§ 28
Besondere Mittel der verdeckten Datenerhebung

(1) Die Polizei kann personenbezogene Daten durch den Einsatz besonderer Mittel der verdeckten Datenerhebung nach Absatz 2 erheben über

1. **die Verantwortlichen nach den §§ 4 und 5 und unter den Voraussetzungen des § 7 über die dort genannten Personen, soweit die Datenerhebung zur Abwehr einer Gefahr für Leib oder Leben erforderlich ist,**
2. **Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten von erheblicher Bedeutung begehen und die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist,**
3. **Personen, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine in § 129a Abs. 1 und 2 des Strafgesetzbuchs bezeichnete Straftat begehen, die dazu bestimmt ist**
   a) **die Bevölkerung auf erhebliche Weise einzuschüchtern,**
   b) **eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder**
   c) **die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen,**

   und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können,
4. **Kontakt- und Begleitpersonen (§ 26 Abs. 3 Satz 2), soweit die Datenerhebung zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist, und**
5. **Personen im Umfeld einer in besonderem Maß als gefährdet erscheinenden Person, soweit die Datenerhebung zur Abwehr der Gefahr erforderlich ist.**

Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Besondere Mittel der verdeckten Datenerhebung im Sinne dieses Gesetzes sind

1. **die planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden oder über einen Zeitraum von mehr als einer Woche durchgeführt werden soll (längerfristige Observation),**
2. **der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen,**

3. der verdeckte Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes,
4. der Einsatz von Polizeibeamten unter einer ihnen auf Dauer angelegten Legende (verdeckte Ermittler),
5. der Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist (Vertrauenspersonen), und
6. der Einsatz technischer Mittel zur Feststellung des jeweiligen Standortes einer Person oder eines Fahrzeuges.

(3) Straftaten von erheblicher Bedeutung im Sinne dieses Gesetzes sind

1. Verbrechen und
2. Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, soweit sie
   a) sich gegen Leib, Leben oder Freiheit einer Person oder bedeutende Sach- oder Vermögenswerte richten,
   b) auf den Gebieten des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- und Wertzeichenfälschung oder des Staatsschutzes (§§ 74a und 120 des Gerichtsverfassungsgesetzes) begangen werden, oder
   c) gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangen werden.

(4) Der Einsatz besonderer Mittel nach

1. Absatz 2 Nr. 1,
2. Absatz 2 Nr. 2, soweit Bildaufzeichnungen bestimmter Personen durchgehend länger als 24 Stunden oder über einen Zeitraum von mehr als einer Woche angefertigt werden sollen,
3. Absatz 2 Nr. 3 bis 5

bedarf der richterlichen Entscheidung. Die Maßnahme nach Absatz 2 Nr. 1 bis 3 ist auf höchstens einen Monat zu befristen; im Fall des Absatzes 2 Nr. 4 und 5 ist die Maßnahme auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 gilt entsprechend. Bei Gefahr im Verzug kann die Maßnahme vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten mit der Befähigung für das vierte Einstiegsamt angeordnet werden; die richterliche Entscheidung ist unverzüglich nachzuholen.

(5) Der Einsatz besonderer Mittel nach Absatz 2 Nr. 2, soweit es keiner richterlichen Entscheidung nach Absatz 4 Satz 1 Nr. 2 bedarf, und Absatz 2 Nr. 6 darf nur durch die Behördenleitung oder einen von ihr besonders

beauftragten Beamten mit der Befähigung für das vierte Einsteigsamt angeordnet werden. Bei Gefahr im Verzug können besondere Mittel nach Absatz 2 Nr. 2 und 6 vorläufig eingesetzt werden; eine Entscheidung nach Satz 1 ist unverzüglich nachzuholen.

(6) Nach Absatz 2 Satz 1 Nr. 1, 3 bis 5[1] erlangte personenbezogene Daten sind besonders zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch die Empfänger aufrechtzuerhalten. Solche Daten dürfen für einen anderen Zweck verwendet werden, soweit sich aus ihnen konkrete Ermittlungsansätze zur

1. **Verfolgung oder Verhütung von Straftaten von erheblicher Bedeutung nach Absatz 3 oder**
2. **zur Abwehr einer Gefahr für Leib oder Leben einer Person**

ergeben und die Verwendung der Daten zu diesem Zweck erforderlich ist. Die Zweckänderung der Daten muss im Einzelfall festgestellt und dokumentiert werden.

(7) Nach Absatz 2 Satz 1 Nr. 2 und 6[2] erlangte personenbezogene Daten dürfen für einen anderen Zweck verwendet werden, soweit dies zur Verfolgung oder Verhütung von Straftaten von erheblicher Bedeutung nach Absatz 3 oder zur Abwehr einer Gefahr für Leib oder Leben einer Person erforderlich ist. Die Zweckänderung der Daten muss im Einzelfall festgestellt und dokumentiert werden.

(8) Soweit es zur Geheimhaltung der wahren Identität des verdeckten Ermittlers erforderlich ist, dürfen entsprechende Urkunden hergestellt, verändert und gebraucht werden. Ein verdeckter Ermittler darf zur Erfüllung seines Auftrages unter Geheimhaltung seiner wahren Identität am Rechtsverkehr teilnehmen sowie mit Einverständnis des Berechtigten, nicht jedoch unter Vortäuschung eines Zutrittsrechts, dessen Wohnung betreten. Soweit es zur Geheimhaltung der Zusammenarbeit einer Vertrauensperson mit der Polizei erforderlich ist, gilt Satz 1 entsprechend.

Erläuterungen

Übersicht

1) Anm. der Verf.: Absatz 2 hat keinen Satz 1. Korrekt müsste es lauten „Absatz 2 Nr. 1, 3 bis 5".
2) Anm. der Verf.: Absatz 2 hat keinen Satz 1. Korrekt müsste es lauten „Absatz 2 Nr. 2 und 6".

V. Richtervorbehalt, Befristung der Maßnahme (Abs. 4)
VI. Behördenleitervorbehalt, Befristung der Maßnahme (Abs. 5)
VII. Kennzeichnung, Zweckänderung bei Daten aus eingriffsintensiven besonderen Mitteln (Abs. 6)
VIII. Zweckänderung bei Daten aus weniger eingriffsintensiven besonderen Mitteln (Abs. 7)
IX. Geheimhaltung der Identität eines verdeckten Ermittlers oder einer Vertrauensperson; Befugnisse des verdeckten Ermittlers (Abs. 8)

I. Allgemeines

1. Entstehungsgeschichte der Vorschrift: § 28 POG wurde durch Gesetz vom 2. März 2004 (GVBl. S. 202) geschaffen. Die Vorgängerregelung in § 25b, die durch Gesetz vom 26. März 1986 (GVBl. S. 77) in das damalige Polizeiverwaltungsgesetz eingefügt worden war, enthielt eine allgemein gehaltene, nicht bereichsspezifische Ermächtigung zur verdeckten Informationserhebung durch den Einsatz „bestimmter besonderer technischer Mittel oder Personen". Durch Gesetz vom 15. Februar 2011 (GVBl. S. 26) wurde die in § 28 Abs. 4 POG a. F. enthaltene Regelung zum Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger gestrichen, weil deren Inhalt in der neu geschaffenen Vorschrift des § 39b POG aufging, die den Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger für alle verdeckten Datenerhebungen regelt. Grundlegend überarbeitet wurde die Vorschrift durch das Gesetz vom 30. Juni 2017 (GVBl. S. 123), mit dem zentrale Vorgaben aus dem Urteil des BVerfG vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – zum Bundeskriminalamtgesetz umgesetzt worden sind (vgl. Erl. I.3). Dies betrifft etwa die Vorgaben zum Richtervorbehalt und zur Zweckänderung. Darüber hinaus wurde in § 28 Abs. 1 Satz 1 Nr. 3 POG die Möglichkeit geschaffen, zur Verhinderung terroristischer Straftaten besondere Mittel der verdeckten Datenerhebung bereits im Vorfeld konkreter Gefahren einzusetzen, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit der Begehung entsprechender Straftaten begründet.

2. Folgende Grundrechte sind von § 28 POG betroffen: Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 13 Abs. 1 GG.

a) Verdeckte Datenerhebungen mit besonderen Mitteln greifen in das Recht auf informationelle Selbstbestimmung als besonderer Ausprägung des allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein (vgl. dazu Erl. I.2 zu § 26). Das Eingriffsgewicht der Maßnahmen kann sehr unterschiedlich sein. Während etwa das Anfertigen einzelner Fotos oder der Einsatz technischer Mittel wie Peilsender eher ein geringeres oder mittleres Eingriffsgewicht haben, kann die längerfristige Observation einen schwerwiegenden Eingriff in

die Privatsphäre darstellen, insbesondere wenn sie mit anderen Maßnahmen gebündelt durchgeführt wird – wie z. B. mit Bild- und Tonaufzeichnungen (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 151, 174).

