UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Fritz-Dobisch-Straße 12 . 66111 Saarbrücken
Postfach 10 26 31 . 66026 Saarbrücken
Telefon 0681/94781 – 0
Telefax 0681/94781-29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de

Unabhängiges Datenschutzzentrum Saarland - Fritz-Dobisch-Str. 12 - 66111 Saarbrücken

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

66121 Saarbrücken

Saarbrücken, 25. Oktober 2019

Az: G 1000 / 022
Bearbeiter/in: Herr Gisch
Durchwahl: -12
E-Mail: gisch@datenschutz.saarland.de

Entwurf eines Gesetzes zur Neuregelung der polizeilichen Datenverarbeitung

Hier: Externe Anhörung

Anlagen: Tabelle mit Formulierungsvorschlägen (15 Seiten)

Sehr geehrter Herr Spaniol,
sehr geehrte Damen und Herren,

für die Möglichkeit zu dem überarbeiteten Gesetzentwurf im Rahmen der externen Anhörung Stellung nehmen zu dürfen, bedanke ich mich. Soweit unsere Anmerkungen aus den bisherigen Stellungnahmen noch aktuell sind, halten wir an diesen weiterhin fest.

1 Anwendungsbereich

[siehe insb. Formulierungsvorschlag 1]

Kritisch sehen wir die Formulierung des Anwendungsbereiches des Gesetzes in § 1 Abs. 1 SPolDVG-E, der auch die Gefahrenabwehr durch die Polizeiverwaltungsbehörden umfasst. Wir nehmen insofern auf unseren bisherigen Schriftverkehr in dieser Sache Bezug.

Die JI-Richtlinie gilt gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Der Zusatz „*einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche*

Sicherheit" macht deutlich, dass Datenverarbeitungen zu Zwecken der Gefahrenabwehr nur dann vom Anwendungsbereich der JIRL erfasst sind, wenn ein Bezug zu den zuvor genannten „*Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung*" besteht. Dass nur die Datenverarbeitung im Rahmen der vollzugspolizeilichen Gefahrenabwehr in den Anwendungsbereich der JIRL fällt, legt auch ErwGr 12 Satz 1 JIRL nahe: „*Die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden sind* ***hauptsächlich*** *auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet, dazu zählen auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht.*" Dies ergibt sich für die Vollzugspolizei aus § 85 Abs. 1 SPolG, der die „*Erforschung und Verfolgung von Straftaten und Ordnungswidrigkeiten*" zu den Hauptaufgaben der Vollzugspolizei zählt.

Primär für die Gefahrenabwehr zuständig und damit nicht im Sinne des ErwGr 12 JIRL „*hauptsächlich*" für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (bzw. Ordnungswidrigkeiten) sind hingegen die Polizeiverwaltungsbehörden nach § 80 Abs. 1 SPolG. Die Polizeiverwaltungsbehörden fallen daher erst dann in den Anwendungsbereich der JIRL, wenn ein verwaltungsrechtliches Verfahren in ein konkretes Ordnungswidrigkeitenverfahren übergeht. Bis zu diesem Zeitpunkt unterfallen die Polizeiverwaltungsbehörden dem Anwendungsbereich der Verordnung (EU) 2016/679 (im Folgenden: DSGVO), auf den in § 1 Abs. 3 SPolDVG-E in Form einer Auffangvorschrift verwiesen wird.

Durch die Formulierung in § 1 Abs. 1 SPolDVG-E wird die Abgrenzung zwischen dem Anwendungsbereich der JIRL und der DSGVO letztlich den Polizeiverwaltungsbehörden, und dort insbesondere den Ortspolizeibehörden, überlassen, die hierdurch einer erheblichen Rechtsunsicherheit ausgesetzt sind. Wir schlagen zur Klarstellung daher eine Formulierung ähnlich wie in § 35 Abs. 1 und 2 DSG NRW bzw. § 45 BDSG vor, mit der eine eindeutige und rechtssichere Abgrenzung durch den Gesetzgeber vorgenommen wird.

2 Drohende Gefahr

Der vorliegende Gesetzentwurf setzt konsequent auf eine Absenkung der Eingriffsvoraussetzungen bei Vorfeldmaßnahmen für schwer in die Privatsphäre und Grundrechte der Bürger eingreifende Ermittlungs- und Überwachungsbefugnisse. Auch wenn er die Begrifflichkeiten vermeidet, so ist doch erkennbar, dass der Gesetzentwurf die Ausführungen des BVerfG im Urteil vom 20. April 2016 - 1 BvR 966/09 – zu den Eingriffsvoraussetzungen bei einer drohenden Gefahr für sich geltend machen will.

Das BVerfG lässt im vorgenannten Urteil (BVerfG, Urteil vom 20. April 2016, - 1 BvR 966/09, Rn. 109ff) die Erhebung von Daten durch heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität im Bereich der Gefahrenabwehr im Vorfeld konkreter Gefährdungen, also bei einer drohenden Gefahr, nur unter besonderen Voraussetzungen und nur zum Schutz „*besonders gewichtiger Rechtsgüter*" zu. Verhältnismäßig ist eine solche Maßnahme nur dann, wenn eine Gefährdung solcher Rechtsgüter im Einzelfall hinreichend konkret absehbar ist – d.h. es müssen bestimmte Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens, das zu

einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt, tragen - und der Adressat der Maßnahmen aus Sicht eines verständigen Dritten den objektiven Umständen nach in sie verfangen ist, was dann der Fall ist, wenn das individuelle Verhalten dieser 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 Gesetzentwurf im Wesentlichen gerecht, da er sich überwiegend an den verfassungsgerichtlichen Anforderungen mit Blick auf die Eingriffsvoraussetzungen und den Schutz „*besonders gewichtiger Rechtsgüter*" orientiert.

Unklarheiten bestehen aus hiesiger Sicht jedoch bei § 31 Abs. 1 Satz 1 SPolDVG-E. Dieser erlaubt unter Rückgriff auf die Formulierungen des BVerfG („*wenn bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine solche Straftat begangen werden soll*") die heimliche Erhebung personenbezogener Daten zur vorbeugenden Bekämpfung von Verbrechen oder anderen gewerbsmäßig, gewohnheitsmäßig oder bandenmäßig begangenen Straftaten. Die hiermit in Bezug genommenen Schutzgüter sind relativ weit und die Vorschrift kann damit auch in Fällen der vorbeugenden Bekämpfung von Gefahren für Sach- und Vermögenswerte herangezogen werden (bspw. gewerbsmäßiger oder bandenmäßiger Diebstahl, § 243 Nr. 3 StGB). Der Schutz von Sach- und Vermögenswerten stellt hingegen nach Auffassung des BVerfG auch bei bedeutsamen Sachwerten kein hinreichend gewichtiges Rechtsgut dar (BVerfG, Urteil vom 20. April 2016, - 1 BvR 966/09, Rn. 155) und kann damit nicht als Grundlage für Vorfeldmaßnahmen zur Abwehr einer drohenden Gefahr herangezogen werden. Dies deutet auf den ersten Blick auf eine Verfassungswidrigkeit der Vorschrift hin.

Für die verfassungsrechtliche Bewertung der Regelung des § 31 Abs. 1 Satz 1 SPolDVG-E ist jedoch zu berücksichtigen, dass Adressaten entsprechender Maßnahmen nur Personen nach § 17 Abs. 2 Nr. 1 und 2 SPolDVG-E sein dürfen. Die Maßnahme nach § 31 Abs. 1 Satz 1 SPolDVG-E darf sich folglich nur gegen solche Personen richten, bei denen in tatsächlicher Hinsicht ein Straftatenbezug vorliegt. Damit verlangt der Gesetzentwurf in Bezug auf den Adressatenkreis - im Vergleich zu den vom BVerfG dargelegten Mindestanforderungen – einen erheblich fundierteren Prognosemaßstab und damit erheblich höhere Eingriffsvoraussetzungen. In dieser Auslegung dürfte die Vorschrift daher verfassungsgemäß sein.

