LANDTAG
Rheinland-Pfalz
17/6958
VORLAGE

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Stellungnahme

zum

Entwurf eines Landesgesetzes zur Änderung des Polizei- und Ordnungsbehördengesetzes (POG-E) sowie beamtenrechtlicher Vorschriften
Gesetzentwurf der Landesregierung
Drucksache 17/12072

im Rahmen der Anhörung des Innenausschusses des Landtags Rheinland-Pfalz am 19. August 2020.

1. Vorbemerkung

Der Gesetzentwurf zur Änderung des Polizei- und Ordnungsbehördengesetzes sowie beamtenrechtlicher Vorschriften hat zum Ziel, die Vorgaben der Richtlinie (EU) 2016/680 auf fachspezifischer Ebene umzusetzen und dient – wie bereits das Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 30. Juni 2017 (GVBl. S. 123) – der Verwirklichung der Vorgaben des Urteils des Bundesverfassungsgerichts (BVerfG) zum Bundeskriminalamtgesetz (BKAG) vom 20. April 2016 (BVerfGE 141, 220).

Aus datenschutzrechtlicher Sicht relevant sind zudem die geschaffenen Rechtsgrundlagen für die Zuverlässigkeitsüberprüfungen zum Schutz der Polizei sowie staatlicher und besonders gefährdeter privater Veranstaltungen (§§ 67 und 68 POG-E).

Angesichts der Vielzahl umfangreicher Neuerungen im Gesetzentwurf, beschränkt sich der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) auf wesentliche kritik- bzw. erörterungswürdige Punkte des Gesetzentwurfs.

2. Einordnung des Gesetzentwurfes

2.1. Ziele des Gesetzentwurfes

Bis zum 6. Mai 2018 war es den Mitgliedsstaaten der Europäischen Union aufgetragen, die Richtlinie (EU) 2016/680 umzusetzen. Das Land Rheinland-Pfalz wurde dem Umsetzungsauftrag zunächst durch die Schaffung des Teils 3 des Landesdatenschutzgesetzes (LDSG) gerecht. Dieser ist auf wesentliche datenschutzrechtliche Kernbereiche, insbesondere Betroffenenrechte, in Verbindung mit dem Polizei- und Ordnungsbehördengesetz anwendbar.

Die Datenverarbeitung durch die Polizei- und Ordnungsbehörden erfolgt sowohl im Rahmen der Zwecke, die den Anwendungsbereich der Richtlinie determinieren als auch zu Zwecken, die unter den Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) fallen. Sowohl inhaltlich als auch strukturell gelingt auf einer abstrakten Ebene die Abgrenzung beider Anwendungsberei-

che. Insbesondere der Anwendungsvorrang der Datenschutz-Grundverordnung wird zutreffend durch § 1 a im Rahmen des "Geltungsbereichs des Gesetzes" festgestellt. In der zugehörigen Gesetzesbegründung ist es zudem gelungen, den Anwendungsbereich der Richtlinie (EU) 2016/680 zum Anwendungsbereich der Datenschutz-Grundverordnung im Rahmen der Gesetzgebungskompetenz des Landes trennscharf abzugrenzen. Das Ordnungswidrigkeitenrecht als Bundesrecht stellt allerdings weitere Anforderungen an die Abgrenzung.

2.2. Gestaltungsspielraum des Gesetzgebers

Der vorliegende Entwurf unterscheidet sich erheblich von dem ursprünglichen Entwurf aus dem Jahr 2019, zu dem der LfDI im Rahmen des Beteiligungs- und Anhörungsverfahrens gem. §§ 27, 28 der Gemeinsamen Geschäftsordnung (GGO) in dem vergangenen Jahr Stellung genommen hat. Einer Reihe von Bedenken und Änderungsvorschlägen, die in der Stellungnahme des LfDI geäußert wurden, wurde dankenswerter Weise Rechnung getragen. Diese betrafen insbesondere die Verarbeitung besonderer Kategorien personenbezogener Daten, die Gewährleistung von Betroffenenrechten und die Ausgestaltungen der Verarbeitungsgrundlagen, insbesondere der Speicherungs- und Übermittlungsgrundlagen sowie die Anforderungen an die Protokollierungen von Verarbeitungen und Kennzeichnung von Daten. Damit wurden die Bedenken des LfDI zu großen Teilen ausgeräumt.

Mit Nachdruck zu befürworten ist die Zurückhaltung des Gesetzgebers, verfassungsrechtlich problematische, insbesondere eingriffsintensive Instrumente oder in ihrer Tragweite ungeklärte Begriffe wie die sog. „drohende Gefahr“ in das Gesetz aufzunehmen. Das Land Rheinland-Pfalz verfolgt das Ziel, die Polizeibehörden mit angemessenen gesetzlichen Regelungen und Befugnissen in die Lage zu versetzen, ihre Aufgaben effektiv zu erfüllen. Zur Erfüllung dieses Ziels wurden die Polizeibehörden bereits durch die vergangenen Novellierungen des Polizei- und Ordnungsbehördengesetzes mit weitreichenden Befugnissen ausgestattet, die aufgrund ihrer verfassungsrechtlich gebotenen und teils restriktiven Ausgestaltung dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit Rechnung tragen. Dies zeigte jüngst eindrucksvoll die Entscheidung des Bundesverfassungsgerichts in Bezug auf die Rechtsgrundlagen zum Abruf und zur Übermittlung von Bestandsdaten (Beschluss des Bundesverfassungsgerichts zur Bestandsdatenauskunft vom 27. Mai 2020; Az. 1 BvR 1873/13, 1 BvR 2618/13). Den Anforderungen des Bundesverfassungsgerichts hält die Regelung des § 31 f POG bzw. des § 42 POG-E im Gegensatz zu den in der Entscheidung gegenständlichen Bundesgesetzen stand.

Auch in der vorliegenden Novellierung verzichtet der Gesetzgeber darauf, auf jeweils aktuelle Bedrohungslagen vorschnell und überzeichnet zu reagieren und Befugnisse der Polizei- und Ordnungsbehörden über das gebotene Maß hinaus zu erweitern. Sowohl die gesetzliche Regelung einer elektronischen Aufenthaltsüberwachung als auch Erweiterungen der DNA-Analyse, um die – verfassungsrechtlich bedenkliche – Analyse zur Feststellung des Geschlechts, der Augen-, Haar- und Hautfarbe, des biologischen Alters und der biogeographischen Herkunft des Spurenverursachers zu bestimmen, wie sie in anderen Ländern vorgenommen wurden, wurden nicht geschaffen. Des Weiteren wurden die umfassenden Videoüberwachungsbefugnisse nicht um eine Möglichkeit der Nutzung biometrischer Gesichtserkennungsverfahren erweitert.