b) Umstritten ist, ob ein Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung gem. Art. 13 Abs. 1 GG vorliegt, wenn ein verdeckter Ermittler (§ 28 Abs. 2 Nr. 4 POG) im Rahmen seiner Ermittlungen eine Wohnung betritt, weil ihm der Wohnungsinhaber, der nicht weiß, dass er es mit einem verdeckten Ermittler zu tun hat, den Zutritt gewährt. Gegen einen Eingriff spricht der Umstand, dass der verdeckte Ermittler die Wohnung mit Einverständnis des Wohnungsinhabers betritt. Andererseits wird dieses Einverständnis durch Täuschung erschlichen, denn der Wohnungsinhaber irrt sich über die wahre Identität des verdeckten Ermittlers. Deshalb könnte das Einverständnis unwirksam sein. Hiergegen wiederum ließe sich einwenden, dass zwar ein Irrtum vorliegt, dieser aber die Wirksamkeit des Einverständnisses unberührt lässt, weil er nur den von Art. 13 Abs. 1 GG nicht geschützten Willensbildungsprozess, nicht hingegen speziell das Zutrittsrecht des verdeckten Ermittlers betrifft. Nach dieser Auffassung liegt ein Eingriff in Art. 13 Abs. 1 GG nur vor, wenn die Täuschung des verdeckten Ermittlers gerade auf das Verschaffen des Wohnungszutritts gerichtet war (Herdegen, in: Bonner Kommentar, Art. 13 Rn. 45). Nach Ansicht von Hilger liegt im bloßen Mitgehen des verdeckten Ermittlers in eine Wohnung kein hoheitlicher Eingriff in Art. 13 Abs. 1 GG, da dieser hier nicht von sich aus in hoheitlicher Funktion tätig werde (Hilger, NStZ 1997, S. 449 f.). Dagegen spricht jedoch, dass der verdeckte Ermittler trotz des zivilen Anscheins die Wohnung als Polizeibeamter im Rahmen seines gefahrenabwehrrechtlichen oder strafprozessualen Ermittlungsauftrags betritt (vgl. zum Streitstand Schneider, NStZ 2004, 359 (365 ff.); BGH, Urteil vom 6. Februar 1997 – 1 StR 527/96 – juris, Rn. 13 ff.). Eine verbreitete Auffassung im Schrifttum geht jedenfalls davon aus, dass das Betreten einer Wohnung unter einer Legende stets einen Eingriff in das Wohnungsgrundrecht darstellt, weil der Wohnungsinhaber darüber getäuscht wird, dass ein Polizeibeamter die Wohnung betritt (Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 375, Rn. 257; Jarass, in: Jarass/Pieroth, GG, Art. 13 Rn. 10; Hauck, in: Löwe/Rosenberg, StPO, § 110c Rn. 17). In der Rechtsprechung ist die Frage eines Eingriffs in Art. 13 Abs. 1 GG – soweit ersichtlich – noch nicht entschieden worden. Geht man von einem Eingriff in Art. 13 Abs. 1 GG aus, stellt sich die Frage nach seiner verfassungsrechtlichen Rechtfertigung. Grundrechtseingriffe zu Strafverfolgungszwecken sind nach Art. 13 Abs. 2 und 3 GG explizit nur bei Durchsuchungen und dem Einsatz technischer Mittel zur akustischen Überwachung erlaubt. § 110c Satz 1 StPO, der das Betreten der Wohnung durch einen verdeckten Ermittler gestattet, könnte deshalb verfassungswidrig sein (vgl. hierzu Hauck, in: Löwe/Rosenberg, StPO, § 110c Rn. 19 ff.; Frister, in: Lisken/Denninger, Handbuch des

Polizeirechts, S. 701, Rn. 332). Im präventiven Bereich sind hingegen nach Art. 13 Abs. 7 GG auch sonstige Eingriffe und Beschränkungen in Art. 13 Abs. 1 GG zugelassen, wenn sie der Abwehr einer gemeinen Gefahr oder Lebensgefahr oder der Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung dienen. Der Gesetzgeber ging wohl davon aus, dass das Betreten einer Wohnung durch einen verdeckten Ermittler keinen Eingriff in Art. 13 Abs. 1 GG darstellt, denn in dem Gesetz vom 2. März 2004 (GVBl. S. 202), mit dem § 28 POG geschaffen wurde, findet sich – entgegen dem Zitiergebot des Art. 19 Abs. 1 Satz 2 GG – kein Hinweis darauf, dass das Grundrecht aus Art. 13 Abs. 1 GG eingeschränkt wird.

3. Urteil des BVerfG vom 20. April 2016 zum Bundeskriminalamtgesetz

a) Mit Urteil vom 20. April 2016 (1 BvR 966/09, 1 BvR 1140/09) hat das BVerfG entschieden, dass die Ermächtigungen im Bundeskriminalamtgesetz zum Einsatz heimlicher Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus zwar im Grundsatz mit der Verfassung vereinbar sind, in ihrer konkreten Ausgestaltung jedoch teilweise dem Verhältnismäßigkeitsgrundsatz nicht genügen. Die Entscheidung betrifft sowohl die Voraussetzungen für die Durchführung der Maßnahmen als auch die Frage der Übermittlung der Daten an andere in- oder ausländische Behörden.

b) Im Einzelnen geht es insbesondere um

- heimliche Überwachungsmaßnahmen außerhalb von Wohnungen (§ 20g BKAG a. F.),
- Wohnraumüberwachung (§ 20h BKAG a. F.),
- Telekommunikationsüberwachung (§ 20l BKAG a. F.),
- verdeckter Eingriff in informationstechnische Systeme (§ 20k BKAG a. F.),
- Schutz des Kernbereichs privater Lebensgestaltung,
- Schutz zeugnisverweigerungsberechtigter Personen (§ 20u BKAG a. F.),
- flankierende Regelungen zur Gewährleistung von Transparenz, Rechtsschutz und aufsichtlicher Kontrolle (insbesondere Benachrichtigungspflichten an den Betroffenen, Berichts- und Protokollierungspflichten, turnusmäßige Kontrollen durch die oder den Datenschutzbeauftragte/-n),
- Datennutzung im Rahmen der Zweckbindung und
- Datenübermittlung an andere in- oder ausländische Behörden (Zweckänderung).

c) Die Mehrzahl der beanstandeten Vorschriften galt mit Einschränkungen bis zum Ablauf des 30. Juni 2018 fort. Verfassungswidrig und nichtig waren nur die Regelungen in § 20h Abs. 1 Nr. 1c BKAG a. F. (Wohnraumüberwachung

von Kontakt- und Begleitpersonen) und § 20v Abs. 6 Satz 5 BKAG a. F. (Unterbleiben der Löschung von Daten). Durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 (BGBl. I S. 1354), das am 25. Mai 2018 in Kraft getreten ist, hat der Bund die Vorgaben des BVerfG umgesetzt.

Das Urteil hat auch Auswirkungen auf das Polizei- und Ordnungsbehördengesetz, da es zum Teil Vorschriften enthält, die mit den vom BVerfG beanstandeten Vorschriften des Bundeskriminalamtgesetzes vergleichbar sind. Durch das Gesetz vom 30. Juni 2017 (GVBl. S. 123) hat der rheinland-pfälzische Gesetzgeber die in Frage stehenden Regelungen überarbeitet und in wesentlichen Punkten an die verfassungsrechtlichen Anforderungen angepasst. Weitere erforderliche Änderungen (etwa zu Dokumentations- und Berichtspflichten oder zur Datenübermittlung an Drittstaaten) sind einem weiteren Gesetzgebungsverfahren vorbehalten worden, mit dem auch die EU-Datenschutzreform umgesetzt werden soll (LT-Drs. 17/2895, S. 2).

d) Die vom BVerfG beanstandeten Befugnisse ermächtigen das BKA im Rahmen der Gefahrenabwehr und Straftatenverhütung zur heimlichen Erhebung personenbezogener Daten und begründen – je nach Befugnis – Eingriffe in die Grundrechte der Unverletzlichkeit der Wohnung, des Telekommunikationsgeheimnisses und der informationellen Selbstbestimmung sowie in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Sämtliche Beanstandungen des BVerfG ergeben sich aus den Anforderungen der Verhältnismäßigkeit im engeren Sinne. Eingriffsbefugnisse, die – wie die Wohnraumüberwachung oder die Onlinedurchsuchung – tief in die Privatsphäre eingreifen, unterliegen als Ausfluss des Verhältnismäßigkeitsgrundsatzes besonderen Vorgaben an ihre Ausgestaltung. So dürfen sich diese Maßnahmen nicht unmittelbar gegen nichtverantwortliche Dritte aus dem Umfeld der Zielperson richten (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 115). Die Anforderungen an den Kernbereichsschutz sind hier besonders streng (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 196 ff., 217 ff.). Besonders strenge Anforderungen gelten hier auch für die weitere Nutzung der Daten im Rahmen der Zweckbindung oder zu anderen Zwecken (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 283, 291).

Aus Gründen der Verhältnismäßigkeit fordert das BVerfG eine Ausweitung des Richtervorbehalts. So bedürfen etwa auch die Anordnung einer längerfristigen Observation, die Aufzeichnung nicht öffentlicher Gespräche außerhalb von Wohnungen und der Einsatz von Vertrauenspersonen einer richterlichen Entscheidung (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 172 ff.).

Darüber hinaus stellt das BVerfG fest, dass allen angegriffenen Ermittlungs- und Überwachungsbefugnissen flankierende rechtsstaatliche Absicherungen fehlen, ohne die die Verhältnismäßigkeit der Eingriffsbefugnisse nicht gewahrt ist (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 134 ff.). So unterliegen die Befugnisse verfassungsrechtlichen Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle. Hierzu gehören Benachrichtigungspflichten an die Betroffenen nach Durchführung der Maßnahme, eine regelmäßige aufsichtliche Kontrolle sowie Berichtspflichten gegenüber Parlament und Öffentlichkeit. Schließlich müssen die Befugnisse mit Löschungspflichten flankiert sein.

Ferner enthält die Entscheidung in Anknüpfung an die bisherige Rechtsprechung neue Differenzierungen für eine Verwendung der Daten, die über das ursprüngliche Ermittlungsverfahren hinausgehen. Maßgeblich sind hierfür die Grundsätze der Zweckbindung und Zweckänderung (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 276 ff.). Die Verhältnismäßigkeitsanforderungen für eine zweckändernde Datenverwendung orientieren sich am Grundsatz der hypothetischen Datenneuerhebung. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 288). Allerdings wendet das BVerfG das Kriterium der hypothetischen Datenneuerhebung nicht strikt an, sondern lässt Abstriche hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts zu (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 290). Etwas anderes gilt für die Wohnraumüberwachung und die Onlinedurchsuchung. Angesichts des besonderen Eingriffsgewichts dieser Maßnahmen ist jede weitere Nutzung der gewonnenen Daten nur zur Abwehr einer dringenden Gefahr oder einer im Einzelfall hinreichend konkretisierten Gefahr zulässig (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 283, 291).