Das BVerfG lässt es in Bezug auf die Rechtskonstruktion einer drohenden Gefahr genügen, dass die Maßnahmen gegen solche bestimmten Personen gerichtet werden dürfen, über deren Identität zumindest soviel bekannt ist, dass von einer Beteiligung an einem seiner Art nach konkretisierten und zeitlich absehbaren Geschehen auszugehen ist - dies stellt letztlich eine Vermutung dar – kompensiert den damit verbundenen Eingriff jedoch durch erhöhte Anforderungen an die zu schützenden Rechtsgüter. Würde man die Regelung des § 31 Abs. 1 Satz 1 SPolDVG-E im vorgenannten Sinne verstehen, so wäre die Vorschrift wegen der fehlenden Begrenzung auf „*besonders gewichtige Rechtsgüter*" verfassungswidrig.

Dass die Vorschrift des § 31 Abs. 1 Satz 1 SPolDVG-E nur in dem von uns verstandenen Sinne aufgefasst werden kann, ergibt sich aus einem Vergleich mit anderen Eingriffsbefugnissen, die im SPolDVG-E normiert sind. So modifiziert etwa § 31 Abs. 1 Satz 2 SPolDVG-E die Eingriffsvoraussetzungen für den Adressatenkreis des § 17 Abs. 2 Nr. 1 und 2 SPolDVG-E, indem nicht mehr das Vorliegen von Tatsachen für die Begehung einer Straftat erforderlich ist, sondern lediglich verlangt wird, dass das individuelle Verhalten der Zielperson / des Adressaten die konkrete Wahrscheinlichkeit begründet, dass innerhalb eines übersehbaren Zeitraums durch sie (diese Person) besonders gewichtige Straftaten begangen werden. Hier verlangt das Gesetz keine Tatsachengrundlage mehr, sondern lässt eine gewisse Wahrscheinlichkeit ausreichen und senkt damit ausnahmsweise das Erfordernis an die Konkretisiertheit der Gefahrenprognose für ein polizeiliches Tätigwerden ab. Dies dient jedoch dem Schutz „*besonders gewichtiger Rechtsgüter*" im oben genannten Sinn und ist daher nicht zu beanstanden. Bekräftigt wird unsere Auffassung auch durch § 38 Abs. 1 SPolDVG-E. Die Norm verwendet ebenfalls die Begrifflichkeit des BVerfG mit Blick auf die Eingriffsvoraussetzungen, verweist jedoch nicht auf § 17 Abs. 2 SPolDVG-E als Adressaten der Maßnahme, sondern spricht nur von „*Personen*".

Verfassungsrechtliche Bedenken bestehen indes - und nicht begrenzt auf die Vorschriften des § 31 SPolDVG-E - mit Blick auf die verwendeten Begrifflichkeiten. Während das BVerfG konsequent verlangt, 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 um eine synonyme Formulierung zu der vom BVerfG verwendeten Begrifflichkeit, sondern um eine andere Qualität des Eingriffs. Während eine Annahme sich letztlich auch als falsch herausstellen kann, vor allem dann, wenn diese Annahme, anders als in § 35 Abs. 1 Nr. 2 SPolDVG-E, noch nicht einmal begründet sein muss, verlangt das BVerfG, dass bestimmte Tatsachen, also wahrheitsfähige Aussagen, den Schluss (Konklusion) und damit die logisch zwingende Folge auf ein bestimmtes hinreichend konkretisiertes Geschehen zulassen. Ein Beispielfall soll dies verdeutlichen: Die Polizei erhält den wahrheitsgemäßen Hinweis, dass der Ex-Mann im Freundeskreis im betrunkenen Zustand geäußert habe, beim nächsten Besuchskontakt mit den gemeinsamen Kindern seine Ex-Frau töten zu wollen. Schon eine solche Äußerung lässt die **Annahme** zu, dass durch den Ex-Mann eine Straftat nach § 211 / § 212 StGB begangen werden soll. Nach der Konzeption des SPolDVG-E dürften bereits jetzt verdeckte Überwachungsmaßnahmen gegen die betroffene Person eingeleitet werden. Indes ist allein aus dieser Äußerung die Schlussfolgerung auf die tatsächliche Planung eines Mordanschlags nicht logisch zwingend. Die Voraussetzungen für verdeckte Überwachungsmaßnahmen liegen nach der Vorstellung des BVerfG in diesem Fall und zu diesem Zeitpunkt gerade noch nicht vor. Vielmehr bedarf es erst weiterer Erkenntnisse, etwa Informationen über die Beschaffung einer Waffe, die zusammen und in Kombination mit der Tatsache der Äußerung den logisch zwingenden Schluss zulassen, dass diese Person ein Attentat auf die Ex-Frau vorbereitet. Die **Annahme** eines bestimmten Geschehens und damit das Abstellen auf eine Wahrscheinlichkeitsprognose erlaubt das BVerfG indes lediglich in Bezug auf die Besonderheiten terroristischer Straftaten, wo es ausreichen soll, dass „*das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft terroristische Straftaten begeht*".

3 Regelung von Abhilfebefugnissen

[siehe insb. Formulierungsvorschlag 2 und 3]

Art. 47 JIRL verpflichtet die Mitgliedstaaten dazu, zugunsten der Aufsichtsbehörden wirksame Abhilfebefugnisse zu regeln. Dieser Verpflichtung will der Gesetzentwurf mit § 6 SPolDVG-E nachkommen. Dabei sieht § 6 Abs. 2 SPolDVG-E eine Anordnungsbefugnis vor, die jedoch nur bei erheblichen Verstößen Anwendung finden soll. Art. 47 JIRL ist eine solche Beschränkung auf erhebliche Verstöße nicht zu entnehmen. Selbst unterschwellige Verstöße stellen eine rechtswidrige Datenverarbeitung dar, denen die Aufsichtsbehörden mit wirksamen Mittel zu begegnen hat. Insbesondere auch Art. 47 Abs. 2 lit. b JIRL trifft keine Unterscheidung in Abhängigkeit von der Schwere des Verstoßes.

Problematisch ist auch das der Anordnung vorgeschaltete Beanstandungsverfahren. Dieses ist nicht näher konkretisiert oder durch verfahrensrechtliche Vorgaben gesetzgeberisch ausgestaltet. Es bleibt insbesondere unklar, wem gegenüber zu beanstanden ist und welche Stellen (bspw. Fach- / Rechtsaufsicht) hierbei zu beteiligen sind sowie ob und gegebenenfalls welche Fristen gelten sollen, ab deren fruchtlosem Verstreichen eine Anordnung gegen die verantwortliche Stelle ergehen kann.

4 Abgleich personenbezogener Daten (§ 28 Abs. 1 SPolDVG-E)

[siehe insb. Formulierungsvorschlag 16]

Eine der problematischsten Vorschriften des Gesetzentwurfs ist die Befugnis zum Abgleich personenbezogener Daten in § 28 Abs. 1 SPolDVG-E, denn sie lässt die Ausführungen des BVerfG im Urteil zum BKA-Gesetz (BVerfG, Urteil vom 20. April 2016, - 1 BvR 966/09) zur Zweckbindung gänzlich unberücksichtigt. In der vorgesehenen 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 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.

5 Zuverlässigkeitsüberprüfungen

Die Überprüfung der Zuverlässigkeit von Personen durch einen Abgleich mit polizeilichen Dateien zur Feststellung, ob sicherheitsrelevante Erkenntnisse gegen diese Personen vorliegen, ist für bestimmte Bereiche zum Zwecke der Abwehr von Gefahren für hinreichend gewichtige Rechtsgüter zweifellos geboten. Allerdings greifen diese Überprüfungen tief in das Grundrecht auf informationelle Selbstbestimmung des Betroffenen ein und bedürfen daher einer normenklaren Regelung, die die Voraussetzungen und Begrenzungen eines solchen Verfahrens regelt.

Die in der Vorschrift allein vorgesehene Einwilligung des Betroffenen in den Datenabgleich kann keine hinreichende Rechtsgrundlage für diese Maßnahmen darstellen.

Insoweit sieht bereits ErwGr 35 der JIRL vor, dass eine Einwilligung der betroffenen Person keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen sollte, da sie keine echte Wahlfreiheit habe, weshalb die Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden könne. Dementsprechend sieht auch § 19 Abs. 4 SPolDVG-E vor, dass eine Einwilligung nur dann wirksam ist, wenn sie auf der freiwilligen Entscheidung der betroffenen Person beruht, wobei bei der Beurteilung, ob die Einwilligung freiwillig erteilt worden ist, die Umstände der Einwilligung berücksichtigt werden müssen.