Bereits bestehende Eingriffsbefugnisse wurden zudem nicht verschärft. Zwar wurde im Rahmen des Beteiligungsverfahrens vorgeschlagen, den Einsatz der Bodycams innerhalb von Wohnungen zuzulassen und die Prerecording-Funktion zu erlauben. Diesen Vorschlägen wurde berechtigterweise und mit zutreffender Begründung (S. 86 der Gesetzesbegründung) nicht entsprochen, denn diese Erweiterungen der Befugnis stehen im Konflikt zu Art. 13 Grundgesetz (GG) und der Rechtsprechung des Bundesverfassungsgerichts zur rechtmäßigen Ausgestaltung von Datenverarbeitungsbefugnissen. In diesem Zusammenhang wird zudem darauf hingewiesen, dass gegen derart ausgestaltete Rechtsgrundlagen in Bayern und in Nordrhein-Westfalen Verfassungsbeschwerden beim Bundesverfassungsgericht anhängig sind.

Auch die Bedenken des Gesetzgebers gegen die Forderungen einzelner Verbände die Befugnisse des kommunalen Vollzugsdienstes zu stärken und diesen stärker auszurüsten, z.B. durch Bodycams, werden geteilt. Neben den in der Gesetzesbegründung angeführten Argumenten, dass die Ermächtigung zu sensiblen (und auch eingriffsintensiven) Grundrechtseingriffen, wie sie mit dem Einsatz von Bodycams verbunden sind, den entsprechend ausgebildeten und sensibilisierten Polizeikräften vorbehalten bleiben sollten, spricht gegen die Erweiterung der Befugnis zur Nutzung der Bodycams zudem, dass deren Nutzung und insbesondere der Zugriff und die Verwertung der Aufnahmen, die durch den Einsatz gewonnen wurden, von einem differenzierten Nutzungs- und Berechtigungskonzept flankiert sein muss, welches bestimmte technische Voraussetzungen und Ressourcen seitens der Polizeidienststellen voraussetzt. Dieses dezidierte technisch-organisatorische Regime trägt der Intensität des Eingriffs zur Erhebung der Daten Rechnung. Auch bei den Kommunen müsste diese Infrastruktur eingerichtet werden, was mit erheblichen Kosten und auch Ressourcen verbunden ist. Diese Tragweite wird nach hiesiger Auffassung in der rechtspolitischen Diskussion (auch aus aktuellem Anlass des Aufgabenzuwachses der Ordnungsbehörden in Zeiten der Pandemie) nicht ausreichend bedacht.

Die anhand dieser gesetzgeberischen Entscheidungen verfolgte Grundlinie des Gesetzgebers verdient aus hiesiger Sicht Zustimmung, weil sie die Gewährleistung von Sicherheit ermöglicht, ohne die Sicherung von Freiheit unangemessen zu verkürzen. Weit überwiegend halten sich die Regelungen des vorliegenden Gesetzentwurfes in diesem Rahmen.

3. Einzelfragen

3.1. Informationspflichten

Die in Art. 13 Richtlinie (EU) 2016/680 verorteten Informationspflichten werden in dem Gesetzentwurf nicht in einer gesonderten Vorschrift zusammenfassend geregelt, sondern in dem § 28 POG-E zu den Grundsätzen der Datenerhebung. Begrüßenswert ist die Tatsache, dass neben den allgemeinen Informationen, die in allgemeiner jedermann zugänglicher Form erbracht werden (§ 28 Abs. 2 S. 2 POG-E), auf Verlangen auch über weitere Informationen, wie die Rechtsgrundlage, unterrichtet wird. Damit trägt der Landesgesetzgeber dem Umsetzungsauftrag Rechnung, dass in "besonderen Fällen" weitergehende Informationen zu erbringen sind.

Es ist an dieser Stelle hervorzuheben, dass auch die offene Datenerhebung unter diese besonderen Fälle gefasst wird und damit speziellere – die konkrete Datenverarbeitung betreffende und determinierende – Informationen nicht nur den Adressaten verdeckter Maßnahmen vorbehalten blei-

ben. Insoweit ist es schlüssig, dass neben der Rechtsgrundlage der Erhebung und gegebenenfalls der weiteren Verarbeitung, über die voraussichtliche Dauer der Datenspeicherung oder, falls dies nicht möglich ist, über die Kriterien für die Festlegung der Dauer sowie gegebenenfalls über die Kategorien der Empfänger der Daten informiert wird. Durch Zurverfügungstellung dieser Informationen kann eine Transparenz geschaffen werden, die die betroffenen Personen in die Lage versetzt zu beurteilen, wer ihre personenbezogenen Daten wie und für welche Dauer verarbeitet. Insbesondere die Weiterverarbeitung der personenbezogenen Daten in Form der Speicherung in polizeilichen Informationssystemen und Dateien wird so der betroffenen Person offengelegt. Vielfach ist es den betroffenen Personen nicht bewusst, dass nach bspw. einer Datenerhebung im Rahmen einer (offenen) Identitätsfeststellung die personenbezogenen Daten zu einem Vorgang gespeichert werden oder ein Vorgang erstellt wird. Auch wenn die grundlegende Datenerhebung offen erfolgt, ist die weitere Verarbeitung damit nicht transparent, ohne dass die betroffene Person darüber informiert wird.

Bezüglich der Regelung des § 28 Abs. 3 S. 6 POG-E wird auf die Ausführungen und auf den Regelungsvorschlag unter Abschnitt 3.6. verwiesen.

3.2. Einwilligung als Datenerhebungsbefugnis personenbezogener Daten

Die Einwilligung als Rechtsgrundlage zur Datenerhebung wird im Rahmen der allgemeinen Datenerhebungsbefugnis (§ 29 Abs. 1 Ziff. 1 POG-E) geregelt.

Diese Regelungstechnik steht grundsätzlich im Widerspruch zu den Wertungen des Datenschutzrechts.