II. Voraussetzungen der verdeckten Datenerhebung (Abs. 1)

1. Abs. 1 benennt die Tatbestandsvoraussetzungen für den Einsatz besonderer Mittel der verdeckten Datenerhebung. Zweck der Maßnahmen ist entweder die Abwehr konkreter Gefahren für hochrangige Rechtsgüter oder die vorbeugende Bekämpfung von Straftaten.

a) Abs. 1 Satz 1 Nr. 1 erlaubt verdeckte Datenerhebungen, soweit sie zur Abwehr einer konkreten Gefahr für Leib oder Leben erforderlich sind. Konkret ist die Gefahr, wenn aufgrund eines bestimmten Sachverhalts die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für die geschützten Rechtsgüter eintritt (BVerfG, Beschluss vom

4. April 2006 – 1 BvR 518/02 – juris, Rn. 144). Ferner wird festgelegt, über wen zum Zwecke der Gefahrenabwehr heimlich Daten erhoben werden dürfen. Betroffene der Datenerhebung dürfen entweder Verantwortliche nach den §§ 4 und 5 POG oder Nichtverantwortliche unter den Voraussetzungen des § 7 POG sein.

b) Nach **Abs. 1 Satz 1 Nr. 2** dürfen heimliche Datenerhebungen auch über potenzielle Straftäter vorgenommen werden, soweit dies zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. Hier geht es um Ermittlungen im Vorfeld konkreter Gefahren, die angesichts der Schwere des mit heimlichen Überwachungsmaßnahmen verbundenen Eingriffs nicht zulässig sind, wenn „nur relativ diffuse Anhaltspunkte für mögliche Gefahren bestehen“ (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 113). Erforderlich ist vielmehr eine auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützte Prognose, die auf eine konkrete Gefahr bezogen ist. Hierzu gehört, dass ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 112, 164). Diesen Anforderungen wird die durch das Gesetz vom 30. Juni 2017 (GVBl. S. 123) neu gefasste Vorschrift gerecht. Der Einsatz besonderer Mittel der verdeckten Datenerhebung ist nach Abs. 1 Satz 1 Nr. 2 nur bei Personen zulässig, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten von erheblicher Bedeutung begehen. Straftaten von erheblicher Bedeutung sind solche, die mindestens dem Bereich der mittleren Kriminalität zuzurechnen und geeignet sind, den Rechtsfrieden empfindlich zu stören sowie das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (BVerfG, Urteil vom 12. April – 2 BvR 581/01 – juris, Rn. 46). In Abs. 3 werden Straftaten von erheblicher Bedeutung näher konkretisiert.

c) Abs. 1 Satz 1 Nr. 3 erlaubt den Einsatz besonderer Mittel der verdeckten Datenerhebung bei Personen, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen werden. Mit dieser durch das Gesetz vom 30. Juni 2017 (GVBl. S. 123) aufgenommenen Regelung hat der Gesetzgeber die Rechtsprechung des BVerfG aufgegriffen, das in seinem Urteil zum Bundeskriminalamtgesetz die Kriterien für die Zulässigkeit heimlicher Überwachungsmaßnahmen im Vorfeld von Terrorgefahren präzisiert hat. So können Überwachungsmaßnahmen in Bezug auf terroristische Straftaten auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zeit begehen wird (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 112). Mit dieser Prognosemöglichkeit, die nicht an ein

konkretisiertes Schadensereignis, sondern an das individuelle Verhalten einer Person anknüpft, wollte das BVerfG den Besonderheiten bei Terrorgefahren Rechnung tragen. Oftmals liegen den Sicherheitsbehörden nur Erkenntnisse darüber vor, dass bestimmte Personen einen Terroranschlag in Deutschland planen. Sie wissen aber nicht, wie dieser Anschlag aussehen soll, sodass der drohende Schaden noch nicht konkretisiert werden kann. In Fällen dieser Art kann die Prognose an das Verhalten der Person anknüpfen. Ergibt sich hieraus die konkrete Wahrscheinlichkeit, dass sie innerhalb eines übersehbaren Zeitraums eine – wenn auch noch nicht näher konkretisierbare – terroristische Straftat begehen wird, liegen die Voraussetzungen vor, die den Einsatz heimlicher Überwachungsmaßnahmen rechtfertigen können. Hinweise, die nach dem individuellen Verhalten Rückschlüsse auf die konkrete Wahrscheinlichkeit einer terroristischen Straftat zulassen, können sich z. B. aus dem Vorverhalten einer Person (z. B. Rückkehr aus einem Terrorcamp) oder aus sonstigen Umständen ergeben (etwa glaubwürdige Aussagen eines Zeugen; LT-Drs. 17/2895, S. 21). Der Begriff der terroristischen Straftat wird in Abs. 1 Satz 1 Nr. 3 näher definiert.

d) Ebenfalls zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erlaubt **Abs. 1 Satz 1 Nr. 4** die verdeckte Datenerhebung über Kontakt- und Begleitpersonen. Dabei handelt es sich nach der Legaldefinition in § 26 Abs. 3 Satz 2 POG um Personen, die mit potenziellen Straftätern in der Weise in Verbindung stehen, dass durch Tatsachen begründete Anhaltspunkte für ihren objektiven Tatbezug sprechen (vgl. im Einzelnen Erl. IV.6. zu § 26). Verdeckte Datenerhebungen mit besonderen Mitteln werden insbesondere zur Bekämpfung der Organisierten Kriminalität eingesetzt. Für eine effektive Bekämpfung ist es notwendig, die Strukturen der Organisierten Kriminalität zu erforschen und Erkenntnisse zu den Hintermännern zu erlangen, zu denen der Polizei in der Regel zunächst keine näheren Informationen vorliegen. Die Hintermänner werden von dem Begriff der Kontakt- und Begleitperson erfasst, da sie als Auftraggeber in den Handlungskomplex der Straftatenbegehung verwickelt sind (Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 390, Rn. 295). Dementsprechend dürfen verdeckte Ermittler oder Vertrauenspersonen auch dazu eingesetzt werden, um Informationen über die der Polizei noch nicht bekannten, aber vermuteten Hintermänner zu beschaffen. In der Gesetzesbegründung wird der Verhältnismäßigkeitsgrundsatz besonders hervorgehoben und ausgeführt, dass eine Datenerhebung über Kontakt- und Begleitpersonen nur als ultima ratio in Betracht kommt, wenn andere Maßnahmen – insbesondere gegen potenzielle Straftäter – ausscheiden und ohne die Einbeziehung der Kontakt- und Begleitpersonen in die Datenerhebung eine Verhinderung künftiger Straftaten zweifelhaft erscheint (LT-Drs. 14/2287, S. 44). Für den Fortbestand krimineller Organisationen sind gerade die Hintermänner von zentraler Bedeutung, sodass eine Datenerhebung über diese Personen zur vorbeugenden

Straftatenbekämpfung in der Regel erforderlich ist und damit auch dem Verhältnismäßigkeitsgrundsatz genügt.

Das BVerfG hat eine ähnliche Vorschrift in § 20g Abs. 1 Satz 1 Nr. 3 BKAG a. F. für verfassungskonform erklärt (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 168). Dabei hat es allerdings die in § 20b Abs. 2 Nr. 2 BKAG a. F. enthaltene Legaldefinition des Begriffs der Kontakt- und Begleitperson in Bezug genommen und heimliche Überwachungsmaßnahmen gegen diesen Personenkreis nur deshalb für zulässig gehalten, weil der Begriff der Kontakt- und Begleitperson gesetzlich näher eingegrenzt wird. So verlangt § 20b Abs. 2 Nr. 2 BKAG a. F. (§ 39 Abs. 2 Nr. 2 BKAG n. F.) eine näher definierte Tatnähe der Kontakt- und Begleitperson, durch die ausgeschlossen wird, dass das gesamte Umfeld der Zielperson überwacht werden darf (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 168 f.). Zwar wird der Begriff der Kontakt- und Begleitperson auch in § 26 Abs. 3 Satz 2 POG definiert. Ob diese Legaldefinition, die allein auf den „objektiven Tatbezug" abstellt, den Kreis der Kontakt- und Begleitpersonen hinreichend eingrenzt, erscheint nach der Entscheidung des BVerfG allerdings fraglich (vgl. auch Erl. IV.6. zu § 26).

e) Schließlich dürfen gem. **Abs. 1 Satz 1 Nr. 5** Daten über Personen im (räumlichen) Umfeld einer in besonderem Maß als gefährdet erscheinenden Person erhoben werden, wenn dies zur Abwehr der Gefahr erforderlich ist. Erforderlich ist die Datenerhebung nur, wenn und soweit hierdurch Erkenntnisse gewonnen werden können, die für den Schutz der bedrohten Person von Bedeutung sind.

2. Nach **Abs. 1 Satz 2** darf die Datenerhebung nach Abs. 1 Satz 1 Nr. 1 bis 5 auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Dritte sind Personen, die in keiner Beziehung zum anlassgebenden Sachverhalt stehen und deren Daten nur bei Gelegenheit des Einsatzes unvermeidbar miterhoben werden. So können etwa bei Ton- oder Bildaufzeichnungen zwangsläufig unbeteiligte Dritte erfasst werden, wenn sie sich am selben Ort wie der eigentlich Überwachte aufhalten.

III. Besondere Mittel der verdeckten Datenerhebung (Abs. 2)

Abs. 2 benennt die besonderen Mittel der verdeckten Datenerhebung, die zur Gefahrenabwehr und zur Verhütung von Straftaten von erheblicher Bedeutung eingesetzt werden können. Da es sich um verdeckte Maßnahmen der Datenerhebung handelt, ist die Regelung des § 39a POG zu beachten, die für Daten aus dem Kernbereich privater Lebensgestaltung ein absolutes Erhebungs- und Verwertungsverbot statuiert.

1. Abs. 2 Nr. 1 regelt die **längerfristige Observation**. Ziel einer präventivpolizeilichen Datenerhebung durch Observation ist zumeist nicht die Abwehr konkreter Gefahren, sondern die vorbeugende Bekämpfung von Straftaten. Durch heimliche Vorfeldermittlungen sollen Sachverhalte aufgeklärt und Erkenntnisse zu bestimmten Personen gewonnen werden, von denen angenommen wird, dass sie Straftaten begehen werden (OVG Saarland, Urteil vom 6. September – 3 A 13/13 – juris, Rn. 48; VG Freiburg, Urteil vom 14. Februar 2013 – 4 K 1115/12 – juris, Rn. 31). Gegebenenfalls kann die Observation auch der Abwehr konkreter Gefahren dienen, so etwa, wenn sie zur Vorbereitung eines Zugriffs auf zur Ausführung eines terroristischen Anschlags bereite Täter eingesetzt wird (Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 384, Rn. 283).

a) Die längerfristige Observation wird definiert als planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden oder über einen Zeitraum von mehr als einer Woche durchgeführt werden soll. Längerfristig ist eine Observation demnach entweder bei einer ununterbrochenen Rund-um-die-Uhr-Beobachtung einer Person von mehr als 24 Stunden oder bei wiederholten zeitweiligen Beobachtungen, die über einen Zeitraum von mehr als einer Woche durchgeführt werden sollen. Keine längerfristige Observation liegt danach vor, wenn eine Person täglich 23 Stunden über die Dauer von sieben Tagen beobachtet werden soll. Längerfristig ist eine Observation aber, wenn eine Person über einen Zeitraum von zwei Wochen täglich nur eine Stunde beobachtet wird. Verglichen mit der strafprozessualen Regelung der längerfristigen Observation in § 163f Abs. 1 Satz 1 StPO, nach der eine Observation bereits dann längerfristig ist, wenn sie an mehr als zwei Tagen stattfinden soll, erscheint der hier gewählte Zeitraum von mehr als einer Woche gerade auch mit Blick auf die Schwere des mit einer Observation verbundenen Grundrechtseingriffs sehr lang. Die Zulässigkeit von Observationen, die nicht längerfristig i. S. d. § 28 Abs. 2 Nr. 1 POG sind, richtet sich nach den Voraussetzungen des § 26 POG.