Bei der vorliegend vorgesehenen Einwilligung der Betroffenen kann indes in der Regel nicht von einer Freiwilligkeit ausgegangen werden, da der Betroffene bei einer Verweigerung der Einwilligung mit erheblichen Nachteilen rechnen muss, die insbesondere in den Fällen des § 28 Abs. 3 Nr. 1 SPolDVG-E Einfluss auf die Ausübung seiner beruflichen Tätigkeit haben können.

Die Einwilligung ist zudem hier auch deshalb ein untaugliches Mittel, da es für die Wirksamkeit einer Einwilligung unabdingbar ist, dass der Betroffene im Zeitpunkt der Abgabe der Erklärung eine ausreichende Fakten-, Tatsachen- und Informationsgrundlage (Informiertheit der Einwilligung) haben muss, um die Folgen und Auswirkungen der Erteilung einer Einwilligung abschätzen zu können. Dies ist im Falle von Zuverlässigkeitsüberprüfungen nicht gewährleistet, 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 der bei der Polizei gespeicherten personenbezogenen Daten, die Eingang in die

Zuverlässigkeitsüberprüfung finden, ebenso wie das spätere Ergebnis der polizeilichen Bewertung, ob mit Blick auf seine Person Sicherheitsbedenken bestehen, nicht abschätzen und voraussehen kann.

Die Vorschrift des § 28 Abs. 3 SPolDVG-E ist daher in der vorliegenden Form zu streichen. Wir schlagen stattdessen vor, in einem neuen Paragraphen eine spezifische Rechtsgrundlage zu schaffen, die Voraussetzungen, Umfang und Schutzvorkehrungen der Zuverlässigkeitsüberprüfungen normenklar regelt.

Anwendung, Umfang, Kreis der betroffenen Personen und die Datenverarbeitung sind auf das Erforderliche zu beschränken. Generell dürfen Zuverlässigkeitsüberprüfungen im Polizeirecht mit Blick auf die Aufgaben der Polizei (§ 1 Abs. 2 SPolG) nur dort eingesetzt werden, wo spezifische Situationen infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden. Korrespondierend müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, es dürfen auch nur hinreichend gewichtige Delikte in die Überprüfung einbezogen werden. Zudem müssen die Kriterien, die zur Annahme von Sicherheitsbedenken führen, einen konkreten Bezug zu den abzuwehrenden Gefahren haben.

Für die sonstigen derzeit in § 28 Abs. 3 SPolDVG-E bezeichneten Fälle sind Zuverlässigkeitsüberprüfungen zwar verfassungsrechtlich nicht von vornherein ausgeschlossen. Es bedarf zu ihrer Durchführung jedoch einer bereichsspezifischen Befugnis im jeweiligen Fachrecht, bspw. im Dienst- und Beamtenrecht, zugunsten der entsprechenden Fachbehörde. Gerade in den Fällen der Zuverlässigkeitsüberprüfung von Bediensteten / Mitarbeitern handelt es sich nämlich nicht um eine im Polizeirecht zu regelnde Maßnahme der Gefahrenabwehr - eine (konkrete) Gefahr liegt in diesen Fällen schlicht nicht vor. Die Beteiligung der Polizei an solchen Zuverlässigkeitsüberprüfungen ist dann allein im Wege der Amtshilfe zu realisieren.

6 Lückenhafter Schutz von Berufsgeheimnisträgern

[siehe insb. Formulierungsvorschlag 19, 20, 21]

Der Gesetzesentwurf sieht einen Schutz des Berufsgeheimnisses bei der Verarbeitung personenbezogener Daten durch die Polizei nur eingeschränkt vor. So statuiert § 41 Abs. 1 Satz 3 SPolDVG-E ein Erhebungsverbot in Bezug auf personenbezogene Daten, die einem Berufsgeheimnis unterliegen, nicht umfassend. In Verbindung mit § 41 Abs. 1 Satz 2 SPolDVG-E ist die Erhebung von Daten, die einem Berufsgeheimnis unterliegen nur dann ausgeschlossen, wenn Anhaltspunkte dafür bestehen, dass **ausschließlich** solche Erkenntnisse erfasst werden sollen. Mit anderen Worten darf bspw. die Telekommunikation zwischen Rechtsanwalt und Mandant bereits dann überwacht und aufgezeichnet werden (§ 35 SPolDVG-E i.V.m § 41 Abs. 1 Satz 2,3 SPolDVG-E), wenn im Rahmen des jeweiligen Telefonats auch über nicht-mandatsbezogene Dinge gesprochen werden soll.

Den verfassungsrechtlichen Vorgaben wird dies nicht gerecht. Eingriffe in das Vertrauensverhältnis bspw. von Rechtsanwälten zu ihren Mandanten sind absolut untersagt und bereits die Erhebung von Daten, die von einem Berufsgeheimnis umfasst sind, ist verfassungsrechtlich unzulässig. Dort, wo Berufsgeheimnisse in Rede stehen, muss schon die Datenerhebung ausgeschlossen werden, um einen effektiven Schutz zu gewährleisten.

Wir schlagen daher vor, zum Schutz von Berufsgeheimnisträgern eine dem § 39b POG Rheinland-Pfalz vergleichbare Regelung aufzunehmen.

7 Benachrichtigungspflichten

[siehe insb. Formulierungsvorschlag 4, 5, 6, 7]

Für problematisch halten wir die in § 10 SPolDVG-E geregelte Benachrichtigungspflicht.

Dies gilt zunächst für den Kreis der Benachrichtigungsempfänger. § 10 Abs. 5 Satz 1 SPolDVG-E sieht eine Regelbenachrichtigung nur für die Personen vor, gegen die sich eine verdeckte Maßnahme richtet. In Bezug auf andere von der Maßnahme (mit)betroffene Personen sieht das Gesetz eine Regelbenachrichtigung nur in den Fällen einer Wohnraumüberwachung vor und damit nur bei Personen, die sich im Zeitpunkt der Maßnahme ebenfalls in der Wohnung aufhielten und überwacht wurden.

Bei allen anderen verdeckten Ermittlungsmaßnahmen soll eine Benachrichtigung in Bezug auf andere (mit)betroffene Personen nur dann erfolgen, wenn besonders schutzwürdige Interessen dies erfordern. Dabei lassen das Gesetz und auch die Begründung offen, wann dies der Fall sein soll und auf wessen Interessen abzustellen ist. Die Vorschrift legt es damit weitgehend in die Hand der Ermittlungsbehörde, wann eine Benachrichtigung zu erfolgen hat. Daher ist die Vorschrift in Bezug auf (mit)betroffene Personen verfassungswidrig und europarechtswidrig. Sowohl die JIRL als auch das BVerfG fordern eine Regelbenachrichtigung aller von einer verdeckten Maßnahme betroffenen Personen und nicht nur derjenigen Personen, gegen die sich die Maßnahme gezielt richtet (Zielperson). Anknüpfungspunkt ist Art. 19 Abs. 4 GG, der nicht nur die Rechtsschutzinteressen der Ermittlungsadressaten schützt, sondern auch die anderer (mit)betroffener Personen. Praktikabilitätsprobleme, die sich bei der Benachrichtigung von anderen Personen als Zielpersonen stellen, können über § 10 Abs. 6 Nr. 2 SPolDVG-E in ausreichendem Maße abgefangen werden. Sinngemäß lässt das BVerfG eine Ausnahme von der grundsätzlichen Pflicht zur Benachrichtigung zu, wenn „*durch die Benachrichtigung von einer Maßnahme, die keine weiteren Folgen gehabt hat, der Grundrechtseingriff noch vertieft würde*." (BVerfG, Urteil 20. April 2016, 1 BvR 966/09, Rn. 136).

Der Kreis der Empfänger einer Regelbenachrichtigung sollte daher auf alle betroffenen Personen im Sinne von Art. 3 Nr. 1 JIRL erstreckt werden. Sinnvoll erscheint aus hiesiger Sicht zudem eine gesetzliche Benennung der

Kategorien von Benachrichtigungsempfängern für jede verdeckte Maßnahme, wie dies bspw. in § 50 BayPAG oder § 33 PolG NRW-E vorgesehen ist, um entsprechenden Rechtsunsicherheiten zu begegnen.