Die Einwilligung stellt nur dann eine taugliche Rechtsgrundlage zur Datenverarbeitung dar, wenn sie freiwillig erfolgt. Von einer Freiwilligkeit ist immer nur dann auszugehen, wenn die betroffene Person eine echte Wahlmöglichkeit hat und die Einwilligung abseits von Zwang geben kann.

Dieser Aspekt wird auch im Rahmen der Erwägungsgründe der Richtlinie (EU) 2016/680 aufgegriffen. Erwägungsgrund 35 stellt insoweit klar, dass bei einem hoheitlichen Agieren der betreffenden Behörden als Verantwortliche im Rahmen der Wahrnehmung der Aufgabe, Straftaten zu verhüten, zu ermitteln, aufzudecken und zu verfolgen, die Verantwortlichen die betroffenen Personen auffordern und anweisen können, Anordnungen zu befolgen. In diesen Situationen bleibt für die Einwilligung als Rechtsgrundlage kein Raum. Entsprechend wird sie auch nicht – anders als in Art. 6 Abs. 1 DS-GVO – in Art. 8 Richtlinie (EU) 2016/680 explizit als Rechtsgrundlage aufgezählt.

Das Polizei- und Ordnungsbehördengesetz in seiner aktuellen und auch in der künftigen Fassung stattet die Polizei- und Ordnungsbehörden bereits mit weitreichenden Datenverarbeitungsbefugnissen aus. In diesem Zusammenhang ist fraglich, für welche Verarbeitungssituationen ein Anwendungsbereich der Einwilligung verbleibt. In jedem Fall sollte jedoch vermieden werden, eine Rechtsgrundlage für die Datenerhebung der Polizei zu schaffen, auf die die Polizei- und Ordnungsbehörden zurückgreifen können für den Fall, dass die Voraussetzungen einer gesetzlichen Grundlage für die Datenerhebung nicht vorliegen (vgl. Bäcker, Die Richtlinie (EU) 2016/680 für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, 63 (71)). Daher ist es zwingend erforderlich, dass der Anwendungsbe-

reich der Einwilligung als Rechtgrundlage ausschließlich Sachverhalten vorbehalten bleibt, in denen die betroffenen Personen tatsächlich über eine echte Wahlfreiheit verfügen. Diese Anforderung des § 33 Abs. 4 LDSG wird durch die Gesetzesbegründung (S. 118) bekräftigt. Dort werden auch zutreffende Beispiele aufgezählt, bei denen eine solche echte Wahlfreiheit in Bezug auf die Verarbeitung ihrer Daten für die betroffenen Personen besteht.

Angesichts der Schaffung gesteigerter Transparenzanforderungen, indem geregelt wird, dass über die Freiwilligkeit der Verarbeitung und über das Widerrufsrecht der betroffenen Person vor der Datenerhebung zu informieren ist, dem Verweis auf die Anforderungen des § 33 LDSG sowie den Beispielen der Gesetzesbegründung, ist die Regelung der Einwilligung in diesen engen Grenzen aus datenschutzrechtlicher Sicht hinnehmbar.

3.3. Besondere Kategorien personenbezogener Daten

In § 27 Abs. 2 POG-E wird die Verarbeitung besonderer Kategorien personenbezogener Daten geregelt. Bedeutsam ist, dass die besonderen Kategorien personenbezogener Daten nicht nur Gesundheitsdaten umfassen, sondern z.B. auch Daten zur "rassischen" und ethischen Herkunft betroffener Personen, Daten aus denen die politische Meinung und religiöse Überzeugungen hervorgehen oder biometrische Daten, die zur eindeutigen Identifizierung einer betroffenen Person verarbeitet werden. Diese Daten sind nicht nur vor dem Hintergrund des Grundrechts auf den Schutz personenbezogener Daten (Art. 8 Europäische Grundrechtecharta) schutzwürdig, sondern insbesondere auch im Hinblick auf das Recht auf Nichtdiskriminierung (Art. 21 Europäische Grundrechtecharta) sowie die Meinungs- und Religionsfreiheit (Art. 10, Art. 11 Europäische Grundrechtecharta) besonders grundrechtssensibel.

Der Landesgesetzgeber ist dabei angemessen seinem Umsetzungsauftrag aus Art. 10 Richtlinie (EU) 2016/680 dahingehend nachgekommen, Rechtsgrundlagen zu schaffen, die sicherstellen, dass die Verarbeitung vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Personen erfolgt. Dem gesteigerten Schutzbedürfnis besonderer Kategorien personenbezogener Daten wird dadurch verstärkt verfahrenstechnisch Rechnung getragen, dass der Zugriff auf solche Daten grundsätzlich beschränkt wird, es sei denn es bestehen keine Risiken für die Rechte und Freiheiten der betroffenen Personen oder, dass andere Garantien im Sinne des § 29 Abs. 2 LDSG vorgesehen werden. Durch die geregelte Dokumentationspflicht unterliegt der Verantwortliche in diesem Zusammenhang einem Rechtfertigungsgebot, das den Zugriff auf besondere Kategorien personenbezogener Daten überprüfbar macht. Dies gilt für die Kontrolle sowohl durch den Verantwortlichen selbst als auch durch den LfDI.

Mit der Regelung ist eine richtlinienkonforme Umsetzung der Anforderungen des Art. 10 Richtlinie (EU) 2016/680 erfolgt, die zudem eine wünschenswerte Konkretisierung des eher pauschalen § 29 LDSG darstellt.

Entsprechend sollten die betreffenden Daten gekennzeichnet werden (dazu unter Abschnitt 3.8.).

3.4. Technisch organisatorischer Datenschutz

Im Rahmen der Anpassung des Polizei- und Ordnungsbehördengesetzes an die Anforderungen des europäischen Datenschutzrechtes werden § 41 POG (Errichtung von polizeilichen Dateien) und § 41 a POG (Technische und organisatorische Maßnahmen des Datenschutzes) aufgehoben. Begründet wird dies damit, dass die Errichtungsanordnungen europarechtlich nicht vorgesehen sind und mit der Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten sowie zur Durchführung einer Datenschutz-Folgenabschätzung neue Instrumente bestehen, die den Wegfall der Errichtungsanordnungen kompensieren. Im Unterschied zu den Errichtungsanordnungen, bei denen der LfDI im Vorfeld beteiligt wurde (§ 41 Abs. 3 POG), ist eine Beteiligung des LfDI bei der Erstellung des Verzeichnisses über Verarbeitungstätigkeiten oder bei der Durchführung der Datenschutz-Folgenabschätzung gesetzlich nicht vorgesehen. Bei Kontrollen und Prüfungen des Landesbeauftragten werden diese beiden Instrumente des Datenschutzmanagements und der Dokumentation regelmäßig und verstärkt Gegenstand der Untersuchung sein.