b) Eine längerfristige Observation liegt nicht nur dann vor, wenn sie von vornherein auf eine Überschreitung der in Abs. 2 Nr. 1 genannten Fristen gerichtet ist, sondern auch dann, wenn sich während einer zunächst nur kurzzeitig geplanten Observation herausstellt, dass die genannten Fristen überschritten werden. Grundsätzlich ist vor Beginn der Maßnahme zu entscheiden, ob die Observation längerfristig oder kurzfristig sein soll.

c) Definitionsgemäß setzt eine Observation die Beobachtung einer Person voraus. Keine Observation liegt deshalb bei einer objektbezogenen Beobachtung vor. Ob es sich um eine personenbezogene oder eine objektbezogene Beobachtung handelt, richtet sich nach Ansicht des VG Cottbus nach der Zielrichtung des polizeilichen Handelns (VG Cottbus, Beschluss vom 13. März 2008 – 3 L

59/08 – juris, Rn. 6). Wird ein Objekt – z. B. ein Tattoostudio oder eine Wohnung – beobachtet, um Informationen zu einer bestimmten Person zu erlangen, handelt es sich um eine Observation. Soll durch die Beobachtung festgestellt werden, welche Personen an diesem Ort verkehren, liegt keine Observation vor (VG Cottbus, Beschluss vom 13. März 2008 – 3 L 59/08 – juris, Rn. 6 f.; vgl. auch Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 382, Rn. 278).

d) Obgleich Observationen in der Regel heimlich durchgeführt werden, ist sie ihrem Wesen nach nicht auf eine heimliche Beobachtung beschränkt (Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 383, Rn. 279; VG Cottbus, Beschluss vom 13. März 2008 – 3 L 59/08 – juris, Rn. 10 zu einer offen durchgeführten Observation eines Tattoostudios). Im Unterschied zu den Regelungen in den Polizeigesetzen anderer Länder (vgl. z. B. § 32 BbgPolG; § 28 Abs. 2 Nr. 1 SPolG; § 16a PolG NRW) bezieht sich § 28 POG entsprechend seiner Überschrift allerdings nur auf verdeckte Datenerhebungen, sodass eine offen durchgeführte Beobachtung nicht auf § 28 POG gestützt werden kann.

e) Für längerfristige offene Beobachtungen, die regelmäßig mit einem schwerwiegenden Grundrechtseingriff verbunden sind, enthält das Polizei- und Ordnungsbehördengesetz keine Rechtsgrundlage. Eine gewissen Bekanntheitsgrad erreichte die offene Observation von **ehemals sicherungsverwahrten Sexual- und Gewaltstraftätern**, die in Folge eines Urteils des Europäischen Gerichtshofs für Menschenrechte aus der Sicherungsverwahrung entlassen werden mussten, obwohl sie nach wie vor als hochgradig rückfallgefährdet galten (EGMR, Urteil vom 17. Dezember – 19359/04; vgl. auch BVerfG, Urteil vom 4. Mai 2011 – 2 BvR 2333/08 u. a.). Der EuGH hatte festgestellt, dass die rückwirkende Verlängerung einer ursprünglich auf maximal zehn Jahre befristeten Sicherungsverwahrung gegen Art. 5 Abs. 1 EMRK (Recht auf Freiheit und Sicherheit) und Art. 7 Abs. 1 EMRK (keine Strafe ohne Gesetz) verstieß. Eine rückwirkende Verlängerung der Sicherungsverwahrung durch die Vollstreckungsgerichte war möglich geworden, nachdem im Jahre 1998 die frühere Höchstfrist einer Sicherungsverwahrung von zehn Jahren gestrichen worden war. Die Entfristung eröffnete die Möglichkeit, die Fortdauer der Sicherungsverwahrung auch für solche rückfallgefährdeten Straftäter anzuordnen, die ihre Straftat zu einem Zeitpunkt begangen hatten, in dem die Höchstfrist der Sicherungsverwahrung noch bei zehn Jahren lag. Da die Sicherungsverwahrung nach deutschem Recht keine Strafe, sondern eine (rein präventive) Maßregel der Besserung und Sicherung ist, gilt das strafrechtliche Rückwirkungsverbot nicht, das nur die rückwirkende Anwendung strafbegründender und strafverschärfende Gesetze verbietet (vgl. § 2 Abs. 6 StGB). Der EuGH stufte jedoch die Sicherungsverwahrung wegen ihrer ähnlichen Vollzugspraxis als „Strafe“ i. S. d. Art. 7 Abs. 1 EMRK ein (EGMR, Urteil vom 17. Dezember 2009 – 19359/04 – juris, Rn. 122). Mit Urteil

vom 4. Mai 2011 hat das BVerfG die rückwirkende Verlängerung der Sicherungsverwahrung über die frühere Zehnjahreshöchstfrist hinaus und die nachträgliche Anordnung der Sicherungsverwahrung für verfassungswidrig erklärt. Für den Zeitraum bis zu einer gesetzlichen Neuregelung der Sicherungsverwahrung hat das BVerfG vorgegeben, dass alle betroffenen Sicherungsverwahrten spätestens bis zum 31. Dezember 2011 freizulassen sind, es sei denn, der Betroffene leidet an einer psychischen Störung i. S. d. § 1 Abs. 1 Nr. 1 Therapieunterbringungsgesetz und es besteht eine hochgradige Gefahr schwerster Gewalt- oder Sexualstraftaten (BVerfG, Urteil vom 4. Mai 2011 – 2 BvR 2333/08 u. a.). Soweit in Folge dieser Rechtsprechung rückfallgefährdete Sexual- und Gewaltstraftäter trotz hohen Gefährdungspotenzials freigelassen werden mussten, wurden diese Personen monatelang – teilweise jahrelang – rund um die Uhr von Polizeibeamten außerhalb ihrer Wohnung offen überwacht. Durch die lückenlose Überwachung sollte der Betroffene von der Begehung weiterer schwerer Straftaten abgehalten werden. Sofern er dennoch dazu angesetzt hätte, hätte die Polizei die Tat durch sofortiges Einschreiten verhindern können. Ob die offene Dauerobservation in Fällen dieser Art auf Regelungen zur längerfristigen Observation, soweit diese auch die offene Überwachung erlauben, oder auf die polizeiliche Generalklausel gestützt werden kann, war Gegenstand mehrerer Gerichtsverfahren. Ohne Zweifel stellt eine langfristige offene Dauerüberwachung rund um die Uhr einen schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht des Betroffenen dar, denn wer ständig von Polizeibeamten beobachtet wird, hat kaum noch die Möglichkeit, ein selbstbestimmtes und eigenverantwortliches Leben zu führen. Gleichzeitig ist hiermit eine Stigmatisierung und soziale Ausgrenzung verbunden, die einer Resozialisierung wenig förderlich sind (BVerfG, Beschluss vom 8. November 2011 – 1 BvR 22/12 – juris, Rn. 23; OVG NRW, Urteil vom 5. Juni 2013 – 5 A 607/11 – juris, Rn. 85 ff.; OVG Saarland, Urteil vom 6. September 2013 – 3 A 13/13 – juris, Rn. 60; VG Freiburg, Urteil vom 14. Februar 2013 – 4 K 1115/12 – juris, Rn. 36; Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 383, Rn. 279). Teilweise gingen die Gerichte davon aus, dass die Maßnahme auf die Regelung der jeweiligen Polizeigesetze zur längerfristigen Observation gestützt werden kann (VG Saarlouis, Urteil vom 28. November 2012 – 6 K 745/10 – juris, Rn. 20 ff.; VG Aachen, Urteil vom 24. Januar 2011 – 6 K 140/10 – juris, Rn. 51). Die obergerichtliche Rechtsprechung sah dies jedoch anders und verwies darauf, dass die längerfristige Observation eine andere, mit der Dauerüberwachung rückfallgefährdeter Straftäter nicht vergleichbare Zielrichtung habe und auch aus verfassungsrechtlichen Gründen nicht ausreiche (OVG NRW, Urteil vom 5. Juni 2013 – 5 A 607/11 – juris, Rn. 66 ff.; OVG Saarland, Urteil vom 6. September 2013 – 3 A 13/13 – juris, Rn. 38 ff.). Die längerfristige Observation diene der Datenerhebung über eine bestimmte Person und sei mit einem Eingriff in das Recht auf informationelle Selbstbestimmung verbunden. Demgegenüber gehe es bei der offenen Dauerobservation im Schwerpunkt nicht um Datenerhebung –

diese sei nur eine Begleiterscheinung der Observation –, sondern um die Verhinderung schwerer Straftaten, deren Durchführung dem Betroffenen angesichts der Dauerpräsenz von Polizeibeamten als aussichtlos erscheinen soll. Diese Art der Dauerüberwachung stelle vorrangig einen Eingriff in das allgemeine Persönlichkeitsrecht dar (OVG NRW, Urteil vom 5. Juni 2013 – 5 A 607/11 – juris, Rn. 75, 85.; OVG Saarland, Urteil vom 6. September 2013 – 3 A 13/13 – juris, Rn. 56 ff.). Letztlich kommen die Gerichte zu dem Schluss, dass es sich bei der längerfristigen Überwachung gefährlicher Sexual- oder Gewaltstraftäter um eine neue Form einer polizeilichen Maßnahme handelt, die aufgrund ihrer gravierenden Folgen für den Betroffenen einer ausdrücklichen, bereichsspezifischen Ermächtigungsgrundlage bedürfe (OVG NRW, Urteil vom 5. Juni – 5 A 607/11 – juris, Rn. 93; OVG Saarland, Urteil vom 6. September 2013 – 3 A 13/13 – juris, Rn. 72). Deshalb sei auch die polizeiliche Generalklausel grundsätzlich nicht geeignet, solche Maßnahmen zu rechtfertigen. Angesichts des Gewichts der in Frage stehenden Rechtsgüter gingen die Gerichte jedoch davon aus, dass die polizeiliche Generalklausel zur Vermeidung gravierender Schutzlücken übergangsweise eine tragfähige Grundlage der Dauerüberwachung darstelle (OVG NRW, Urteil vom 5. Juni 2013 – 5 A 607/11 – juris, Rn. 97 ff.; OVG Saarland, Urteil vom 6. September 2013 – 3 A 13/13 – juris, Rn. 75 ff.). Dies ist vom BVerfG in Bezug auf eine Entscheidung des VGH Baden-Württemberg vom 8. November 2011 (1 S 2538/11) nicht beanstandet worden. Bei strenger Beachtung der Verhältnismäßigkeitsanforderungen dürfe – so das BVerfG – die an sich nicht ausreichende polizeiliche Generalklausel bei unvorhergesehenen Gefahrensituationen vorläufig zur Anwendung kommen. Es liege dann „in der Verantwortung des Gesetzgebers hierauf zu reagieren oder in Kauf zu nehmen, dass solche Maßnahmen von den Gerichten auf Dauer als von der geltenden Rechtslage nicht als gedeckt angesehen werden“ (BVerfG, Beschluss vom 8. November 2012 – 1 BvR 22/12 – juris, Rn. 25). Dementsprechend hat das VG Freiburg entschieden, dass die polizeiliche Generalklausel die Dauerüberwachung jedenfalls nach mehr als zweieinhalb Jahren, die der Gesetzgeber ungenutzt hat verstreichen lassen, nicht mehr rechtfertigen kann (VG Freiburg, Urteil vom 14. Februar 2013 – 4 K 1115/12 – juris, Rn. 37 ff.). In Hamburg ist für die polizeiliche Begleitung gefährlicher Sexual- oder Gewaltstraftäter in § 12c SOG HH eine Rechtsgrundlage geschaffen worden.

