierbei die Befugnisse des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) auf die Instrumente der Beanstandung, der aus Art. 47 Abs. 2 lit. a) der JI-Richtlinie 2016/680 entnommenen Warnung und auf sonstige nicht regelungsbedürftigen Möglichkeiten, den als öffentliche Stelle an Recht und Gesetz gebundenen Verantwortlichen auf die aus Sicht der Aufsichtsbehörde rechtswidrige Verarbeitung personenbezogener Daten aufmerksam zu machen.
§ 6 Abs. 2 SPolDVG hingegen überträgt der LfDI weitreichendere Befugnisse bis hin zum Verbot der Verarbeitung der Daten. Die äußerst weitreichende Befugnis des Verbotes lässt sich im Bereich der Straftatenverhütung, -ermittlung und –verfolgung sowie der straftatenbezogenen Gefahrenabwehr nicht mit der Sensibilität und Komplexität der entsprechenden Verarbeitungen und dem Bedürfnis nach ständiger Verfügbarkeit rechtmäßig erhobener Daten und Datenverarbeitungsanlagen in Einklang bringen (vgl. BT-Drs. 18/11325, S. 88). So wäre eine effiziente und sachgerechte Aufgabenwahrnehmung beispielsweise gefährdet, wenn die Datenverarbeitung unter Einsatz des Vorgangsbearbeitungs-/-verwaltungssystems POLADIS verboten würde. Die gesetzliche Pflicht zur Unterrichtung des BKA als Zentralstelle im Informationsverbund (§ 32 BKAG) wäre erheblich gefährdet, würde die Datenverarbeitung innerhalb des polizeilichen Fahndungs- und Informationssystems POLIS Saarland verboten.

Lösungsansatz: Verzicht auf die in § 6 Abs. 2 Nr. 3 SPolDVG-E der LfDI eingeräumte Möglichkeit des Verbotes (vgl. § 42 LDSG RP, § 14 HDSIG HE).

6) § 31 SPolDVG-E (Drittbetroffenheit durch besondere Formen der Erhebung personenbezogener Daten)

Die Norm regelt die verdeckte Erhebung pbD durch gesetzliche bestimmte Maßnahmen wie etwa Observation oder verdeckte Bildaufnahmen. Die Maßnahmenadressaten werden durch § 17 Abs. 2 Nr. 1 (potentielle Tatverdächtige) oder Nr. 2 (Kontaktpersonen zu vorgenannten) SPolDVG-E abschließend bestimmt. In Betrachtung der Anwendungspraxis dieser Maßnahmen wird offensichtlich, dass eine Drittbetroffenheit durch solche Maßnahmen nicht ausgeschlossen werden kann. So findet beispielsweise die Observation potentieller Tatverdächtiger, z.B. eines islamistischen Gefährders, gerade im öffentlichen Raum statt. Ziel der Observation ist es dabei auch, Kontaktpersonen, welche im Sinne des § 17 Abs. 2 Nr. 2 lit. a bis c SPolDVG-E mit der potentiellen Straftat in Verbindung gebracht werden können, zu identifizieren. Da gerade die Observation geeignet ist, entsprechende Informationen zu der kontaktierten Person zu liefern, kann in vielen Fällen nicht vermieden werden, dass unbeteiligte Dritte durch die Maßnahmen in ihren Grundrechten betroffen werden. Der Wortlaut des § 31 SPolDVG-E lässt es jedoch nicht zu, dass dritte Personen auch nur geringfügig von den verdeckten Informationserhebungsaßnahmen betroffen werden dürfen, wie dies z.B. in § 35 Abs. 1 S. 3 SPolDVG-E Regelungsgegenstand ist (vgl. auch § 28 POG RP oder § 45 BKAG).

Lösungsansatz: Ergänzung des Wortlautes in § 31 Abs. 1 um folgenden Satz: „Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind."