Mit Blick auf Art, Umfang, Sensitivität und Zweck der von der Polizei verarbeiteten Daten dürfte regelmäßig ein hohes Risiko im Sinne des § 56 Abs. 1 LDSG bzw. Art. 27 Abs. 1 Richtlinie (EU) 2016/680 gegeben sein. Daher ist in solchen Fällen, zu denen (operative) Verfahren der Polizei regelmäßig zählen, eine Datenschutz-Folgenabschätzung durchzuführen.

Erfreulich ist dagegen, dass die Regelung des IT-Sicherheits- und Datenschutzaudits in § 41 a Abs. 3 POG durch die Regelung des § 27 Abs. 5 POG-E aufrecht erhalten wurde. Durch diese Auditierungsverfahren ist ein adäquates Sicherheits- und Datenschutzniveau regelmäßig Gegenstand einer formalen Betrachtung, was gerade im Hinblick auf die Zunahme von Datenverarbeitungen mit überörtlicher Bedeutung und künftige Ausweitungen des Informationsaustausches der Polizeien des Bundes und der Länder erforderlich ist. So kann eine einheitliche Qualität der IT-Verfahren und Datenverarbeitung sichergestellt werden.

3.5. Datenschutzkontrolle durch den LfDI (§ 47 Abs. 5 POG-E)

Durch § 47 Abs. 5 POG-E werden dem LfDI Kontrollpflichten bezüglich besonders eingriffsintensiver Maßnahmen auferlegt, die mindestens alle zwei Jahre erfüllt werden sollen. Die aufsichtliche Kontrolle wird als eine der Determinanten aufgezählt, durch die eingriffsintensive Maßnahmen, die in ihrer Ausgestaltung einen wirksamen Individualrechtsschutz erschweren oder unmöglich machen, im Rahmen des kompensatorischen Grundrechtsschutzes verhältnismäßig bleiben (BVerfG NJW 2016, 1781 Rn. 141). Ein maßgeblicher Wesenszug der Datenschutzaufsicht ist ihre Unabhängigkeit. Sie muss frei über diejenigen Ressourcen und Befugnisse verfügen, die für einen wirksamen Grundrechtsschutz erforderlich sind (vgl. EuGH, NJW 2010, 1265 ff.). Dieses Erfordernis der Unabhängigkeit wurde entsprechend auch in Art. 41- 44 der Richtlinie (EU) 2016/680 festgelegt. Insofern versteht der LfDI die Regelung als eine Klarstellung, dass der datenschutzrechtlichen Kontrolle durch den LfDI eine tragende Rolle zukommt und der LfDI insoweit im Rahmen eine europarechtskonformen Auslegung der Gesetze (LDSG, POG) Prioritäten und Schwerpunkte setzen kann.

Im Sinne der betroffenen Personen, die Adressaten der in § 47 Abs. 5 POG-E aufgeführten Maßnahmen sind, wird der zweijährige Turnus der Kontrolle durch den LfDI grundsätzlich angestrebt.

Dankenswerterweise wurde auch die Zurverfügungstellung entsprechender Unterlagen geregelt, wie bereits im Rahmen der Stellungnahme zum vorherigen Gesetzentwurf des Polizei- und Ordnungsbehördengesetz gefordert (LT-Drs 17/1541). Sowohl die verfassungsmäßigen als auch die europarechtlichen Anforderungen an eine effektive Datenschutzaufsicht stehen allerdings in einem engen Zusammenhang zu ausreichenden personellen und sachlichen Ressourcen sowie einer dementsprechenden ausreichenden Ausstattung der Datenschutzaufsicht.

3.6. Benachrichtigung bei verdeckten Maßnahmen (§ 48 POG-E)

Die Benachrichtigungspflichten bei verdeckten Maßnahmen wurden im Vergleich zu der vorherigen Regelung der Unterrichtung in § 40 Abs. 5 und Abs. 6 POG zu Recht erheblich erweitert. Erfreulicherweise wurde die anlasslose Kennzeichenerfassung ebenfalls in die Reihe der Maßnahmen, die eine Benachrichtigung nach sich ziehen, mit aufgenommen.

Bei zahlreichen Maßnahmen wurde die Benachrichtigung neben dem Adressaten der Maßnahme auf die Personen beschränkt, deren Daten erhoben und weiterverarbeitet wurden. In diesem Zusammenhang ist zu betonen, dass unter "Weiterverarbeitung" im Sinne der Vorschrift jede Verarbeitung im Sinne des § 27 Nr. 2 Landedatenschutzgesetz zu fassen ist, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Insofern ist bereits die Speicherung auch personenbeziehbarer Daten, wie z.B. einer Mobilfunknummer, die im Wege der Funkzellenabfrage erhoben wurde, eine Weiterverarbeitung im Sinne der Norm, die die Benachrichtigungspflicht nach sich ziehen könnte. Vor diesem Hintergrund dürfte die Einschränkung nicht von erheblicher Tragweite sein. Im Ergebnis werden die von der verdeckten Maßnahme betroffenen Personen in Bezug auf ihre Betroffenenrechte insoweit erheblich gestärkt.

Die Benachrichtigungspflicht wird jedoch durch den im Rahmen der Verweisung des § 48 Abs. 2 auf § 28 Abs. 3 Satz 6 POG-E geregelten Zustimmungsvorbehalt der Verfassungsschutzbehörden des Bundes oder der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erheblich eingeschränkt. Dies stellt eine neue Regelung dar, die weder europa- noch verfassungsrechtlich geboten ist. Die Einschränkung der Benachrichtigungspflicht wird nicht durch Ausnahmetatbestände der Richtlinie (EU) 2016/680 abgedeckt (Öffentliche Sicherheit gem. Art. 13 Abs. 3 lit. c Richtlinie (EU) 2016/680 oder nationale Sicherheit (Art. 13 Abs. 3 lit. d Richtlinie (EU) 2016/680)), denn es fehlt die Regelung einer Bedingung bzw. Umsetzung des Art. 13 Abs. 3 1. Hs Richtlinie (EU) 2016/680.