2. Abs. 2 Nr. 2 regelt den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen. Verdeckt ist ihr Einsatz, wenn die Verwendung der technischen Mittel bewusst verschleiert wird und für den Betroffenen nicht erkennbar sein soll. Der verdeckte Einsatz technischer Mittel ist auf der Grundlage des § 28 POG nur außerhalb von durch Art. 13 Abs. 1 GG geschützten Wohnungen zulässig (z. B. in einem Pkw). Sollen durch den verdeckten Einsatz technischer Mittel Daten in oder aus Wohnungen erhoben werden, müssen die Voraussetzungen des § 29 POG erfüllt sein.

3. Abs. 2 Nr. 3 erlaubt den verdeckten Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes außerhalb von Wohnungen. Die Zulässigkeit der akustischen Wohnraumüberwachung richtet sich nach § 29 POG.

4. Abs. 2 Nr. 4 nennt als besonderes Mittel der verdeckten Datenerhebung den Einsatz eines **verdeckten Ermittlers** und definiert diesen als Polizeibeamten, der unter einer ihm auf Dauer angelegten Legende ermittelt.

a) Die Begriffsbestimmung orientiert sich an § 110a Abs. 2 StPO (LT-Drs. 14/2287, S. 44). Unter einer Legende versteht man eine zu Tarnungszwecken auf Dauer angelegte, veränderte Identität eines Beamten des Polizeidienstes. Name, Anschrift, Beruf, familiäre und persönliche Umstände des Beamten werden durch erfundene Angaben ersetzt, damit er unter Täuschung über seine wahre Identität verdeckt ermitteln kann (Meyer-Goßner, StPO, § 110a Rn. 7). Dass der Staat sich der Methode der Täuschung bedienen darf, ist in einem freiheitlich-demokratisch geprägten Land nicht selbstverständlich, zur Bekämpfung gefährlicher und schwer aufklärbarer Kriminalität aber teilweise unumgänglich, da anderenfalls der staatliche Auftrag zur Gefahrenabwehr oder Strafverfolgung nicht erfüllt werden könnte. Insbesondere in konspirativ agierenden Kreisen der Organisierten Kriminalität oder des internationalen Terrorismus können Ermittlungsmethoden erforderlich sein, „die es erlauben, in das Innere der kriminellen Organisationen einzudringen“ (BT-Drs. 12/989, S. 41). Im Strafverfahrensrecht sind verdeckte Ermittler und Vertrauenspersonen schon seit Mitte der 1980iger Jahre Gegenstand gemeinsamer Richtlinien der Justiz- und Innenminister des Bundes und der Länder (vgl. Anlage D zur RiStBV; abgedruckt bei Meyer-Goßner, StPO). Bereits vor Einführung des § 110a StPO durch Gesetz vom 15. Juli 1992 (BGBl. I S. 1302) war höchstrichterlich anerkannt, dass die Polizei unter bestimmten Voraussetzungen verdeckte Ermittler einsetzen darf (vgl. BVerfG, Beschluss vom 11. April 1991 – 2 BvR 196/91). Keinesfalls aber dürfen durch deren Einsatz rechtsstaatliche Prinzipien missachtet werden (Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 373 f., Rn. 251). Straftaten darf ein verdeckter Ermittler grundsätzlich nicht begehen, auch nicht sog. milieubedingte (Frister, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 702, Rn. 335; Meyer-Goßner, StPO, § 110c Rn. 4). Zulässig ist aber die Vortäuschung der Begehung von Straftaten (OLG Zweibrücken, Beschluss vom 26. Mai 2010 – 1 Ws 241/09 – juris, Rn. 45).

b) Nicht jeder verdeckt operierende Polizeibeamter, selbst wenn er einen falschen Namen verwendet, ist ein verdeckter Ermittler im Sinne des § 28 Abs. 2 Nr. 4 POG. Maßgeblich ist, ob er unter einer auf Dauer angelegten Legende agiert. Dies ist der Fall, wenn sein Ermittlungsauftrag über wenige, konkret bestimmte Ermittlungshandlungen hinausgeht, mit der Folge, dass eine unbestimmte Vielzahl von Personen über die Identität des Beamten getäuscht wird.

Ferner muss von vornherein absehbar sein, dass der Schutz des Beamten seine Geheimhaltung auch für die Zukunft erfordert (BGH, Urteil vom 6. Februar 1997 – 1 StR 527/96 – juris, Rn. 10). Polizeibeamte, die etwa nur gelegentlich als Scheinaufkäufer von Betäubungsmitteln auftreten, sind danach keine verdeckten Ermittler (BGH, Urteil vom 6. Februar 1997 – 1 StR 527/96 – juris, Rn. 11). Auch verdeckt im Internet – etwa in Chatrooms – ermittelnde Polizeibeamte sind keine verdeckten Ermittler (Meyer-Goßner, StPO, § 110a Rn. 4). Die Vorgaben für den Einsatz verdeckter Ermittler, insbesondere der Richtervorbehalt in § 28 Abs. 4 Satz 1 Nr. 3 POG, gelten für nicht offen ermittelnde Polizeibeamte, die keine verdeckten Ermittler sind, nicht.

5. Abs. 2 Nr. 5 erlaubt den Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist (**Vertrauenspersonen**). Vertrauenspersonen, die man salopp auch als „Polizeispitzel" bezeichnen könnte, sind Privatpersonen (also keine Polizeibeamte), die die Polizei bei der vorbeugenden Bekämpfung von Straftaten unterstützen. Häufig stammen Vertrauenspersonen aus demselben Milieu, in dem sie von der Polizei eingesetzt werden. Grund für eine Zusammenarbeit mit der Polizei dürften nicht zuletzt finanzielle Erwägungen sein, denn die Vertrauenspersonen werden in der Regel für ihre Dienste entlohnt (Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 378, Rn. 266). Obwohl Vertrauenspersonen offen agieren, handelt es sich um eine verdeckte Ermittlungsmethode, weil die Vertrauensperson Informationen über Personen sammelt, denen nicht bekannt ist, dass diese mit der Polizei zusammenarbeitet. Die Bezeichnung als „Vertrauensperson" meint nicht, dass die Person besonders vertrauenswürdig ist, sondern bezieht sich auf die Vertraulichkeit der Zusammenarbeit mit der Polizei, die Dritten gegenüber geheim gehalten wird (Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 379, Rn. 262).

Keine Vertrauenspersonen sind bloße Hinweisgeber oder polizeiliche Informanten. Im Unterschied zu Vertrauenspersonen werden diese Personen von der Polizei nicht zielgerichtet eingesetzt, um zu einem näher beschriebenen Ermittlungsauftrag zu berichten. Teilweise sind die Grenzen zwischen Informanten und Vertrauenspersonen fließend. Die bloße Bitte, „Augen und Ohren offen zu halten" dürfte noch nicht als zielgerichteter Einsatz gewertet werden (Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 378, Rn. 264).

6. Abs. 2 Nr. 6 erlaubt die Standortfeststellung einer Person oder eines Fahrzeugs durch den Einsatz technischer Mittel. Für Standortermittlungen eines Mobiltelefons oder eines sonstigen Telekommunikationsendgeräts gilt § 31a POG als speziellere Vorschrift. Technische Mittel, die für eine Standortfeststellung nach § 28 POG in Betracht kommen, sind insbesondere der herkömmliche Peilsender und das satellitengestützte Navigationssystem „Global Positioning

System“ (GPS). Als Beispiel für den Einsatz solcher Mittel nennt die Gesetzesbegründung die entsprechende Präparation von Fluchtfahrzeugen bei Geiselnahmen. Damit könne die mit einer klassischen Observation durch Nachfahren verbundene Gefährdung der Geiseln vermindert werden (LT-Drs. 14/2287, S. 44). Die für den Einsatz des technischen Mittels notwendigen Begleitmaßnahmen – wie etwa das heimliche Öffnen eines Fahrzeugs oder seine kurzzeitige Verbringung in eine Werkstatt – sind unter Beachtung des Verhältnismäßigkeitsgrundsatzes im Wege der Annexkompetenz von § 28 POG abgedeckt (BGH, Urteil vom 24. Januar – 3 StR 324/00 – juris, Rn. 18 zu § 100c StPO a. F.).

IV. Straftaten von erheblicher Bedeutung (Abs. 3)

Abs. 3 benennt Straftaten, die von erheblicher Bedeutung sind. Hierzu gehören alle Verbrechen, d. h. alle Straftaten, die im Mindestmaß mit Freiheitsstrafe von einem Jahr oder darüber bedroht sind (§ 12 Abs. 1 StGB) und Vergehen, die nicht als einzelne Straftatbestände, sondern wie in § 98a und § 110a StPO generalisierend benannt werden. Vergehen sind danach Straftaten von erheblicher Bedeutung, wenn sie im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören und unter die in den Buchstaben a) bis c) genannten Fallgruppen fallen. Sie müssen sich entweder gegen hochrangige Rechtsgüter richten, bestimmten Deliktsbereichen angehören (unerlaubter Waffen- oder Betäubungsmittelverkehr, Geld- und Wertzeichenfälschung, Staatsschutzdelikte) oder gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangen werden. Trotz dieser gesetzlichen Vorgaben können im Einzelfall Unsicherheiten bestehen, ob ein Vergehen im Einzelfall von erheblicher Bedeutung ist oder nicht. Insbesondere ist unklar, was unter der „Eignung zur besonderen Störung des Rechtsfriedens“ zu verstehen ist und welche eigenständige Bedeutung diesem Merkmal neben den genannten Fallgruppen zukommen soll. So dürften die unter den Buchstaben a) bis c) genannten Fallgruppen gerade solche sein, die regelmäßig mit einer Eignung zur besonderen Störung des Rechtsfriedens einhergehen.