Unzureichend sind auch die Dokumentationspflichten und die Pflicht zur Einholung einer richterlichen Bestätigung beim befristeten oder endgültigen Unterlassen einer Benachrichtigung. Das BVerfG fordert in allen Fällen, in denen eine nachträgliche Benachrichtigung unterbleibt, eine richterliche Bestätigung. Es ist insoweit unzulässig, die richterliche Bestätigung nur in den Fällen der Zurückstellung nach § 10 Abs. 5 SPolDVG-E zu fordern. Erforderlich ist eine richterliche Bestätigung auch und gerade in den Fällen des endgültigen Absehens von einer Benachrichtigung nach § 10 Abs. 6 SPolDVG-E. Gleiches gilt für die Dokumentationspflicht.

Sinnvoller, weil systematisch korrekt, erscheint daher eine einheitliche Regelung des Verfahrens der richterlichen Bestätigung und der Dokumentationspflicht in einem eigenen Absatz, der für beide Fälle, der Zurückstellung der Benachrichtigung nach Abs. 5 und dem Absehen von einer Benachrichtigung nach Abs. 6, einheitliche Vorgaben macht.

8 Einbeziehung von Kontaktpersonen

[siehe insb. Formulierungsvorschlag 10]

§ 17 Abs. 2 Nr. 2 lit. c SPolDVG-E erweitert den Adressatenkreis polizeilicher Datenverarbeitungsbefugnisse auf Personen, die selbst in keiner Weise verantwortlich sind, wenn diese Personen mit einer verdächtigen Person nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und die verdächtige Person „*sich ihrer zur Begehung der Straftat bedienen könnte*". Dies umfasst erkennbar einen potentiell weiten Kreis von gutgläubigen Umfeldpersonen, gegen die selbst keinerlei Verdachtsmomente vorliegen. Das BVerfG hat die ähnliche, aber im Vergleich zu § 17 Abs. 2 Nr. 2 lit. c SPolDVG-E einschränkendere Regelung des damaligen § 20b Abs. 2 Nr. 2 BKAG nur im Zuge einer verfassungskonformen Reduktion hingenommen, indem es nämlich verlangte: „Freilich dürfen die Merkmale von Verfassungs wegen nicht entgrenzend weit verstanden werden." Voraussetzung ist danach, dass die „*Instrumentalisierung des Betroffenen in einem engen Konnex zur Tat selbst*" stehen muss. Die vorgeschlagene Regelung in § 17 Abs. 2 Nr. 2 lit. c SPolDVG-E bleibt aber selbst hinter diesen Vorgaben des BVerfG zum damaligen § 20b Abs. 2 Nr. 2 BKAG noch zurück und erlaubt eine weitgehend unbegrenzte Erfassung von undolosen Kontakt- und Begleitpersonen. Der Entwurf des SPolDVG trifft keine Vorkehrungen, um durch eine entsprechend enge Formulierung der Eingriffsermächtigung einer „*entgrenzenden*" Interpretation vorzubeugen.

9 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 7 Abs. 2 der JIRL. Danach hat der Mitgliedstaat angemessene Fristen

vorzusehen, nach deren Ablauf eine Überprüfung der Notwendigkeit der weiteren Speicherung personenbezogener Daten vorzunehmen ist. Zwar sieht der Entwurf in § 26 Abs. 2 Satz 2 SPolDVG-E entsprechende Aussonderungsprüffristen vor. 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 jedoch 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. 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 Bagatelldelikte zeitlebens mitgeführt wird. Eine Überprüfung nach „angemessenen Fristen" (Art. 5 JIRL) findet in diesen Fällen überhaupt nicht statt. Dies verstößt gegen Art. 5 JIRL und gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

10 Zugriff auf informationstechnische Systeme

[siehe insb. Formulierungsvorschlag 18]

§ 35 Abs. 2 SPolDVG-E erlaubt zur Ermöglichung der Aufzeichnung von Telekommunikation, bevor diese verschlüsselt wird, den Zugriff auf informationstechnische Systeme einer verdächtigen Person. Diese Zugriffe auf informationstechnische Systeme der Betroffenen stellen einen Eingriff in das Grundrecht auf 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 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 Vertraulichkeit und Integrität informationstechnischer Systeme folgt daher 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.

11 Einsatz von Körperkameras in Wohnungen

§ 32 Abs. 3 S. 2 SPolDVG-E regelt die rechtliche Zulässigkeit des Einsatzes von Körperkameras (Body-Cams) in Wohnungen. Die Vorschrift nimmt unmittelbaren Bezug auf § 32 Abs. 3 S. 1 SPolDVG-E – bislang § 27 Abs. 3

SPolG – und erweitert dessen Anwendungsbereich über den Einsatz in öffentlich zugänglichen Räumen hinaus. Auch in Wohnungen soll die Vollzugspolizei „(…)*zum Schutz der eingesetzten Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten"* in Zukunft Body-Cams einsetzen dürfen, wenn dies zur *„Abwehr einer dringenden Gefahr für Leib oder Leben erforderlich ist*.".

In polizei- und ordnungsrechtlicher Hinsicht betritt die in Bezug genommene Regelung weitgehend Neuland. Soweit ersichtlich, haben bislang lediglich die Bundesländer Nordrhein-Westfalen und Bayern den Einsatz von Körperkameras in Wohnungen kodifiziert (vgl. § 15c PolG NRW, Art. 33 Abs. 4 S. 3 BayPAG).

Aus hiesiger Sicht hält die Vorschrift einer verfassungsrechtlichen Prüfung nicht stand und scheidet daher aus datenschutzrechtlicher Sicht als Verarbeitungsgrundlage aus.

Die Regelung in § 32 Abs. 3 S. 1 u. 2 SPolDVG-E stellt einen Eingriff in das verfassungsrechtlich geschützte Recht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) dar, welcher nur durch die engen Schranken des Art. 13 Abs. 5 S. 1 GG gerechtfertigt werden kann. Diese Vorschrift erlaubt den Einsatz technischer Mittel in Wohnungen, sofern diese ausschließlich dem Schutz der Einsatzpersonen dienen.

Es ist in diesem Zusammenhang bereits fraglich, ob die Schranke des Art. 13 Abs. 5 S. 1 GG im Rahmen von Einsätzen durch uniformierte Polizeivollzugsbeamte überhaupt Anwendung findet. Aus der Normsetzungsgeschichte lässt sich entnehmen, dass das Hauptanliegen des verfassungsgebenden Gesetzgebers „(…) *ausschließlich die Eigensicherung der verdeckt ermittelnden Personen*" war. Diese restriktive Sichtweise des Anwendungsbereichs von Art. 13 Abs. 5 S. 1 GG erscheint folgerichtig, sind es doch gerade die nicht uniformierten Ermittlungspersonen, welche bei verdeckten Ermittlungen in besonderem Maße gefährdet sind. Es dürfte bei ihnen nicht der Regel entsprechen, dass sie mindestens in Begleitung einer weiteren Amtsperson Wohnungen betreten. In vielen Einsatzsituationen sind sie demnach auf sich gestellt und können die vor Ort fehlende Absicherung durch einen Kollegen/eine Kollegin nur durch eine technische Verbindung nach außen kompensieren, von wo aus im Ernstfall eingegriffen werden kann. Darüber hinaus profitieren sie gerade nicht von der „Autorität der Uniform". Sie treten dem/der Inhaber/in der Wohnung nicht als Organ der Staatsgewalt sondern als „gleichgestellte" Privatperson gegenüber, was die Hemmschwelle des Einsatzes von körperlicher Gewalt im Allgemeinen senken dürfte.

Es bestehen aus hiesiger Seite darüber hinaus erhebliche Bedenken an der Geeignetheit des Einsatzes von Körperkameras zu Zwecken des Personenschutzes. Im einschlägigen Schrifttum herrscht überwiegend Konsens dahingehend, dass Art. 13 Abs. 5 GG, welcher den Gefahrenbegriff nicht näher umschreibt, im Regelungszusammenhang mit Art. 13 Abs. 4 GG zu sehen ist, welcher als Eingriffsschwelle die Abwehr einer „(…) *dringenden Gefahr* (…)" erfordert. Der Begriff der dringenden Gefahr geht über den Begriff der konkreten Gefahr hinaus. Er nimmt sowohl Bezug auf das Ausmaß des Schadens, als auch auf dessen Wahrscheinlichkeit. Es muss sich um eine Gefahr für Leben, Leib und Freiheit der eingesetzten Person, d.h. zumindest um eine Körperverletzung von einigem Gewicht handeln. Dieser verfassungsrechtliche Maßstab an den Begriff der

dringenden Gefahr ist auch im Rahmen der einfachgesetzlichen Konkretisierung innerhalb des SPolDVG-E ungeschmälert anzuwenden.