Zudem würde es hinsichtlich des Zwecks der Einschränkung, dass durch die Benachrichtigung nicht der Erfolg der Maßnahme gefährdet wird (Gesetzesbegründung S. 117) ausreichen, im Rahmen der Benachrichtigung Informationen über die betreffenden Sicherheitsbehörden als Empfänger der personenbezogenen Daten nicht an die betroffene Person zu übermitteln.

Wird durch die Benachrichtigung, dass die personenbezogenen Daten an die betreffenden Sicherheitsbehörden im Sinne des § 48 Abs. 3 POG-E übermittelt wurden, eines der Schutzgüter des Abs. 2 gefährdet und die Zustimmung dieser Sicherheitsbehörden deswegen nicht erteilt, ist dies

hinreichend zu begründen. In richtlinienkonformer Auslegung (Art. 13 Abs. 2 Richtlinie (EU) 2016/680) sollte zudem geregelt werden, dass die ansonsten zu erteilende Benachrichtigung nur dann die Angabe über die betreffenden Sicherheitsbehörden enthalten darf, wenn diese zugestimmt haben.

§ 28 Abs. 3 Satz 6 POG-E ist wie folgt zu fassen:
"Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden des Bundes oder der Länder, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst, ist ~~sie~~ **die Angabe nach S. 5 über die Kategorien der Empfänger** nur nach Zustimmung dieser Stellen zulässig."

3.7. Einschränkung des Zweckbindungsgrundsatzes zu Identitätszwecken mittels Verarbeitung von Grunddaten

Die allgemeine Vorschrift zu Zweckbindung und Zweckänderung in § 50 Abs. 1 und Abs. 2 POG-E sowie die Regelungen zum Grundsatz der hypothetischen Datenneuerhebung in § 51 POG-E stehen grundsätzlich in Einklang mit der Rechtsprechung des Bundesverfassungsgerichts.

Verfassungsrechtlichen Bedenken begegnet dagegen § 50 Abs. 3 POG-E, der in Anlehnung an § 12 Abs. 4 BKAG vorsieht, dass die strengen Vorgaben der Zweckbindung und der Grundsatz der hypothetischen Datenneuerhebung dann nicht gelten, wenn die Grunddaten einer Person zu Identifizierungszwecken verwendet werden sollen. Sinn und Zweck der Regelung bestehe darin, die zweifelsfreie Klärung der Identität einer Person zu erreichen, um Identitätsverwechslungen auszuschließen (Gesetzesbegründung S. 137).

Die Verarbeitung der Grunddaten einer betroffenen Person zum Zwecke der Identitätsfeststellung stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz sowie das Recht auf den Schutz personenbezogener Daten gem. Art. 8 der Europäischen Grundrechtecharta dar, der durch eine normenklare, verhältnismäßige Rechtsgrundlage gerechtfertigt sein muss. Das Bundesverfassungsgericht hat dazu jüngst wieder betont, dass auch unter Berücksichtigung eines nicht erheblichem Eingriffsgewichts infolge des allgemeinen Charakters der erhobenen Daten, wie es in der Gesetzesbegründung (S. 137) zu den sog. Grunddaten angeführt wird, im Bereich der Gefahrenabwehr begrenzende, spezifische Eingriffsschwellen zwingend sind, die sicherstellen, dass auf Daten nur bei einem auf tatsächliche Anhaltspunkte gestützten Eingriffsanlass zugegriffen werden kann. Insbesondere unzulässig sei die Schaffung eines offenen Datenvorrats für vielfältige und ohne äußeren Eingriffsanlass begrenzte Verwendungen im gesamten einer Behörde zugewiesenen Aufgabenbereich (BVerfG, Beschl. vom 27. Mai 2020, 1 BvR 1873/13, 1 BvR 2817/13, Rn. 145).

Trotz der nicht unerheblichen grundrechtlichen Eingriffswirkung durch die Verarbeitung einer Vielzahl von Daten, die zu den Grunddaten gehören sollen (z.B. "gegenwärtiger Aufenthaltsort und frühere Aufenthaltsorte") wird die Datenverarbeitung zur Identitätsfeststellung dagegen unter keine Tatbestandsvoraussetzungen gestellt. Dass diese niedrigstschwellige Datenverarbeitung bereits in

das Bundeskriminalamtgesetz Einzug genommen hat, trägt nicht zur Verfassungsmäßigkeit der Vorschrift bei.

Die Regelung hat zur Folge, dass bei jeder im Rahmen anderer Maßnahmen erforderlichen Identitätsfeststellung dieser weite Datenkranz abgefragt werden kann.

Die Vorschrift ist ersatzlos zu streichen.

3.8. Kennzeichnung (§ 53 POG-E)

Eine zu großen Teilen überzeugende und zentrale Regelung hat in dem Gesetzentwurf die Kennzeichnungspflicht gefunden. Die Kennzeichnung von personenbezogenen Daten bei der Speicherung in polizeilichen Informationssystemen dient einer Vielzahl von grundrechtssichernden Zwecken, die das Bundesverfassungsgericht und auch der europäische Gesetzgeber für die polizeiliche Datenverarbeitung etabliert haben. Durch die Kennzeichnung ist es möglich, der besonderen Schutzbedürftigkeit von personenbezogenen Daten Rechnung zu tragen, die z.B. aufgrund der Zugehörigkeit zu den besonderen Kategorien personenbezogener Daten im Sinne des Art. 10 Richtlinie (EU) 2016/680 oder aufgrund der Eigenschaft als durch Telekommunikationsüberwachung gewonnene Erkenntnisse bestehen.

Zudem befähigt die Kennzeichnung personenbezogener Daten die Verantwortlichen dazu, die Grundsätze der hypothetischen Datenneuerhebung einzuhalten. Nicht zuletzt kann durch Kennzeichnung die Anforderung der Art. 6 Richtlinie (EU) 2016/680 umgesetzt werden, nach verschiedenen Kategorien betroffener Personen zu unterscheiden. Dadurch, dass an die Kennzeichnungen Zugriffsbeschränkungen geknüpft werden können, bildet die Kennzeichnung auch den Grundstein für weitere technisch-organisatorische Maßnahmen.