V. Richtervorbehalt, Befristung der Maßnahme (Abs. 4)

1. Durch das Gesetz vom 30. Juni 2017 (GVBl. S. 123) ist in Umsetzung des Urteils des BVerfG vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – ein Richtervorbehalt für alle eingriffsintensiven besonderen Mittel der verdeckten Datenerhebung eingeführt worden. Nach bisheriger Rechtslage stand die längerfristige Observation nicht unter Richtervorbehalt. Der verdeckte Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen sowie der Einsatz von verdeckten Ermittlern und Vertrauenspersonen bedurfte nur dann einer richterlichen Entscheidung, wenn die Maßnahme länger als sieben Tage durchgeführt werden sollte oder durchgeführt wurde. Das BVerfG hat mit Blick auf

das Eingriffsgewicht dieser Maßnahmen entschieden, dass bereits die erstmalige Anordnung einer längerfristigen Observation, das Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes und der Einsatz von verdeckten Ermittlern oder Vertrauenspersonen einer richterlichen Entscheidung bedarf (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 174).

2. Nach **Abs. 4 Satz 1 Nr. 1 bis 3** stehen nunmehr folgende Mittel der verdeckten Datenerhebung bereits vor ihrer erstmaligen Anordnung unter Richtervorbehalt:

- die längerfristige Observation (Nr. 1),
- der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen, soweit Bildaufzeichnungen bestimmter Personen durchgehend länger als 24 Stunden oder über einen Zeitraum von mehr als einer Woche angefertigt werden sollen (Nr. 2), sowie
- der verdeckte Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes, der Einsatz verdeckter Ermittler und der Einsatz von Vertrauenspersonen (Nr. 3).

Für kurzfristige verdeckte Bildaufzeichnungen sowie den Einsatz technischer Mittel zur Feststellung des jeweiligen Standorts einer Person oder eines Fahrzeugs gilt nach Abs. 5 ein Behördenleitervorbehalt. Warum der Gesetzgeber für längerfristige Bildaufzeichnungen in Abs. 4 Satz 1 Nr. 2 explizit einen Richtervorbehalt vorgesehen hat, erschließt sich nicht unmittelbar. Bildaufzeichnungen, die durchgehend länger als 24 Stunden oder über einen Zeitraum von mehr als einer Woche angefertigt werden sollen, gehen zwangsläufig mit einer längerfristigen Observation einher, für die bereits nach Abs. 4 Satz 1 Nr. 1 ein Richtervorbehalt gilt.

3. Nach **Abs. 4 Satz 2** ist die Maßnahme zu befristen. Während die Anordnung einer längerfristigen Observation und der Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen auf höchstens einen Monat zu befristen ist, gilt für den Einsatz von verdeckten Ermittlern und Vertrauenspersonen eine Höchstfrist von drei Monaten. Nach **Abs. 4 Satz 3** ist eine Verlängerung um jeweils nicht mehr als denselben Zeitraum zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen. Eine zeitliche Obergrenze für die Verlängerung der Maßnahme ist gesetzlich nicht festgelegt. Diese kann sich aber aus dem Grundsatz der Verhältnismäßigkeit ergeben, da das Eingriffsgewicht mit zunehmender Dauer der Überwachungsmaßnahmen intensiver wird und schließlich dazu führen kann, dass eine weitere Verlängerung verfassungsrechtlich unzulässig ist (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 171).

4. Nach **Abs. 4 Satz 4** ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat, für die Entscheidung über die Anordnung zuständig. Durch den Verweis in **Abs. 4 Satz 5** auf § 21 Abs. 1 Satz 3 POG werden für das Verfahren vor dem Amtsgericht die Bestimmungen des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit für entsprechend anwendbar erklärt. Bei Gefahr im Verzug kann die Maßnahme gem. **Abs. 4 Satz 6** vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten mit der Befähigung für das vierte Einstiegsamt angeordnet werden; die richterliche Entscheidung ist dann unverzüglich nachzuholen.

VI. Behördenleitervorbehalt, Befristung der Maßnahme (Abs. 5)

1. Abs. 5 Satz 1 regelt die Anordnungskompetenz für den Einsatz besonderer Mittel, die kein so schwerwiegendes Eingriffsgewicht haben, dass ihre Anordnung durch einen Richter verfassungsrechtlich geboten ist. Hierbei handelt es sich zum einen um Bildaufzeichnungen, die nur für einen kürzeren Zeitraum angefertigt sollen, d. h. durchgehend für weniger als 24 Stunden oder nicht länger als eine Woche. Zum anderen geht es um den Einsatz technischer Mittel zur Feststellung des jeweiligen Standorts einer Person oder eines Fahrzeugs. In Fällen dieser Art kann die Maßnahme durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten mit der Befähigung für das vierte Einstiegsamt angeordnet werden.

2. Nach **Abs. 5 Satz 2** ist die Maßnahme zu befristen und kann wiederholt angeordnet werden. Zwar ist keine zulässige Höchstfrist vorgegeben, im Hinblick auf die Anordnung von verdeckten Bildaufzeichnungen darf die Maßnahme aber nicht für einen durchgehenden Zeitraum von länger als 24 Stunden oder für einen Zeitraum von mehr als einer Woche angeordnet werden, weil dann nach Abs. 4 Satz 1 Nr. 2 ein Richtervorbehalt besteht. Bei Gefahr im Verzug können die genannten Mittel gem. **Abs. 5 Satz 3** vorläufig eingesetzt werden. Eine Entscheidung der Behördenleitung bzw. eines besonders beauftragten Beamten mit der Befähigung für das vierte Einstiegsamt ist unverzüglich nachzuholen.

VII. Kennzeichnung, Zweckänderung bei Daten aus eingriffsintensiven besonderen Mitteln (Abs. 6)

1. Abs. 6 Satz 1 enthält Vorgaben zur Kennzeichnung personenbezogener Daten, die aus den eingriffsintensiven Maßnahmen nach Abs. 2 Nr. 1, 3 bis 5 erlangt worden sind. Hierdurch wird sichergestellt, dass der Grundsatz der Zweckbindung und die Grenzen einer zulässigen Zweckänderung gewahrt werden. Dies ist nur möglich, wenn nach der Datenerhebung erkennbar bleibt, mittels welcher Maßnahmen die Daten erlangt wurden. Dementsprechend ist die

Kennzeichnung gem. **Abs. 6 Satz 2** auch nach einer Übermittlung durch die Empfänger der Daten aufrechtzuerhalten.

2. Abs. 6 Satz 3 regelt die Voraussetzungen für eine zulässige zweckändernde Verwendung der aus den eingriffsintensiven Maßnahmen nach Abs. 2 Nr. 1, 3 bis 5 erlangten Daten. Dabei handelt es sich um Daten, die aus einer längerfristigen Observation (Abs. 2 Nr. 1), dem verdeckten Einsatz technischer Mittel zum Abhören und Aufzeichnungen des nicht öffentlich gesprochenen Wortes (Abs. 2 Nr. 3), dem Einsatz verdeckter Ermittler (Abs. 2 Nr. 4) oder dem Einsatz von Vertrauenspersonen (Abs. 2 Nr. 5) stammen.

a) Nach dem Grundsatz der Zweckbindung gilt, dass Daten nur für den Zweck verwendet werden dürfen, zu dem sie erhoben worden sind. Allerdings kann eine weitere Nutzung der Daten zu anderen Zwecken als denen der ursprünglichen Datenerhebung gesetzlich erlaubt werden, wenn dem Eingriffsgewicht der Datenerhebung auch hinsichtlich der neuen Nutzung Rechnung getragen wird (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 284). Ursprünglich hat das BVerfG die Frage der Verhältnismäßigkeit und damit die Zulässigkeit einer Zweckänderung danach beurteilt, ob die geänderte Nutzung mit der ursprünglichen Zwecksetzung „vereinbar" ist (vgl. BVerfG, Urteil vom 3. März 2004 – 1 BvR 2378/98, 1 BvR 1084/99 – juris, Rn. 345). Inzwischen stellt das BVerfG auf das Kriterium der **hypothetischen Datenneuerhebung** ab. Danach ist eine Zweckänderung zulässig, wenn die neue Nutzung der Daten zum Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 288). Allerdings wendet das BVerfG das Kriterium der hypothetischen Datenneuerhebung in seiner Entscheidung zum Bundeskriminalamtgesetz nicht strikt an, sondern lässt gewisse Abstriche hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts zu. Ausreichend für eine weitere Nutzung der Daten zu geänderten Zwecken ist, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 289). Der Gesetzgeber kann eine Zweckänderung daher bereits dann zulassen, wenn sich aus den erhobenen Daten Informationen ergeben, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 290). Den Begriff des „konkreten Ermittlungsansatzes" führt das BVerfG nicht näher aus. Gemeint sein dürften damit tatsächliche Anhaltspunkte für begangene Straftaten oder drohende Gefahren, die sich zumindest in Umrissen konkretisieren lassen.

Etwas anderes gilt für Daten aus einer Wohnraumüberwachung oder einer Onlinedurchsuchung. Wegen des besonderen Eingriffsgewichts dieser Maßnahmen ist eine zweckändernde Nutzung der gewonnenen Daten hier nur zulässig, wenn dies zur Abwehr einer dringenden Gefahr oder einer im Einzelfall hinreichend konkretisierten Gefahr für die jeweils maßgeblichen Rechtsgüter erforderlich ist (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 291).

b) Abs. 6 Satz 3 setzt die verfassungsrechtlichen Anforderungen an eine zulässige Zweckänderung um. So dürfen die Daten für einen anderen Zweck nur verwendet werden, wenn sich aus ihnen konkrete Ermittlungsansätze zur Verfolgung oder Verhütung von Straftaten von erheblicher Bedeutung (Nr. 1) oder zur Abwehr einer Gefahr für Leib oder Leben einer Person (Nr. 2) ergeben und die Verwendung der Daten zu diesem Zweck erforderlich ist. Die Zulässigkeit einer Zweckänderung zur Verfolgung oder Verhütung von Straftaten von erheblicher Bedeutung entspricht dem Kriterium der hypothetischen Datenneuerhebung, da die zweckändernde Nutzung der Daten wie die Datenerhebung an Straftaten von erheblicher Bedeutung ausgerichtet ist. Gleichzeitig gewährleistet die Regelung, dass nur solche Daten zu Zwecken der Strafverfolgung oder Straftatenverhütung verwendet werden dürfen, die konkrete Ermittlungsansätze zur Aufdeckung oder Verhütung der Straftaten erkennen lassen (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 289 f.). Eine zweckändernde Nutzung der Daten zur Abwehr einer Gefahr für Leib oder Leben einer Person ist mit dem Kriterium der hypothetischen Datenneuerhebung ebenfalls vereinbar, da es insoweit um die Abwehr von Gefahren für hochrangige Rechtsgüter geht, zu deren Schutz eine Neuerhebung mit vergleichbar schwerwiegenden Mitteln zulässig wäre.

c) Damit die Zweckänderung nachvollziehbar ist und ihre Zulässigkeit gegebenenfalls überprüft werden kann, muss sie nach **Abs. 6 Satz 4** im Einzelfall festgestellt und dokumentiert werden.