7) § 32 Abs. 3 Satz 2 i.V.m. § 23 Abs. 2, 3 SPolDVG-E (Verwendungsbeschränkung pbD im Rahmen des Einsatzes der Bodycam in Wohnungen)

Die Zielrichtung des Einsatzes der Bodycam in Wohnungen ist zunächst präventiver Natur und soll potentielle Angriffe auf Polizeibeamten verhindern. Dennoch entspricht es der Praxis, dass es zu Angriffen auf Polizeibeamte in Wohnungen kommt. Die im Wege des Einsatzes der Bodycam hergestellten Bildaufnahmen sollen in diesen Fällen sekundär dazu dienen, ein beweissicheres Strafverfahren durchzuführen. Aufgrund der Tatsache, dass der Einsatz der Bodycam seine verfassungsrechtliche Schranke in Art. 13 Abs. 5 GG findet, sind bei der zweckändernden Verwendung der pbD die Anforderungen der Verfassung zu berücksichtigen, wonach die Zweckänderung unter Richtervorbehalt gestellt wird.
Während in § 23 Abs. 1 S. 4 SPolDVG-E bei der zweckidentischen Verarbeitung pbD, welche im Rahmen des Einsatzes der Bodycam erlangt wurden, den verfassungsrechtlichen Richtervorbehalt berücksichtigt, fehlt es bei der zweckändernden Verarbeitung (hyDaNe) in den Absätzen 2 und 3 an einer entsprechenden Regelung.

Lösungsansatz: Ergänzung des Wortlautes in § 23 Abs. 3 SPolDVG-E um einen entsprechenden Richtervorbehalt (analog § 23 Abs. 1 SPolDVG-E)

8) Begründung zu § 12 Abs. 1 Satz 2 SPolDVG-E (Richtigkeit von Aussagen und Beurteilungen)

Gemäß den Erwägungsgründen 30 und 47 soll sich der seitens der JI-Richtlinie 2016/680 geforderte Grundsatz der sachlichen Richtigkeit bei subjektiven Wahrnehmungen nicht auf deren Inhalt beziehen. In § 12 Abs. 1 Satz 2 SPolDVG-E wird diesem Grundsatz durch die Formulierung: „Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung.“, grundsätzlich Rechnung getragen. Gleichwohl drängt sich bei der gewählten Formulierung die Frage des Gegenstandes der sachlichen Richtigkeit auf (Was betrifft die Frage der Richtigkeit, wenn nicht den Inhalt der Aussage oder Beurteilung?).

Der Anregung des Landespolizeipräsidiums zur Klarstellung den Satz 2 um den beispielsweise in § 58 BDSG vorzufindenden Halbsatz „…, sondern die Tatsache, dass die Aussage oder Beurteilung so erfolgt ist“ zu ergänzen, will das MIBS nach eigener Aussage in der Besprechung vom 23.11.2018 nicht folgen. Jedoch wurde in selbiger Besprechung in Aussicht gestellt, die Anregung des LPP in der Gesetzesbegründung zu berücksichtigen. Die dort vorzufindende derzeitige Formulierung lautet: „Die Vorschrift des Satzes 2 bezieht sich dabei nicht auf den Inhalt von Aussagen, sondern ausschließlich auf den Umstand der Vernehmung selbst.“

Der bereits erwähnte Grundsatz der sachlichen Richtigkeit der Daten soll sich gerade nicht auf die Richtigkeit subjektiver Aussagen beziehen, sondern lediglich auf die Tatsache, dass eine solche Aussage getätigt wurde. Eine Aussage in diesem Sinne kann nicht nur - wie in der Gesetzesbegründung aufgeführt - eine Vernehmung und somit der Inhalt einer Beschuldigten- oder Zeugenaussage sein. Umfasst hiervon sind insbesondere auch polizeifachliche Bewertungen, wie beispielsweise die „Negativ-/Wiederholungsprognose“ im Sinne des aktuellen § 30 Abs. 2 SPolG oder des zukünftigen § 23 Abs. 4 SPolDVG-E. Die derzeitige Formulierung hingegen birgt das Risiko, dass lediglich der „Umstand von *Vernehmungen*“ von Satz 2 umfasst wird.

Lösungsansatz: Anpassung der Gesetzesbegründung wie folgt: „*Satz 2 dient der Berücksichtigung der im Erwägungsgrund (EG) 30 der JI-RiLi vorzufindenden Aussage, dass der Grundsatz der sachlichen Richtigkeit sich nicht auf die Richtigkeit einer Aussage beziehen sollte, sondern lediglich auf die Tatsache, dass eine bestimmte Aussage gemacht worden ist. Gleichzeitig findet sich der in EG 47 der JI-RiLi enthaltende Gedanke wieder, wonach zur Vermeidung massenhafter und nicht erfolgversprechender Anträge klargestellt wird, dass sich die Berichtigung auf Tatsachen bezieht, die die betroffene Personen berühren, und nicht etwa auf den Inhalt von Zeugenaussagen. Hiervon umfasst sind auch polizeifachliche Bewertungen.“*