Dieses Potential schöpft § 53 POG-E teilweise, aber nicht vollständig aus. Die Angaben, die gem. § 53 Abs. 1 POG-E zukünftig gekennzeichnet werden sollen, ermöglichen grundsätzlich, dass die Grundsätze der hypothetischen Datenneuerhebung im Rahmen von bspw. Verbundsystemen eingehalten werden können, sofern die Verantwortlichen gem. Absatz 2 nach Übermittlung (oder Abruf der Daten) die Kennzeichnung auch aufrechterhalten. Durch die Angaben der Kategorien nach § 29 Abs. 3 und § 27 Abs. 4 POG-E wird zudem dem Umsetzungserfordernis aus Art. 6 Richtlinie (EU) 2016/680 angemessen Rechnung getragen.

Gerade im Hinblick auf etwaige organisatorische Folgemaßnahmen, um der Schutzbedürftigkeit der Daten durch Zugriffsbeschränkungen oder andere Maßnahmen technisch-organisatorischer Art Rechnung zu tragen, sollte die Kennzeichnungspflicht jedoch weitere Angaben umfassen. Bereits unter 3.3. erwähnt wird in diesem Zusammenhang die Verarbeitung personenbezogener Daten, die zu den besonderen Kategorien personenbezogener Daten im Sinn des Art. 10 RL (EU) 2016/680 gehören.

Des Weiteren sollte dem Umsetzungsauftrag aus Art. 7 Abs. 1 Richtlinie (EU) 2016/680 durch Kennzeichnung Rechnung getragen werden. Zwar wird in § 27 Absatz 3 POG-E in Umsetzung des

Art. 7 Abs. 1 der Richtlinie (EU) 2016/680 geregelt, dass soweit möglich erkennbar werden muss, ob Daten auf Tatsachen oder persönlichen Einschätzungen beruhen, damit diese Unterscheidung z. B. bei der Festlegung der erforderlichen Speicherdauer berücksichtigt werden kann (§ 50 Abs. 4 Satz 3 POG) (Gesetzesbegründung S. 114), jedoch ist diese "Erkennbarkeit" nicht näher definiert. Die Kennzeichnung würde sich als geeignetes Mittel dazu erweisen.

Dass gem. § 53 Abs. 3 POG-E ein Verarbeitungsverbot für solche Daten besteht, die nicht nach Maßgabe des § 53 Abs. 1 POG-E gekennzeichnet wurden, ist konsequent und begrüßenswert.

3.9. Auskunftsrecht § 66 POG-E

Das Auskunftsrecht wurde umfassend geregelt und die Rechte des Einzelnen, auf Antrag Transparenz bezüglich der Verarbeitung seiner personenbezogenen Daten zu erlangen, deutlich gestärkt. Die Regelung trägt den Anforderungen aus Art. 14 Richtlinie (EU) 2016/680 hinreichend Rechnung. Das Auskunftsrecht versetzt die betroffene Person in die Lage, weitere Betroffenenrechte auszuüben, wie das Recht auf Berichtigung oder Löschung personenbezogener Daten.

Der Zustimmungsvorbehalt der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes bezüglich der Beauskunftung von personenbezogenen Daten, die diese Stellen verarbeiten, begegnet den gleichen Bedenken, die im Hinblick auf die Benachrichtigung nach §§ 28 und 48 POG-E bestehen. Auf die Kritik und den Lösungsvorschlag unter Gliederungspunkt 3.6 wird verwiesen.

Ein Kernelement des Auskunftsrechts der betroffenen Person ist der nachgelagerte Rechtsschutz durch Anrufung des LfDI für den Fall, dass die Auskunft verweigert wird. Wie bereits nach § 40 Abs. 3 POG, wird die betroffene Person bei einer Auskunftsverweigerung über die Möglichkeit in Kenntnis gesetzt, das Auskunftsrecht über den LfDI ausüben und diesen zwecks Überprüfung der Datenverarbeitung gem. § 48 LDSG anrufen zu können.

Dieses Recht der betroffenen Person und die Aufgabe des LfDI als unabhängige Aufsichtsbehörde im Sinne des Art. 42 Abs. 1 Richtlinie (EU) 2016/680 werden durch § 45 Abs. 7 S. 3 LDSG erheblich eingeschränkt. Dies widerspricht den Vorgaben der Richtlinie (EU) 2016/680, denn Einschränkungen des Auskunftsrechts sind gem. Art. 15 Richtlinie (EU) 2016/680 nur gegenüber der betroffenen Person möglich. Auch Art. 17 Richtlinie (EU) 2016/680 sieht keine entsprechenden Einschränkungen gegenüber der zuständigen Aufsichtsbehörde vor.

Vor diesem Hintergrund ist es positiv hervorzuheben, dass der Forderung des LfDI im Rahmen der Beteiligtenanhörung entsprochen wurde, eine Regelung nach hessischem Vorbild (§ 14 Abs. 5 S. 1 HDSIG) zu schaffen. Stellt eine oberste Landesbehörde im Einzelfall fest, dass die Sicherheit des Bundes oder eines Landes dies gebietet, sind die Gründe für die Ablehnung eines Auskunftsantrages dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit persönlich zur Verfügung zu stellen und die Rechte nach § 42 Abs. 2 LDSG nur von der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit persönlich ausgeübt werden. So bleiben die Betroffenenrechte gewahrt und der LfDI wird nicht in seiner unionsrechtlich garantierten Unabhängigkeit eingeschränkt.

3.10. Zuverlässigkeitsüberprüfungen von Personen, die eine Tätigkeit als Bedienstete bei der Polizei anstreben oder einen privilegierten Zutritt zu besonders gefährdeten Veranstaltungen erhalten.

Die Schaffung einer Ermächtigungsgrundlage für Zuverlässigkeitsüberprüfungen durch die Polizei ist zunächst sehr begrüßenswert. Infolge der zunehmend angespannten Sicherheitslage in vielen Situationen besteht ein legitimes Bedürfnis der Sicherheitsbehörden, durch Zuverlässigkeitsüberprüfungen sicherzustellen, dass bei Personen, die sich auf den Liegenschaften der Polizei aufhalten oder die in einer Weise für die Polizei tätig sind, die den Zugang zu sicherheitsrelevanten Bereichen erfordert, keine Sicherheitsbedenken bestehen. Ein weiteres Feld, in dem durch Zuverlässigkeitsüberprüfungen mehr Sicherheit gewährleistet werden soll, sind Großveranstaltungen – sowohl durch öffentliche als auch private Veranstalter.