VIII. Zweckänderung bei Daten aus weniger eingriffsintensiven besonderen Mitteln (Abs. 7)

1. Abs. 7 Satz 1 regelt die zweckändernde Nutzung von Daten, die durch die weniger gewichtigen Eingriffe nach Abs. 2 Nr. 2 und 6 erlangt wurden, d. h. durch den verdeckten Einsatz zur Anfertigung von Bildaufzeichnungen (Abs. 2 Nr. 2) oder zur Feststellung des jeweiligen Standortes einer Person oder eines Fahrzeugs (Abs. 2 Nr. 6). Soweit die Maßnahmen allerdings im Rahmen einer längerfristigen Observation nach Abs. 2 Nr. 1 zum Einsatz gekommen sind, richtet sich die Zulässigkeit einer Zweckänderung nach Abs. 6 Satz 3. Die Daten

sind dann durch eine eingriffsintensive Maßnahme gewonnen worden und dürfen nur unter den Voraussetzungen des Abs. 6 Satz 3 zweckändernd weiterverwendet werden. Eine Zweckänderung ist nach Abs. 7 Satz 1 unter im Vergleich zu Abs. 6 Satz 3 erleichterten Voraussetzungen zugelassen. Zwar kommt eine Zweckänderung auch hier nur in Betracht, wenn die erlangten Daten zur Verfolgung oder Verhütung von Straftaten von erheblicher Bedeutung oder zur Abwehr einer Gefahr für Leib oder Leben einer Person erforderlich sind. Im Unterschied zur Abs. 6 Satz 3 müssen sich aus den Daten aber noch keine konkreten Ermittlungsansätze im Sinne von tatsächlichen Anhaltspunkten für begangene Straftaten oder drohende Gefahren ergeben haben. Da eine Datennutzung „ins Blaue hinein" jedoch grundsätzlich unzulässig ist, müssen hier zumindest Ansätze vorliegen, die eine weitere Sachverhaltsaufklärung rechtfertigen können. Die weitere Sachverhaltsaufklärung kann dann dazu dienen, konkrete Anhaltspunkte im Sinne eines konkreten Ermittlungsansatzes für begangene Straftaten von erheblicher Bedeutung oder drohende Gefahren für Leib oder Leben einer Person zu gewinnen.

2. Nach **Abs. 7 Satz 2** muss die Zweckänderung der Daten im Einzelfall festgestellt und dokumentiert werden.

IX. Geheimhaltung der Identität eines verdeckten Ermittlers oder einer Vertrauensperson; Befugnisse des verdeckten Ermittlers (Abs. 8)

1. Abs. 8 Satz 1 enthält eine Ermächtigung zur Herstellung, Veränderung und zum Gebrauchen der für den Aufbau und die Aufrechterhaltung der Legende erforderlichen Urkunden (z. B. Personalausweis, Führerschein, Kreditkarte). Der verdeckte Ermittler darf zur Erfüllung seines Auftrags nach **Satz 2** unter Geheimhaltung seiner Identität am Rechtsverkehr teilnehmen. Demnach darf er unter seiner Legende Verträge jeglicher Art abschließen, z. B. eine Wohnung mieten, heiraten, einen Kredit aufnehmen oder ein Auto kaufen, ohne dabei Gefahr zu laufen, sich wegen Urkundenfälschung strafbar zu machen. Ebenfalls kann er unter seiner Legende klagen oder verklagt werden.

2. Satz 2 ermächtigt den verdeckten Ermittler außerdem, unter Geheimhaltung seiner Identität mit Einverständnis des Berechtigten dessen Wohnung zu betreten. Soweit durch diese Vorschrift eine Strafbarkeit wegen Hausfriedensbruch ausgeschlossen werden soll, ist die Regelung rein deklaratorischer Natur, denn ein Hausfriedensbruch ist wegen des Einverständnisses des Hausrechtsinhabers tatbestandlich ohnehin ausgeschlossen. Daran ändert auch der Umstand nichts, dass das Einverständnis durch Täuschung über die wahre Identität des verdeckten Ermittlers erschlichen wurde (vgl. Lenckner, in: Schönke/Schröder, StGB, § 123 Rn. 22). Er darf das Einverständnis aber nur dadurch herbeiführen, dass er seine Legende nutzt und sich nicht als Polizeibeamter zu erkennen gibt. Eine

darüber hinausgehende Täuschung ist ihm nicht gestattet. Dies stellt Satz 2 explizit klar, indem es heißt, dass der verdeckte Ermittler die Wohnung nicht unter Vortäuschung eines Zutrittsrechts betreten darf. Er darf sich also z. B. nicht als Hausmeister oder Schornsteinfeger ausgeben, um sich hierdurch Zugang zu einer Wohnung zu verschaffen.

2. Verdeckte Ermittler sind Polizeibeamte, für die, auch wenn sie unter einer Legende ermitteln, der Gesetzesvorbehalt gilt. Deshalb haben sie auch als verdeckte Ermittler nur die Befugnisse, die sich aus dem Polizei- und Ordnungsbehördengesetz, der Strafprozessordnung oder aus sonstigen Gesetzen ergeben. Soweit die Befugnisse nur zu einem offenen Eingreifen ermächtigen – wie etwa bei einer Festnahme oder Sicherstellung – darf auch der verdeckte Ermittler hiervon nur offen Gebrauch machen. De facto bedeutet dies, dass der verdeckte Ermittler von diesen Befugnissen keinen Gebrauch machen wird, denn würde er sich als Polizeibeamter zu erkennen geben, könnte er anschließend nicht mehr unter seiner Legende weiter ermitteln. Außerdem könnte eine Enttarnung mit einer erheblichen Eigengefährdung verbunden sein.

3. Informationen erlangen verdeckte Ermittler nicht nur durch Beobachten und Zuhören, sondern auch durch gezielte Befragungen. Es liegt auf der Hand, dass sie den Befragten nicht gem. § 9a Abs. 3 Satz 4 POG über ein gegebenenfalls bestehendes Auskunftsverweigerungsrecht belehren können. Entsprechendes gilt, wenn verdeckte Ermittler strafverfolgend tätig sind und Tatverdächtige ausfragen. Belehrungspflichten stehen der Ausforschung von Personen durch verdeckte Ermittler aber nicht entgegen, weil die Vorschriften hier nicht anwendbar sind. Belehrungen über ein Auskunftsverweigerungsrecht sollen den zu Befragenden vor der irrtümlichen Annahme bewahren, dass er zur Aussage verpflichtet sei. Niemand würde aber auf die Idee kommen, dass er gegenüber einer Privatperson zu einer Aussage verpflichtet ist. Belehrungspflichten setzen nach ihrer ratio legis deshalb voraus, dass der Fragende dem Befragten in amtlicher Funktion gegenübertritt (Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 359 f., Rn. 202). Verdeckte Ermittler treten aber gerade nicht als Amtsperson auf. Unter Umständen kann sich für solchermaßen erlangte Erkenntnisse allerdings ein Beweisverwertungsverbot in einem Strafverfahren ergeben (vgl. BGH, Urteil vom 26. Juli 2007 – 3 StR 104/07, der ein Beweisverwertungsverbot annimmt, wenn ein verdeckter Ermittler einer Person unter Ausnutzung eines geschaffenen Vertrauensverhältnisses durch beharrliche Fragen Äußerungen entlockt, zu denen der Befragte bei einer förmlichen Vernehmung nicht bereit gewesen wäre).

4. Verdeckte Ermittler, die zum Zwecke der Gefahrenabwehr oder zur vorbeugenden Bekämpfung von Straftaten in ein kriminelles Milieu eingeschleust werden, werden bei Gelegenheit ihres Einsatzes häufig auch Informationen erlangen, die den Anfangsverdacht einer Straftat begründen. Denkbar ist auch, dass

sie selbst Zeugen einer gerade stattfindenden Straftat werden. Als Polizeibeamte unterliegen sie dem Legalitätsprinzip und sind gem. § 163 Abs. 1 Satz 1 StPO grundsätzlich zur Strafverfolgung verpflichtet (vgl. Nr. 2.6 der gemeinsamen Richtlinien der Justiz- und Innenminister des Bundes und der Länder, Anlage D zur RiStBV; abgedruckt bei Meyer-Goßner, StPO). Ein Verstoß gegen das Legalitätsprinzip kann eine Strafbarkeit wegen Strafvereitelung im Amt durch Unterlassen (§§ 258, 13 StGB) zur Folge haben. Allerdings braucht der verdeckte Ermittler nach der Nr. 2.6.2 der gemeinsamen Richtlinien der Justiz- und Innenminister des Bundes und der Länder einem Anfangsverdacht einer Straftat solange nicht nachzugehen, als dies ohne Gefährdung seiner Ermittlungen nicht möglich ist. Einzelne Ermittlungshandlungen können hier deshalb zurückgestellt werden. Dies gilt jedoch nicht, wenn sofortige Ermittlungsmaßnahmen wegen der Schwere der neu entdeckten Tat geboten sind.

5. Wird der verdeckte Ermittler Zeuge einer Straftat und verhindert er sie nicht, obwohl er es könnte, stellt sich die Frage, ob er sich durch Unterlassen an der Straftat beteiligt und damit ebenfalls strafbar macht (vgl. zu dieser Problematik Krey, Rechtsprobleme des strafprozessualen Einsatzes verdeckter Ermittler, 1993, Rn. 503 f.).

6. Die wahre Identität des verdeckten Ermittlers kann gem. § 110b Abs. 3 Satz 3 StPO durch eine Sperrerklärung des Innenministers nach § 96 StPO in einem Strafverfahren geheim gehalten werden. Zulässig ist die Geheimhaltung nach § 110b Abs. 3 Satz 3 StPO insbesondere, wenn Anlass zu der Besorgnis besteht, dass die Offenbarung Leben, Leib oder Freiheit des verdeckten Ermittlers oder einer anderen Person oder die Möglichkeit der weiteren Verwendung des verdeckten Ermittlers gefährden würde. Unter entsprechender Anwendung des § 96 StPO können auch Vertrauenspersonen gesperrt werden.