Letzteren Vorgaben wird § 32 Abs. 3 S. 2 SPolDVG-E durch eine entsprechende Anwendung von § 34 Abs. 1 SPolDVG-E zwar formal gerecht, es ist indes fraglich, ob der bloße Einsatz von Körperkameras ein taugliches Mittel ist, einer solchen Gefahr zu begegnen. Die Körperkameras dienen gerade nicht dem Zweck einer Übertragung des Livebildes nach außen, etwa zu einer bereitstehenden Einsatzverstärkung, welche dann eingreifen kann, wenn es zu Gewalt gegen die sich in der Wohnung befindlichen Polizeibeamten kommt. Der Grund ihres Einsatzes basiert vielmehr ausschließlich auf einer vermuteten generalpräventiven Wirkung des Einsatzes von Körperkameras, welche jedoch nicht hinreichend belegt ist. Gerade bei gewaltbereiten, alkoholisierten oder unter Drogeneinfluss stehenden Personen, mithin bei demjenigen Personenkreis, vor welchem der Einsatz der Körperkameras die Polizeibeamten schützen soll, bestehen Bedenken, dass das Aggressionspotential die abschreckende Wirkung der Kameras überlagert.

Es erscheint vielmehr folgerichtig, im Fall der Annahme einer dringenden Gefahr für die eingesetzten Personen, den Einsatz von vornherein hierauf auszurichten. Dies dürfte in erster Linie durch die Einsatzplanung, die Anzahl der Einsatzkräfte und eine entsprechende Schutzausrüstung geschehen. Der Einsatz von Körperkameras erbringt aus hiesiger Sicht indes in einer solchen Situation für die Gefahrenabwehr keinen erkennbaren Mehrwert und kann demnach mangels entsprechender (Teil-)Geeignetheit den tiefgreifenden Grundrechtseingriff nicht rechtfertigen.

Mit freundlichen Grüßen

Monika Grethel
Die Landesbeauftragte für Datenschutz
und Informationsfreiheit im Saarland

Entwurf eines Gesetzes zur Neuregelung der polizeilichen Datenverarbeitung

Externe Anhörung

Stellungnahme zu Art. 2 – Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG-E)

Anmerkungen der Landesbeauftragten für Datenschutz
und Informationsfreiheit

Stand: 25. Oktober 2019

Erster Teil - Allgemeine Bestimmungen

Nr.	Norm	Gesetzentwurf MIBS	Formulierungs-/Änderungsvorschlag LfDI	Begründung
	§ 1 Anwendungsbereich			
1	§ 1 Abs. 1	Die Vorschriften dieses Gesetzes gelten für die Verarbeitung personenbezogener Daten durch die Polizei im Sinne des § 1 Absatz 1 des Saarländischen Polizeigesetzes in der Fassung der Bekanntmachung vom 26. März 2001 (Amtsbl. S. 1074), zuletzt geändert durch Artikel 1 des Gesetzes vom 15. März 2017 (Amtsbl. I S. 486), zum Zweck der Verhütung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung.	Die Vorschriften dieses Gesetzes gelten für die Verarbeitung personenbezogener Daten durch die Polizei im Sinne des § 1 Absatz 1 des Saarländischen Polizeigesetzes in der Fassung der Bekanntmachung vom 26. März 2001 (Amtsbl. S. 1074), zuletzt geändert durch Artikel 1 des Gesetzes vom 15. März 2017 (Amtsbl. I S. 486), zum Zweck der Verhütung, Ermittlung, Aufdeckung, Verfolgung und Ahndung von Straftaten oder Ordnungswidrigkeiten. Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den ~~, einschließlich des~~ Schutz~~es~~ vor und ~~der~~ die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung. Für Polizeiverwaltungsbehörden gelten die Vorschriften dieses Gesetzes, soweit sie Ordnungswidrigkeiten verfolgen, ahnden sowie Sanktionen vollstrecken.	Regelungsumfang der JI-Richtlinie (JIRL) ist lediglich die straftatenbezogene Gefahrenabwehr, nicht jedoch die allgemeine Gefahrenabwehr durch die Verwaltungspolizeibehörden bzw. Sonderordnungsbehörden. Der Formulierungsvorschlag übernimmt die Regelung aus § 35 Abs. 1 und 2 DSG NRW. Ebenso § 45 BDSG. Siehe ebenso Lisken/Denninger, 6. Auflage, G. Rn. 378.
	§ 6 Befugnisse der Aufsichtsbehörde			
2	§ 6 Abs. 2 Satz 1	Sofern die oder der Landesbeauftragte für Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Schutz personenbezogener Daten oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten festgestellt und beanstandet hat, kann sie oder er geeignete	Sofern die oder der Landesbeauftragte für Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Schutz personenbezogener Daten oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten festgestellt und beanstandet hat, kann sie oder er geeignete Maßnahmen anordnen, wenn dies	Siehe Begründung im Anschreiben.

		Maßnahmen anordnen, wenn dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist.	zur Beseitigung eines ~~erheblichen~~ Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist.	
3	§ 6 Abs. 2 Satz 2	Dabei kann sie oder er insbesondere 1. einen Verantwortlichen oder einen Auftragsverarbeiter warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen datenschutzrechtliche Vorschriften verstoßen, 2. den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung, 3. eine vorübergehende oder endgültige Beschränkung der Verarbeitung, ein-schließlich eines Verbots, verhängen.	Dabei kann sie oder er insbesondere 1. einen Verantwortlichen oder einen Auftragsverarbeiter warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen datenschutzrechtliche Vorschriften verstoßen, 2. den Verantwortlichen oder den Auftragsverarbeiter an~~zu~~weisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den ~~nach dieser Richtlinie erlassenen~~datenschutzrechtlichen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung, 3. eine vorübergehende oder endgültige Beschränkung der Verarbeitung, ein-schließlich eines Verbots, verhängen.	Redaktionelle Anpassungen.
	§ 10 Benachrichtigung der betroffenen Person			
4	§ 10 Abs. 3	Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an die Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst oder ist die Sicherheit eines Landes oder des Bundes berührt, ist sie nur mit Zustimmung der jeweils zuständigen Stellen zulässig.	Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an die Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst oder ist die Sicherheit eines Landes oder des Bundes berührt, ~~ist sie nur mit Zustimmung der jeweils zuständigen Stellen zulässig~~kann die Benachrichtigung insoweit unterbleiben, als die Polizei nach Anhörung der jeweils zuständigen Stelle feststellt, dass die	Die Zustimmungsbedürftigkeit der erscheint in dieser Form – als gebundene Entscheidung – europarechtswidrig, da sie zu einer Verschiebung der Verantwortlichkeiten führt, die nicht von der JIRL vorgesehen ist. Die genannten Stellen liegen sowohl außerhalb der Kontrollmechanismen der JIRL als auch der DSGVO und damit außerhalb des Schutzes, den diese Rechtsvorschriften und die zuständigen Aufsichtsbehörden den betroffenen Personen bieten sollen.