9) § 28 Abs. 1 SPolDVG-E (Abgleich von personenbezogenen Daten)

Der Abgleich von pbD gehört zweifelsohne zu einer Standardmaßnahme polizeilichen Handelns. Dabei wird mit § 28 Abs. 1 SPolDVG-E geregelt, dass pdD der Normadressaten mit zu polizeilichen Zwecken gespeicherten personenbezogenen

Daten abgeglichen werden dürfen. Die Formulierung lässt jedoch offen bzw. ist dahingehend unbestimmt, welcher Datenbestand (Dateisystem) und welcher Datenumfang für den jeweiligen Abgleich im Einzelfall herangezogen werden darf (vgl. BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 142/15, Rn. (109 ff.).
Dass die Unbestimmtheit der Norm zu praktischen Problemen führt, wird z.B. im Kontext des PoC Datenkonsolidierung augenscheinlich. Hier stellt sich die Frage, ob es für die Polizei des Saarlandes zulässig ist, einen Abgleich im Rahmen eines Datenverbundes in einem Datenbestand der Polizei Rheinland-Pfalz durchzuführen oder ob nur eigene (saarländische) Datenbestände für den Abgleich zugelassen sind. Durch eine Schärfung des Wortlautes könnte dieser Probelmstellung begegnet werden. Darüber hinaus muss allerdings auch eine zweckbezogene Begrenzung des Abgleichs im Einzelfall erfolgen (vgl. BVerfG. a.a.O., Rn. 111).

Lösungsansatz: Konkretisierung des Regelungsinhaltes dahingehend, dass

- **der Abgleich mit dem Inhalt von Dateisystemen zulässig ist, welche die Vollzugspolizei selbst führt oder für die sie eine Berechtigung zum Abruf hat,**
- **der Abgleich auf die Dateisysteme zu beschränken ist, welche den legitimen Zweck fördern.**

10) § 45 Abs. 2 SPolDVG-E (Datenverbund)

In der Befassung zum PoC Datenkonsolidierung fand vor dem Hintergrund eines informellen „Positionspapiers“ seitens des Unabhängigen Datenschutzzentrums des Saarlandes am 26.09.2019 eine Besprechung mit Herrn Gadorosi (Gesamtprogrammleiter Polizei 2020) statt. In diesem Kontext wurde durch das BKA vorgetragen, dass die bloße Rechtsgrundlage zur Einrichtung eines Dateienverbundes - wie mit § 42 Abs. 2 SPolDVG-E beabsichtigt - als nicht ausreichend erachtet wird, um polizeiliche gespeicherte Daten unterhalb der sog. Verbundschwelle des § 30 BKAG zwischen den am Datenverbund teilnehmenden Ländern verfügbar zu machen. Vielmehr müsse aus der Norm selbst oder zumindest aus der Begründung zur Norm deutlich hervorgehen, dass ein solcher Dateienverbund, wie er insbesondere auch mit dem PoC Datenkonsolidierung bezweckt wird, außerhalb der Regelungen des BKAG zum polizeilichen Informationsverbund (§§ 29 ff. BKAG) stattfinden kann.

Lösungsansatz: Ergänzung der Gesetzesbegründung
Formulierungsvorschlag: „*Absatz 2 ersetzt den § 35 Absatz 2 SPolG und transformiert den der Regelungsintention nicht mehr entsprechenden Begriff des automatisierten Abrufverfahrens in den des Datenverbundes und schafft so eine den technischen Anforderungen folgende Rechtsgrundlage für einen qualitativ erhöhten,* ***auch außerhalb des polizeilichen Informationsverbundes im Sinne des BKAG stattfindenden*** *Informationsaustausch zwischen den genannten Polizeibehörden.* […]“

11) § 23 Abs. 3 SPolDVG-E (Zweckändernde Nutzung personenbezogener Daten, nach Erhebung durch eine präventive Wohnraumüberwachung)

Den verfassungsrechtlichen Anforderungen an den Schutz der Wohnung muss insbesondere hinsichtlich der Verwendung von pbD, welche mittels Video- oder Fototechnik zu präventiven Zwecken i.S. Art. 13 Abs. 4 GG erhoben wurden, Rechnung getragen werden. Daher muss eine Verwendungsbegrenzung dieser speziellen pbD dahingehend stattfinden, dass bei einer Zweckänderung eine repressive Nutzung unzulässig ist.