Der LfDI steht zu dieser Thematik bereits seit längerem im Austausch mit dem Ministerium des Innern und für Sport. Neben der Schaffung einer Rechtsgrundlage wird diesseitig insbesondere das Anliegen verfolgt, ein rechtsstaatliches und transparentes Verfahren zu etablieren. Bei der Bewertung der vorliegenden Regelung muss zum einen berücksichtigt werden, dass die Zuverlässigkeitsüberprüfung eine Vielzahl betroffener Personen umfasst, die persönlich keinen Anlass zu einer solchen Überprüfung geben und zum anderen, dass die Personen, gegen die Sicherheitsbedenken ausgesprochen werden, keine konkrete oder abstrakte Gefahr im Sinne des Polizeirechts verursacht haben. Staatliche Eingriffe in das Recht auf informationelle Selbstbestimmung sind nur zulässig, wenn sie auf einer gesetzlichen Grundlage beruhen, die den Grundsatz der Verhältnismäßigkeit beachtet und aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfGE 65, 1).

Diesen Anforderungen wird die Rechtsgrundlage, die nunmehr geschaffen wurde, nur teilweise gerecht.

3.10.1. Zuverlässigkeitsüberprüfungen zum Schutz der Polizei und von staatlichen Veranstaltungen

Die Bestimmung der in § 67 Abs. 1 POG-E definierten Personengruppen, die einer Zuverlässigkeitsüberprüfung ausgesetzt werden, ist grundsätzlich nachvollziehbar. Bedenken bestehen jedoch in Bezug auf Satz 2 2. Hs., der Personen einschließt, für die ein privilegierter Zutritt zu einer Veranstaltung einer Behörde oder öffentlichen Stelle beantragt wird. Laut Gesetzesbegründung sind davon insbesondere Servicepersonal sowie Journalisten umfasst (Gesetzesbegründung S. 175). Während die Personengruppen nach Abs. 1 in einer sicherheitsrelevanten Funktion tätig sind, halten sich die Personengruppen nach Satz 2 2. Hs. lediglich in dem sicherheitsrelevanten Bereich auf. Es ist höchst fraglich, ob dieser Aufenthalt eine Datenabfrage in der Tiefe, wie sie durch Absatz 3 geregelt wird, rechtfertigt. Zumal vor dem Hintergrund der Pressefreiheit des Art. 5 Abs. 1 GG bestehen im Hinblick auf Journalisten Zweifel.

Hinsichtlich des Absatzes 2 ist zunächst erfreulich, dass nunmehr die Überprüfung die Zustimmung der betroffenen Personen erfordert und nicht mehr eine Einwilligung im Sinne des § 33 LDSG, wie es in dem ursprünglichen Gesetzentwurf vorgesehen war.

Im Gegensatz zur Einwilligung ist die Zustimmung in diesem Zusammenhang keine gesetzliche Legitimation zur Datenverarbeitung, verstärkt aber die Legitimationswirkung einer vorhandenen Befugnisnorm (vgl. Petri, in: Möstl/Schwabenbauer, Art. 31 PAG Rn. 9) als Ausdruck des Grundrechtsschutzes durch Verfahren (vgl. Erwägungsgrund 35 a.E.). Sie kann als Element der Verhältnismäßigkeitsprüfung verstanden werden. Allerdings ist zu beachten, dass dieses Instrument rechtlich noch ungeklärt ist. Die Zustimmung kann jedenfalls nur dann wirksam sein, wenn die betroffene Person sie eindeutig hinreichend informiert erteilt und dies dokumentiert ist. Durch das Schriftlichkeitsgebot werden diese Anforderungen erfüllt.

Des Weiteren bestehen Bedenken hinsichtlich der in Absatz 3 geregelten Tiefe der Datenabfrage. Zwar wird durch die Einschränkung des § 67 Abs. 3 S. 2 POG-E sichergestellt, dass die Abfrage der Datenbestände der Polizeien des Bundes und der Länder sowie ggfs. denen der Justizbehörden und Gerichte, des Verfassungsschutzes und des Bundesamtes für Migration und Flüchtlinge nur dann erfolgt, wenn dies im Einzelfall erforderlich ist. Die Wertung, ob dies der Fall ist, richtet sich dabei maßgeblich nach der Ausprägung der besonderen Gefährlichkeit (siehe S. 175 der Gesetzesbegründung) der Veranstaltung, die im Rahmen des Anzeige- bzw. Genehmigungsverfahrens gem. § 26 POG-E festgestellt wird.

Es erschließt sich jedoch vorliegend nicht, warum für den Fall, dass die betroffene Person ein "Ausländer" ist, ein Datenabgleich mit den Datenbeständen des Bundesamts für Migration und Flüchtlinge erfolgt, wozu u.a. das Ausländerzentralregister zählt. Das Ausländerzentralregister steht vielfach in Kritik insbesondere hinsichtlich der Qualität der dort vorgehaltenen Daten. Zu diesen Daten dürften insbesondere den besonderen Kategorien unterfallende personenbezogene Daten zählen, die nur nach Maßgabe des § 29 LDSG verarbeitet werden dürfen. Zur Feststellung der Identität ist der Zugriff auf diesen Datenbestand soweit ersichtlich nicht erforderlich. Zudem begünstigt diese Regelung ein sog. "Racial Profiling" des Verantwortlichen (dazu die Beiträge von Seckelmann, Bender, Cremer/Töpfer, Hesse und Hunold in: Kugelmann (Hrsg.), Polizei und Menschenrechte, 2019). Das Recht auf Nichtdiskriminierung gem. Art. 21 Europäische Grundrechtecharta ist ein hohes Gut und kann durch solch eine Verfahrensweise beeinträchtigt werden.

Durch die generalisierende Umschreibung der "Datenbestände" wird zudem eine Abfragemöglichkeit geschaffen, die sich auch auf zukünftige Datenverbünde beziehen kann, deren Eingriffswirkung in Bezug auf die Datenschutzgrundrechte der betroffenen Personen nicht absehbar ist.