			Sicherheit eines Landes oder des Bundes berührt ist.	Zwar ist eine solche Einschränkung prinzipiell zulässig. Sie erfordert aber wenigstens die Überprüfung der Zustimmungsverweigerung durch den Verantwortlichen und die Aufsichtsbehörde.
5	§ 10 Abs. 4	Im Fall der Einschränkung nach Absatz 2 gilt § 11 Absatz 7 und 8 entsprechend.	Im Fall der Einschränkung nach Absatz 2 und 3 gilt § 11 Absatz 7 und 8 entsprechend.	Die Zustimmungsbedürftigkeit in § 10 Abs. 3 ist in dieser Form unzulässig, da die Verantwortlichkeit für die Benachrichtigung auf eine Stelle verlagert wird, die weder in den Anwendungsbereich der JIRL noch der DSGVO fällt und damit außerhalb des entsprechenden Schutzniveaus (siehe oben). Dies kann nur dadurch kompensiert werden, dass die nicht gegebene Zustimmung überprüft werden kann und keine gebundene Entscheidung darstellt. Der Formulierungsvorschlag ermöglicht eine Überprüfung der Ablehnung durch die Aufsichtsbehörde.
6	§ 10 Abs. 5	Personen, gegen die sich eine verdeckte Datenerhebung nach Maßgabe der § 31, §§ 34 bis 36 und § 40 richtet, sind nach Abschluss der Maßnahme hierüber zu unterrichten. Dabei ist die betroffene Person auch über die Tatsache der Erhebung, Speicherung und Löschung von personenbezogenen Daten aus dem Kernbereich der privaten Lebensgestaltung nach § 41 Absatz 3 zu unterrichten. Auf die Möglichkeit nachträglichen Rechtsschutzes ist hinzuweisen. Sonstige betroffene Personen sind nach Maßgabe der Sätze 1 bis 3 zu unterrichten, soweit eine Datenerhebung nach § 34 erfolgt ist oder andere besonders schutzwürdige Interessen dies erfordern. Die Unterrichtung nach den Sätzen 1 oder 4 kann zurückgestellt werden,	~~Personen, gegen die sich~~Im Falle einer verdeckten Datenerhebung ~~nach Maßgabe der § 31, §§ 34 bis 36 und § 40 richtet,~~ sind die betroffenen Personen nach Abschluss der Maßnahme hierüber zu ~~unterrichten~~benachrichtigen. Dabei ist die betroffene Person auch über die Tatsache der Erhebung, Speicherung und Löschung von personenbezogenen Daten aus dem Kernbereich der privaten Lebensgestaltung nach § 41 Absatz 3 zu unterrichten. Auf die Möglichkeit nachträglichen Rechtsschutzes ist hinzuweisen. ~~Sonstige betroffene Personen sind nach Maßgabe der Sätze 1 bis 3 zu unterrichten, soweit eine Datenerhebung nach § 34 erfolgt ist oder andere besonders schutzwürdige Interessen dies erfordern.~~ Die ~~Unterrichtung~~ Benachrichtigung ~~nach den Sätzen 1 oder 4~~	Siehe Begründung im Anschreiben. Sprachliche Vereinheitlichung der Vorschrift mit Blick auf die Normenüberschrift „Benachrichtigung“. Auch die Gesetzesbegründung spricht ausschließlich von der „Benachrichtigung“. Das BVerfG fordert in allen Fällen, in denen eine nachträgliche Benachrichtigung unterbleibt eine richterliche Bestätigung. Es ist insoweit unzulässig die richterliche Bestätigung nur in den Fällen der Zurückstellung nach Abs. 5 zu fordern. Erforderlich ist eine richterliche Bestätigung gerade auch in den Fällen des endgültigen Absehens von einer Benachrichtigung nach Abs. 6. Gleiches gilt für die Dokumentationspflicht. Sinnvoller, weil systematisch korrekt, erscheint daher eine einheitliche Regelung

		soweit Leib, Leben oder Freiheit einer Person, besondere Vermögenswerte oder der Zweck der Maßnahme gefährdet werden. Wird die Unterrichtung nach Satz 5 zurückgestellt, sind die Gründe aktenkundig zu machen. Erfolgt die Benachrichtigung nicht binnen zwölf Monate nach Beendigung der Maßnahme, bedürfen jegliche weiteren Zurückstellungen der gerichtlichen Zustimmung; zuständig ist das Gericht, welches die Maßnahme angeordnet hat. Bedurfte die Maßnahme nicht der richterlichen Anordnung, ist für die Zustimmung das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat, zuständig. Das Gericht bestimmt die Dauer weiterer Zurückstellungen. Es kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Zurückstellung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft weiter vorliegen werden. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 7 genannte Frist mit der Beendigung der letzten Maßnahme.	kann zurückgestellt werden, soweit Leib, Leben oder Freiheit einer Person, besondere Vermögenswerte oder der Zweck der Maßnahme gefährdet werden. ~~Wird die Unterrichtung nach Satz 5 zurückgestellt, sind die Gründe aktenkundig zu machen. Erfolgt die Benachrichtigung nicht binnen zwölf Monate nach Beendigung der Maßnahme, bedürfen jegliche weiteren Zurückstellungen der gerichtlichen Zustimmung; zuständig ist das Gericht, welches die Maßnahme angeordnet hat. Bedurfte die Maßnahme nicht der richterlichen Anordnung, ist für die Zustimmung das Amts-gericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat, zuständig. Das Gericht bestimmt die Dauer weiterer Zurückstellungen. Es kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Zurückstellung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft weiter vorliegen werden. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 7 genannte Frist mit der Beendigung der letzten Maßnahme.~~	des Verfahrens der richterlichen Bestätigung und der Dokumentationspflicht in einem neuen Abs. 7.
7	§ 10 Abs. 7 *(neu)*	---	Die Gründe für eine Zurückstellung nach Abs. 5 und für ein Absehen von einer Benachrichtigung nach Abs. 6 Nr. 2 und 3 sind aktenkundig zu machen. Erfolgt die Benachrichtigung nicht binnen zwölf Monate nach Beendigung der Maßnahme, bedürfen jegliche weiteren Zurückstellungen der gerichtlichen Zustimmung; zuständig ist das Gericht, welches die Maßnahme angeordnet hat. Bedurfte die	Nicht nur in den Fällen einer Rückstellung, sondern gerade auch in den Fällen des Abs. 6 Nr. 2 und 3 wird das Absehen auf Gründe gestützt, die im Nachhinein durch ein Gericht oder die Aufsichtsbehörde nachvollzogen werden müssen. Das endgültige Absehen nach Abs. 6 ist gegenüber der Rückstellung nach Abs. 5 zudem noch wesentlich eingriffsintensiver und bedarf daher erst recht den gleichen gesetzlichen Garantien wie die bloße zeitlich

			Maßnahme nicht der richterlichen Anordnung, ist für die Zustimmung das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat, zuständig. Das Gericht bestimmt die Dauer weiterer Zurückstellungen. Frühestens nach Ablauf von fünf Jahren, in den Fällen des Abs. 6 auch früher, kann das Gericht dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Zurückstellung nach Abs. 5 oder ein Absehen von einer Benachrichtigung nach Abs. 6 Nr. 2 und 3 mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft weiter vorliegen werden. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 7 genannte Frist mit der Beendigung der letzten Maßnahme.	begrenzte Zurückstellung. (siehe auch die Begründung zu § 10 Abs. 5, oben) Das BVerfG hält ein endgültiges Absehen von einer Benachrichtigung nach frühestens 5 Jahren für zulässig (BVerfG, Urteil 20. April 2016, 1 BvR 966/09, Rn. 262).
	§ 11 Auskunftsrecht der betroffenen Person			
8	§ 11 Abs. 2	Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.	~~Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.~~	Die Regelung setzt Art. 15 Abs. 1 JIRL um. Gleichwohl lässt sie sich nicht auf einen der in Art. 15 Abs. 1 lit. a bis lit. e JIRL genannten Zwecke stützen. Sie ist daher nicht richtlinienkonform ausgestaltet.

9	§ 11 Abs. 3	Von der Auskunftserteilung kann abgesehen werden, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.	Von der Auskunftserteilung kann abgesehen werden, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, obwohl ihr das möglich und zumutbar wäre, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand, insbesondere bei nicht-automatisierten Verfahren, außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.	Die Auskunftserteilung dient ja gerade dazu, zu erfahren, ob und in welchem Umfang überhaupt personenbezogene Daten verarbeitet werden. Im Regelfall wird der Betroffene daher überhaupt keine Angaben hierzu machen können. Deutlich wird dies am Beispiel der Negativauskunft, die unzweifelhaft von Art. 14 JIRL umfasst ist. Würde man das Recht auf Auskunft so verstehen, dass der Betroffene bereits Kenntnis darüber haben muss, dass zu seiner Person bezogene Daten verarbeitet werden und er die Auskunft nur noch dazu nutzen möchte zu erfahren, was konkret über ihn gespeichert ist, verbliebe für die Fälle der Negativauskunft kein Raum. Art. 15 Abs. 1 JIRL enthält zudem eine abschließende Liste von Zwecken, die eine Einschränkung des Auskunftsrechts rechtfertigen können. Eine Auffinde- und Rechercheaufwand gehört nicht dazu. Die Entwurfsvorschrift bleibt noch hinter dem derzeitigen § 40 SPolG zurück.
	§ 17 Kategorien betroffener Personen			
10	§ 17 Abs. 2 Nr. 2	(…) Personen, die mit einer der in Nummer 1 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und (…) c) die Person nach Nummer 1 sich ihrer zur Begehung der Straftat bedienen könnte,	(…) Personen, bei denen Anhaltspunkte bestehen, dass ~~die~~ sie mit einer der in Nummer 1 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und bei denen zu erwarten ist, dass Hinweise für die Verfolgung oder vorbeugende Bekämpfung dieser Straftaten gewonnen werden können, weil sie (…) c) ~~die Person nach Nummer 1 sich ihrer zur Begehung der Straftat bedienen könnte~~an der Planung und Vorbereitung der Straftat mitwirken,	Die Einschränkung soll einer Entgrenzung Betroffenenkreis im Sinne der vom BVerfG geforderten engen Interpretation entgegenwirken und orientiert sich an § 19 Abs. 1 BKAG.