Lösungsansatz: Wiederaufnahme einer klarstellenden Formulierung aus dem Entwurfsstand des SPolDVG vom 20.12.2018 („Personenbezogene Daten, die durch Herstellung von Lichtbildern oder Bildaufzeichnungen über eine Person im Wege eines verdeckten Einsatzes technischer Mittel in oder aus Wohnungen nach § 34 erlangt wurden, dürfen nicht zu Strafverfolgungszwecken verarbeitet werden.)

12) § 42 Abs. 1 Satz 3 SPolDVG-E (Zustimmungsvorbehalt zur Datenübermittlung in laufenden Ermittlungsverfahren seitens der Staatsanwaltschaft)

Die Regelung stellt die Übermittlung von pbD, welche im Sinne § 23 Abs. 4 und 5 SPolDVG-E zur vorbeugenden Bekämpfung von Straftaten gespeichert wurden, während eines laufenden Ermittlungsverfahrens unter Zustimmungsvorbehalt der Staatsanwaltschaft.
Die Speicherung § 23 Abs. 4 und 5 SPolDVG-E ist in einer Vielzahl von Fällen bereits vor Abschluss eines laufenden Ermittlungsverfahrens rechtlich möglich. Vor dem Hintergrund, dass mit der Saarbrücker Agenda das Ziel verfolgt wird „jederzeit“ die für die Aufgabenerledigung erforderlichen Information den Anwendern zur Verfügung zu stellen, scheint der gegenständliche Zustimmungsvorbehalt nicht mehr sachgerecht. Weiterhin kritisch wird dieser Zustimmungsvorbehalt mit Blick auf die Konzeption des Datenhauses für die deutsche Polizei gesehen, wonach bundesweit alle polizeilichen Daten, also auch die Daten aus Ermittlungsverfahren, (logisch) nur noch einmal existieren und potentiellen Bedarfsträgern im Wege des automatisierten Abrufs zur Verfügung stehen sollen. Sofern Ermittlungsverfahren schützenswerte Inhalte beinhalten und eine Übermittlung der Daten aus diesem Grund im Einzelfall nicht gestattet werden soll, sollte in diesen Fällen, welche nach hiesiger Einschätzung der deutlich kleinere Teil darstellen werden, eine Übermittlungssperre eingerichtet werden. Eine Regelung, wie sie § 42 Abs. 1 Satz 3 SPolDVG-E vorsieht, existiert in vielen Polizeigesetzten indessen nicht (vgl. PolG BW, HB, NW, RP; Anmerkung: ein vergleichbarer Zustimmungsvorbehalt seitens der Staatsanwaltschaft existiert hingegen in § 40 Abs. 3 POG RP – Auskunft an den Betroffenen).

Lösungsansatz: Ersatzloser Wegfall der Regelung (§ 42 Abs. 1 Satz 3 SPolDVG-E)

13) Redaktionelle Anpassungen u. a. infolge der Notwendigkeit der Beachtung der hypothetischen Datenneuerhebung (hyDaNe)

Es wird um nachfolgende Anpassungen gebeten:

- Streichen der Worte „verändern oder sonst verwenden“ in den Absätzen 4 und 5 des § 23 SPolDVG-E; in der aktuellen Lesart der Norm findet durch § 23 Abs. 2 S. 3 SPolDVG-E die hyDaNe für die Absätze 4 und 5 keine Anwendung, dennoch muss gerade bei einem „verändern oder sonst verwenden“ die hyDaNe Berücksichtigung finden. Bei dem Speichern – d. h. der Bevorratung – hingegen nicht (vgl. Verfassungsbeschwerde, Prof. Dr. Matthias Bäcker, vom 21.05.2019, S. 57-59).
- Ersetzen des Begriffs der „Weiterverarbeitung“ in
  - § 22 Abs. 2 SPolDVG-E
  - § 23 Abs. 2 Satz 2 SPolDVG-E
  - Begründungen zu § 2, § 17, § 22

  durch „Verarbeitung“.
- § 17 Abs. 2 SPolDVG-E: Die Ziffer vor dem Wort „Zeuginnen“ durch die Ziffer 4 ersetzen
- Normadressat in § 60 Abs. 1 SPolDVG-E (Verzeichnis der Verarbeitungstätigkeiten) ist der „Verantwortliche“

Mit freundlichen Grüßen

(im Original gezeichnet)

Norbert Rupp

Landespolizeipräsident