Die Regelung ist ersatzlos zu streichen.

3.10.2. Zuverlässigkeitsüberprüfungen zum Schutz von privaten Veranstaltungen

Zu begrüßen ist die einschränkende Voraussetzung, dass die Zuverlässigkeitsüberprüfungen nur bei besonders gefährdeten Veranstaltungen durchgeführt werden sollen. Die in der Gesetzesbegründung (S. 182) genannten Kriterien ermöglichen es, die besondere Gefährlichkeit zu bestimmen. Diese Gefährdungsprognose eignet sich dazu, die Zuverlässigkeitsüberprüfungen auf das

Erforderliche zu beschränken. Korrespondierend zu der festgestellten Gefährlichkeit müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, sondern 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 (siehe auch die Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018 "Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren").

Durch das eingeführte Anhörungsrecht des LfDI gem. § 68 Abs. 1 a.E. POG-E wird verfahrenstechnisch gewährleistet, dass bei Zuverlässigkeitsüberprüfungen bei privaten Veranstaltungen die Rechte der betroffenen Personen gewahrt werden.

4. Weitere Optimierungspotenziale

4.1. Protokollierungen von Bestandsdatenauskünften

Ein Aspekt des Beschlusses des Bundesverfassungsgericht zum Abruf und der Übermittlung von Bestandsdaten (BVerfG, Beschl. vom 27. Mai 2020, 1 BvR 1873/13, 1 BvR 2817/13), der sich bislang nicht in dem Gesetzentwurf wiederfindet, betrifft die Dokumentation der Entscheidungsgrundlagen in Bezug auf den Abruf dynamischer IP-Adressen (BVerfG, Beschl. vom 27. Mai 2020, 1 BvR 1873/13, 1 BvR 2817/13, Rn. 248, 259). Vor diesem Hintergrund müssten Maßnahmen des § 42 Abs. 2 POG-E in den Katalog des § 47 Abs. 2 POG-E aufgenommen werden.

4.2. Speicherdauer und Mitziehautomatik

Im Rahmen des Gesetzgebungsverfahrens wurde diskutiert, ob die Fristen zur Speicherung personenbezogener Daten verkürzt werden sollten. Dies wäre aus datenschutzrechtlicher Perspektive vorteilhaft gewesen. Im Ergebnis wurde von diesem Vorhaben jedoch Abstand genommen, weil sich in einem Einzelfall die Möglichkeit des Zugriffs auf jahrzehntelang gespeicherte Daten als ausschlaggebend für einen erheblichen Ermittlungserfolg erwiesen hat. Diesen Ermittlungserfolg möchte der LfDI genauso wenig in Abrede stellen wie die Notwendigkeit, im Falle besonders schwerwiegender Straftaten, wie politisch motivierter Gewaltkriminalität oder im Falle von Verbrechen gegen die sexuelle Selbstbestimmung (insbesondere von Kindern) erweiterte Speicherfristen vorzusehen. Dies sollte jedoch durch ein interessengerechtes und damit verhältnismäßiges Konzept in Bezug auf Speicher- und Löschfristen realisiert werden. Die pauschale Beibehaltung langer Höchstspeicherfristen unabhängig vom Speicherungsanlass erweist sich dagegen nicht als überzeugende Lösung.

Dies gilt insbesondere vor dem Hintergrund der Regelung des § 52 Abs. 5 S. 2 POG-E, die eine sogenannte „Mitziehautomatik“ enthält. Dadurch, dass jede weitere Speicherung personenbezogener Daten über dieselbe Person dazu führt, dass für alle Speicherungen einheitlich der Prüfungstermin gilt, der als letzter eintritt, oder die Aufbewahrungsfrist, die als letztes endet, kann dies zur Folge haben, dass der in § 52 Abs. 5 S. 1 POG-E genannte fristauslösende Zeitpunkt des „letzten Ereignisses“ niemals eintritt.

Die Thematik erfordert eine differenziertere Auseinandersetzung und eine schlüssige Systematik. Dies führt zumindest auf untergesetzlicher Ebene zu Handlungsbedarf.

5. Zusammenfassende Einschätzung

Das Gesetzgebungsverfahren wurde überwiegend dazu genutzt, das neue europäische Rechtsregime des Datenschutzes systematisch und normenklar im Sicherheitsrecht umzusetzen.
Auch die Verwirklichung der Vorgaben des Urteils des Bundesverfassungsgerichts (BVerfG) zum Bundeskriminalamtgesetz (BKAG) vom 20. April 2016 (BVerfGE 141, 220) ist grundsätzlich gelungen. Es werden Mechanismen eingeführt und ausgebaut, die das Datenschutzniveau der polizeilichen Datenverarbeitung in Rheinland-Pfalz heben. Insbesondere die Betroffenenrechte wurden – auch aufgrund der Anforderungen der Richtlinie (EU) 2016/680 – erheblich gestärkt.

Durch die Änderungen wird das Polizei- und Ordnungsbehördengesetz des Landes Rheinland-Pfalz modernisiert und wird dem Anspruch gerecht, die Polizeibehörden mit zeitgemäßen und verhältnismäßigen Eingriffsbefugnissen auszustatten. Es ist dem Gesetzgeber erneut gelungen, den Ausgleich zwischen Freiheit und Sicherheit herzustellen, ohne dass die polizeiliche Aufgabenerfüllung über Gebühr erschwert wird.

Flankiert sind diese Regelungen von einer effektiven Datenschutzkontrolle durch den LfDI. Der LfDI nimmt die ihm vom Gesetzgeber zugewiesenen zusätzlichen Aufgaben gerne an. Dies geht mit der Notwendigkeit einher, dass der Behörde entsprechende Ressourcen zur Verfügung stehen, worauf an dieser Stelle ausdrücklich hingewiesen wird.

Die Vorschriften des POG-E sind ausführlich und zukunftsgewandt, die teils Vorbildcharakter tragen. Regelungslücken sind nicht ersichtlich. Dadurch wird ein transparentes und grundrechtsfreundliches Regelungsregime etabliert. Dies betrifft gerade auch die Wahrung des Rechts auf informationelle Selbstbestimmung und die verfahrensrechtlichen Vorkehrungen zum Schutz dieses Rechts.

Dieter Kugelmann

Prof. Dr. Dieter Kugelmann