	§ 18 Erhebung personenbezogener Daten			
11	§ 18 Abs. 2	Die Vollzugspolizei darf personenbezogene Daten über die in § 17 Absatz 2 Nummer 1 bis Nummer 4 genannten Personen erheben, soweit dies erfahrungsgemäß zur vorbeugenden Bekämpfung von Straftaten erforderlich ist.	Die Vollzugspolizei darf personenbezogene Daten über die in § 17 Absatz 2 Nummer 1 bis Nummer 4 genannten Personen erheben, soweit dies erfahrungsgemäß zur vorbeugenden Bekämpfung von Straftaten erforderlich ist und die §§ 28 bis 41 Erhebungsbefugnisse der Polizei nicht besonders regeln.	Die Ergänzung soll Funktion und Charakter der Auffangvorschrift deutlicher zum Ausdruck bringen und damit für Rechtsklarheit sorgen.

Zweiter Teil - Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Nr.	Norm	Gesetzentwurf MIBS	Formulierungs-/Änderungsvorschlag LfDI	Begründung
	§ 20 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten			
12	§ 20 Abs. 1 Nr. 1	Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des § 2 Absatz 15 ist nur zulässig, wenn dies zur Aufgabenerfüllung unbedingt erforderlich ist und 1. nach geltendem Recht zulässig ist, 2. (…)	Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des § 2 Absatz 15 ist nur zulässig, wenn dies zur Aufgabenerfüllung unbedingt erforderlich ist und 1. ~~nach geltendem Recht zulässig ist~~auf Grund gesetzlicher Vorschriften ausdrücklich vorgesehen ist, 2. (…)	Die Ermächtigungsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten genügt nicht den Vorgaben der Richtlinie. Diese verlangt in den Fällen des Art. 10 lit. a eine Konkretisierung der Verarbeitungssituationen. Nicht ausreichend ist es den Wortlaut der Art. 10 JIRL einfach zu wiederholen. EG 37 verlangt, dass der Gesetzgeber seinem Regelungsauftrag durch in *„Rechtsvorschriften geregelten Fällen“* nachkommt. Dies folgt mit Blick auf die Eingriffsintensität bei der Verarbeitung besonderer Kategorien personenbezogener Daten aus den verfassungsrechtlichen Grundsätzen der Normenklarheit und Normenbestimmtheit.
	§ 21 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten			
13	§ 21 Abs. 1 Satz 3	Die Verwendung einschließlich ihrer erneuten Speicherung und einer Veränderung zu einem anderen polizeilichen Zweck durch die Polizeiverwaltungsbehörden ist jedoch zulässig, soweit die Polizeiverwaltungsbehörden die personenbezogene Daten zu diesem Zweck erheben dürften. Die Vollzugspolizei kann personenbezogene Daten nur unter den Voraussetzungen des § 23 zu anderen Zwecken verarbeiten.	~~Die Verwendung einschließlich ihrer erneuten Speicherung und einer Veränderung zu einem anderen polizeilichen Zweck durch die Polizeiverwaltungsbehörden ist jedoch zulässig, soweit die Polizeiverwaltungsbehörden die personenbezogen Daten zu diesem Zweck erheben dürften.~~ Die ~~Vollzugspolizei~~ Polizei kann personenbezogene Daten nur unter den Voraussetzungen des § 23 zu anderen Zwecken verarbeiten.	Es ist nicht nachvollziehbar, dass die Vorgaben für eine Zweckänderung bei den Polizeiverwaltungsbehörden anders ausgestaltet werden als bei der Vollzugspolizei.

	§ 26 Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten			
14	§ 26 Abs. 3 Nr. 4	Löschung und Vernichtung unterbleiben, wenn (…) 4. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.	Löschung und Vernichtung unterbleiben, wenn (…) ~~4. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist~~.	Die Richtlinie sieht in Art. 16 Abs. 3 eine solche Ausnahme nicht vor. Zudem sollen IT-Systeme so gestaltet werden, dass Löschbegehren problemlos umgesetzt werden können. Die Vorschrift setzt daher auch falsche Anreize bei der Auswahl und Gestaltung von IT-Systemen.
	§ 27 Protokolldaten, Protokollierung verdeckter oder eingriffsintensiver Maßnahmen			
15	§ 27 Abs. 2 Satz 2	Darüber hinaus dürfen die protokollierten Daten für die Überprüfung der Rechtmäßigkeit der Verarbeitung, der Eigenüberwachung, für die Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für die Abwehr dringender Gefahren oder für die Verfolgung von Straftaten verwendet werden.	Darüber hinaus dürfen die protokollierten Daten nur für die Überprüfung der Rechtmäßigkeit der Verarbeitung, der Eigenüberwachung, für die Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten verwendet werden, ~~sowie für die Abwehr dringender Gefahren oder für die Verfolgung von Straftaten~~es sei denn, es liegen Anhaltspunkte dafür vor, daß ohne ihre Verwendung die Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person aussichtslos oder wesentlich erschwert wäre. ~~verwendet werden.~~	Die Vorschrift setzt Art. 25 Abs. 2 JIRL um. Diese erlaubt eine Verwendung der Protokolldaten hingegen „ausschließlich“ zu den dort genannten Zwecken. Eine zweckändernde Verarbeitung für die Abwehr dringender Gefahren entspricht nicht den Richtlinienvorgaben und ist daher europarechtswidrig. Die Vorschrift ist zudem unverhältnismäßig, da sie eine Zweckänderung von Protokolldaten zur Verfolgung jeglicher Straftaten erlaubt. Dies wird der Sensibilität der Protokolldaten nicht gerecht. Diese könnten zur Verhaltens- und Leistungskontrolle gegenüber den abrufenden Beamten verwendet werden (z.B. Nachweis Arbeitszeitbetrug). Zudem können über die Auswertung von Protokolkdaten Löschfristen umgangen werden. Ihre Verwendung über die Zwecke der Kontrolle ist eng zu begrenzen.

	§ 28 Abgleich personenbezogener Daten, Zuverlässigkeitsüberprüfung			
16	§ 28 Abs. 1	Die Vollzugspolizei kann personenbezogene Daten der in den §§ 4, 5 des Saarländischen Polizeigesetzes sowie in § 17 Absatz 2 Nummer 1 und 2 dieses Gesetzes genannten Personen mit zu polizeilichen Zwecken gespeicherten personenbezogenen Daten abgleichen. Personenbezogene Daten anderer Personen kann die Vollzugspolizei abgleichen, wenn das auf Grund tatsächlicher Anhaltspunkte zur Erfüllung polizeilicher Aufgaben erforderlich erscheint. Die Vollzugspolizei kann ferner im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen. Ein Abgleich der gemäß § 17 Absatz 1 Nummer 5 bis 8 erlangten personenbezogenen Daten ist nur mit Zustimmung der betroffenen Person zulässig.	Die Vollzugspolizei kann personenbezogene Daten der in den §§ 4, 5 des Saarländischen Polizeigesetzes sowie in § 17 Absatz 2 Nummer 1 und 2 dieses Gesetzes genannten Personen mit ~~zu polizeilichen Zwecken gespeicherten personenbezogenen Daten~~dem Inhalt polizeilicher Dateien im Rahmen der Zweckbindung dieser Dateien abgleichen, soweit dies zur Durchführung einer konkreten polizeilichen Maßnahme erforderlich. Personenbezogene Daten anderer Personen kann die Vollzugspolizei nach Satz 1 abgleichen, wenn das auf Grund tatsächlicher Anhaltspunkte zur Erfüllung polizeilicher Aufgaben erforderlich erscheint. Die Vollzugspolizei kann ferner soweit dies im Rahmen der Wahrnehmung polizeilicher Aufgaben erforderlich ist, ~~im Rahmen ihrer Aufgabenerfüllung erlangte~~ personenbezogene Daten mit dem Fahndungsbestand abgleichen. Ein Abgleich ~~der gemäß~~mit Daten über Personen im Sinne des § 17 Absatz 1 Nummer 5 bis 8 ~~erlangten personenbezogenen Daten~~ ist nur mit ~~Zustimmung~~ Einwilligung der betroffenen Person zulässig.	In der vorgesehenen 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. Die Vorschrift des § 28 SPolDVG-E bedarf daher aus verfassungsrechtlicher Sicht einer Festlegung von Zweckvorgaben und Eingriffsschwellen. Insbesondere bedarf es einer Orientierung am Erforderlichkeitsgrundsatz um eine am Einzelfall orientierte verfassungskonforme Normanwendung gewährleisten zu können. Satz 4 beinhaltet den Vorschlag einer redaktionellen Änderung.

Dritter Teil – Besondere Befugnisse zur Verarbeitung personenbezogener Daten

Nr.	Norm	Gesetzentwurf MIBS	Formulierungs-/Änderungsvorschlag LfDI	Begründung
	§ 32 Bild- und Tonaufzeichnungen			
17	§ 32 Abs. 2 Satz 3 *(neu)*	Auf Maßnahmen nach Satz 1 ist durch Schilder oder in sonstiger geeigneter Form hinzuweisen. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.	Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Fest installierte Anlagen sind alle zwei Jahre daraufhin zu überprüfen, ob die Voraussetzungen für ihren Betrieb weiterhin vorliegen.	Gerade bei fest installierten Videoüberwachungsmaßnahmen an kriminogenen Örtlichkeiten besteht die Möglichkeit, dass sich bspw. etablierte Drogenmilieus auf andere nicht-überwachte Bereiche des Stadtgebiets verlagern. Es bedarf daher in regelmäßigen Abständen einer Überprüfung, ob die Voraussetzungen des § 32 Abs. 2 SPolDVG-E noch fortbestehen.
	§ 35 Überwachung und Aufzeichnung der Telekommunikation			
18	§ 35 Abs. 2 Nr. 3	Die eingesetzten technischen Mittel sind nach dem Stand der Technik gegen unbefugte Verwendung zu schützen.	Die eingesetzten technischen Mittel sind nach dem Stand der Technik gegen unbefugte Verwendung zu schützen. Erfolgt der Einsatz technischer Mittel unter Ausnutzung von Sicherheitslücken in der Hard- und Software des informationstechnischen Systems, so dürfen nur solche Sicherheitslücken verwendet werden, die dem jeweiligen Hersteller bereits bekannt sind.	Siehe Begründung im Anschreiben.
	§ 41 Schutz des Kernbereichs privater Lebensgestaltung			
19	§ 41 Abs. 1 Satz 3	Der Kernbereich privater Lebensgestaltung umfasst auch das Berufsgeheimnis des in den §§ 53, 53a der Strafprozessordnung genannten Personenkreises.	~~Der Kernbereich privater Lebensgestaltung umfasst auch das Berufsgeheimnis des in den §§ 53, 53a der Strafprozessordnung genannten Personenkreises.~~	Siehe Begründung im Anschreiben

	§ 41a Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger			
20	§ 41a Abs. 1 *(neu)*	---	Verdeckte Datenerhebungen in einem durch ein Berufsgeheimnis geschützten Vertrauensverhältnis im Sinne des § 53 Abs. 1 und des § 53 a Abs. 1 der Strafprozessordnung sind unzulässig. Dennoch erlangte Daten sind unverzüglich zu löschen. Erkenntnisse hierüber dürfen nicht verwertet werden. Die Tatsache der Datenerhebung ist zu dokumentieren.	Siehe Begründung im Anschreiben
21	§ 41a Abs. 2 *(neu)*	---	Absatz 1 gilt nicht, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person für die Gefahr verantwortlich ist.	Siehe Begründung im Anschreiben

Fünfter Teil – Besondere Regelungen für die Verarbeitung personenbezogener Daten und die Auftragsverarbeitung

Nr.	Norm	Gesetzentwurf MIBS	Formulierungs-/Änderungsvorschlag LfDI	Begründung
	§ 54 Durchführung einer Datenschutz-Folgenabschätzung			
22	§ 54 Abs. 1 Satz 1	Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person zur Folge, ist vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffene Person durchzuführen.	Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ~~eine erhebliche Gefahr~~ein hohes Risiko für die ~~Rechtsgüter~~ Rechte und Freiheiten der betroffenen Person zur Folge, ist vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffene Person durchzuführen.	Die Vorschrift setzt Art. 27 JIRL um, die an entsprechender Stelle von einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen spricht. Die unterschiedlichen Formulierungen führen zu erheblichen Rechtsunsicherheiten. Die Begriffe des Risikos und der Gefahr weisen einen unterschiedlichen Bedeutungsgehalt auf. Risiko ist als Kategorie niedriger als die Gefahr einzustufen und meint die nicht sichere Eintrittswahrscheinlichkeit von Schäden.
	§ 58 Anhörung der oder des Landesbeauftragten für Datenschutz			
23	§ 58 Abs. 1 Satz 1	Vor dem erstmaligen Einsatz neuer Dateisysteme oder neuer Verfahren oder der wesentlichen Änderung bestehender Verfahren ist die oder der Landesbeauftragte für Datenschutz anzuhören, wenn 1. aus einer Datenschutz-Folgenabschätzung nach § 54 hervorgeht, dass die Verarbeitung eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person zur Folge hätte, wenn der Verantwortliche keine Abhilfemaßnahmen treffen würde, oder 2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person zur Folge hat. (…)	Vor dem erstmaligen Einsatz neuer Dateisysteme oder neuer Verfahren oder der wesentlichen Änderung bestehender Verfahren ist die oder der Landesbeauftragte für Datenschutz anzuhören, wenn 1. aus einer Datenschutz-Folgenabschätzung nach § 54 hervorgeht, dass die Verarbeitung ~~eine erhebliche Gefahr~~ein hohes Risiko für die ~~Rechtsgüter~~ Rechte und Freiheit der betroffenen Person zur Folge hätte, wenn der Verantwortliche keine Abhilfemaßnahmen treffen würde, oder 2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ~~eine erhebliche Gefahr~~ein hohes Risiko für die ~~Rechtsgüter~~	Zur Unterscheidung der Begrifflichkeit Risiko / Gefahr siehe Begründung zu § 54, oben.

			Rechte und Freiheiten der betroffenen Person zur Folge hat. (…)	
	§ 61 Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Landesbeauftragten für Datenschutz			
24	§ 61 Abs. 1 Satz 1	Die jeweilige Polizeibehörde hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihr bekannt geworden ist, der oder dem Landesbeauftragten für Datenschutz zu melden, es sei denn, dass die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen mit sich gebracht hat.	Die jeweilige Polizeibehörde hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihr bekannt geworden ist, der oder dem Landesbeauftragten für Datenschutz zu melden, es sei denn, dass die Verletzung voraussichtlich ~~keine Gefahr~~nicht zu einem Risiko für die ~~Rechtsgüter~~Rechte und Freiheiten natürlicher Personen mit sich ~~gebracht hat~~führt.	Die Vorschrift setzt Art. 30 Abs. 1 JIRL um. Danach kann von einer Benachrichtigung an die Aufsichtsbehörde abgesehen werden, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Es handelt sich hierbei um eine Zukunftsprognose, die die Polizei stellen muss. Der Wortlaut des Gesetzentwurfs berücksichtigt dies nicht, indem nur auf die Vergangenheit abgestellt wird („geführt hat“). Zur Unterscheidung der Begrifflichkeit Risiko / Gefahr siehe Begründung zu § 54, oben.
	§ 62 Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten			
25	§ 62 Abs. 1 Satz 1	Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine erhebliche Gefahr für Rechtsgüter betroffener Personen zur Folge, sind diese unverzüglich über den Vorfall zu benachrichtigen.	Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ~~eine erhebliche Gefahr~~ein hohes Risiko für ~~Rechtsgüter~~ die Rechte und Freiheiten betroffener Personen zur Folge, sind diese unverzüglich über den Vorfall zu benachrichtigen.	Zur Unterscheidung der Begrifflichkeit Risiko / Gefahr siehe Begründung zu § 54, oben.