7. Soweit es zur Geheimhaltung der Zusammenarbeit einer Vertrauensperson mit der Polizei erforderlich ist, gilt nach **Abs. 8 Satz 3** die Regelung in Abs. 8 Satz 1 entsprechend. Zum Zwecke der Geheimhaltung der Zusammenarbeit mit der Polizei dürfen demnach Urkunden hergestellt, verändert oder gebraucht werden. Im Unterschied zum verdeckten Ermittler darf die Vertrauensperson aber nicht mit diesen Urkunden am Rechtsverkehr teilnehmen.

§ 38
Besondere Formen des Datenabgleichs

(1) Die Polizei kann von öffentlichen und nicht öffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist.

(2) Die Übermittlung ist auf Namen, Anschrift, Tag und Ort der Geburt der betreffenden Personen sowie auf im Einzelfall festzulegende Merkmale zu beschränken. Ist ein Aussondern der zu übermittelnden personenbezogenen Daten nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, so dürfen die weiteren Daten ebenfalls übermittelt werden. Eine Verwendung dieser weiteren Daten ist unzulässig.

(3) Die Maßnahme bedarf der richterlichen Entscheidung. Zuständiges Gericht ist das Oberverwaltungsgericht Rheinland-Pfalz. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist unverzüglich zu unterrichten. Bei Gefahr im Verzug kann die Maßnahme vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten mit der Befähigung für das vierte Einstiegsamt angeordnet werden; die richterliche Entscheidung ist unverzüglich nachzuholen.

(4) Nach Absatz 1 erlangte Daten sind besonders zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch die Empfänger aufrechtzuerhalten. Solche Daten dürfen für einen anderen Zweck verwendet werden, soweit

1. **sich aus ihnen konkrete Ermittlungsansätze zur Verfolgung von Straftaten von erheblicher Bedeutung ergeben, die nach der Strafprozessordnung eine Rasterfahndung rechtfertigen,**
2. **dies zur Abwehr einer dringenden Gefahr im Sinne des Absatzes 1 erforderlich ist.**

(5) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und die im Zusammenhang mit dem Abgleich zusätzlich angefallenen Daten zu löschen und die Unterlagen zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind. Die getroffene Maßnahme ist zu dokumentieren. Diese Dokumentation ist gesondert aufzubewahren und durch organisatorische und technische Maßnahmen zu sichern. Sie ist sechs Monate nach der Benachrichtigung nach § 40 Abs. 5 zu löschen. Ist die Datenschutzkontrolle nach § 41b noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

Erläuterungen

Übersicht

I. Allgemeines

1. Entstehungsgeschichte der Vorschrift: Die Rasterfahndung wurde durch das Gesetz vom 26. März 1986 (GVBl. S. 77) als § 25d in das damalige Polizeiverwaltungsgesetz aufgenommen. Zulässig war sie nach ihrer ursprünglichen Fassung nur zur Abwehr einer gegenwärtigen erheblichen Gefahr. Unter dem Eindruck der terroristischen Anschläge vom 11. September 2001 in den USA wurde die Eingriffsschwelle durch das Gesetz vom 2. März 2004 (GVBl. S. 202) deutlich herabgesenkt. Nunmehr war eine Rasterfahndung nach § 38 POG bereits zur Abwehr einer erheblichen Gefahr oder zur vorbeugenden Bekämpfung von besonders schwerwiegenden Straftaten erlaubt. Am 4. April 2006 hat das BVerfG in einem gegen die gerichtlichen Entscheidungen über die Anordnung einer präventiv polizeilichen Rasterfahndung nach § 31 des Polizeigesetzes Nordrhein-Westfalen in der Fassung vom 24. Februar 1990 (GVBl. S. 70) gerichteten Verfassungsbeschwerde die Auslegung des Begriffs der konkreten Gefahr durch die Gerichte für verfassungswidrig erklärt. Gleichzeitig hat es ausgeführt, dass eine Rasterfahndung im Grundsatz mit dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG vereinbar ist, angesichts ihrer Eingriffsintensität aber nur zur Abwehr einer konkreten Gefahr für hochrangige Rechtsgüter verfassungsrechtlich gerechtfertigt werden kann (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02). Aus dieser Entscheidung ergab sich erneuter Änderungsbedarf für die rheinland-pfälzische Regelung, denn mit der Ermächtigung zur Durchführung einer Rasterfahndung „zur vorbeugenden Bekämpfung von besonders schwerwiegenden Straftaten“ hatte der Gesetzgeber auf das Erfordernis einer konkreten Gefahr verzichtet und die Vorschrift zu einer polizeilichen Befugnis im Vorfeld einer konkreten Gefahr ausgestaltet. Durch das Gesetz vom 15. Februar 2011 (GVBl. S. 26) wurde die Zulässigkeit einer Rasterfahndung an die verfassungsrechtlichen Anforderungen angepasst. Danach darf eine Rasterfahndung nur zur Abwehr einer konkreten Gefahr für hochrangige Rechtsgüter angeordnet werden. Durch das Gesetz vom 30. Juni 2017 (GVBl. S. 123) wurde die bisherige Zuständigkeit des Amtsgerichts für die richterliche Entscheidung in § 38 Abs. 3 Satz 2 POG

auf das OVG Rheinland-Pfalz übertragen, da es sich bei der Rasterfahndung – wie bei anderen verdeckten Überwachungsmaßnahmen, für die bereits eine Anordnungskompetenz des OVG Rheinland-Pfalz besteht – ebenfalls um eine heimliche Ermittlungsmaßnahme mit hoher Eingriffsintensität handelt (LT-Drs. 17/2895, S. 26 f.). Ferner wurde in einem neu eingefügten Abs. 4 eine Regelung zur Kennzeichnung und Zweckänderung aufgenommen, die den Anforderungen des BVerfG aus seinem Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – zum Bundeskriminalamtgesetz entspricht. Schließlich wurden in Abs. 5 die Vorgaben des BVerfG zur Aufbewahrungsfrist von Löschungsprotokollen umgesetzt (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – juris, Rn. 272 und Erl. VI.2.).

2. Folgende Grundrechte sind von § 38 POG betroffen: Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

Die Rasterfahndung greift in das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein. Dieses Recht gewährleistet die aus dem Grundsatz der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 69). Ein Eingriff in den Schutzbereich des Grundrechts liegt vor, wenn personenbezogene oder -beziehbare Daten erhoben, gesammelt, gespeichert, verwendet oder weitergegeben werden (Jarass, in: Jarass/Pieroth, GG, Art. 2 Rn. 53). Kein Eingriff liegt vor, wenn Daten lediglich technikbedingt erhoben, dann aber anonym und spurenlos wieder ausgesondert werden (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 74). Eine Rasterfahndung kann in das Recht auf informationelle Selbstbestimmung derjenigen Personen eingreifen, deren Daten an die Polizei übermittelt werden. Das BVerfG beschränkt die Eingriffsqualität hier allerdings auf die Personen, deren Daten nach einem ersten Datenabgleich noch Gegenstand weiterer, nachfolgender Maßnahmen, insbesondere weitergehender Datenabgleiche werden sollen (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 75). Nur in diesen Fällen – so das BVerfG – hat sich das behördliche Interesse an den betroffenen Daten derart verdichtet hat, dass „ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen ist" (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 74). Eingriffe in das Grundrecht auf informationelle Selbstbestimmung sind zulässig, wenn sie durch überwiegende Allgemeininteressen gerechtfertigt sind und auf einer gesetzlichen Grundlage beruhen, die dem Grundsatz der Verhältnismäßigkeit und dem Gebot der Normenklarheit entspricht (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 81). Die Rasterfahndung stellt nach Auffassung des BVerfG einen schwerwiegenden Grundrechtseingriff dar. So erlauben die bei einer Rasterfahndung übermittelten Daten durch ihre Verknüpfung mit anderen Daten persönlichkeitsbezogene Einblicke, die je nach Art und

Inhalt der übermittelten oder der anderen Daten, mit denen die übermittelten Daten abgeglichen werden, erhebliche Persönlichkeitsrelevanz besitzen können (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 99 ff.). Hinzukommt, dass die Rasterfahndung für die Betroffenen – im Falle ihres Bekanntwerdens – eine stigmatisierende Wirkung haben kann und das Risiko begründet, Ziel weiterer staatlicher Ermittlungsmaßnahmen zu werden (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 108 ff.). Schließlich handelt es sich bei der Rasterfahndung um eine Maßnahme mit erheblicher Streubreite, deren Adressaten keinen Anlass für den Eingriff gegeben haben müssen. Da mithilfe einer präventiven Rasterfahndung potenzielle Störer erst gefunden werden sollen, sind die Rasterkriterien relativ unspezifisch, sodass eine Vielzahl von Personen betroffen ist, die in keiner Beziehung zu der abzuwehrenden Gefahr steht (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 116 ff.).

3. Bedeutung der Vorschrift: Nach den Terroranschlägen vom 11. September 2001 in den USA wurde in Deutschland eine präventive Rasterfahndung nach bundesweit abgestimmten Rasterkriterien durchgeführt, nachdem bekannt geworden war, dass einige der Attentäter in Deutschland gelebt hatten. Ziel der Rasterfahndung war die Aufdeckung von Personen, die versuchen, ein möglichst unauffälliges Leben zu führen, um währenddessen terroristische Anschläge vorzubereiten (sog. Schläfer). Obwohl den Landeskriminalämtern 5,2 Millionen Datensätze übermittelt wurden, aus denen 11.004 Datensätze herausgefiltert wurden, die mit den Rasterkriterien übereinstimmten, führte die Rasterfahndung letztlich nicht zur Aufdeckung von „Schläfern“ (vgl. BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 7 ff.; BT-Drs. 14/7206).

Seit der Novellierung der rheinland-pfälzischen Vorschrift im Jahr 2004 wurde in Rheinland-Pfalz keine präventive Rasterfahndung mehr durchgeführt und, soweit ersichtlich, auch in anderen Bundesländern nicht.

II. Begriffsbestimmung

Bei einer Rasterfahndung werden von öffentlichen oder nicht öffentlichen Stellen personenbezogene Daten auf Ersuchen an die Polizei übermittelt und automatisiert mit anderen Datenbeständen abgeglichen, um bestimmte Personen zu ermitteln (Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 888, Rn. 528). Durch den Datenabgleich soll diejenige Schnittmenge von Personen ausfindig gemacht werden, auf die bestimmte, vorab festgelegte Merkmale (Rasterkriterien) zutreffen und die für die weiteren Ermittlungen als bedeutsam eingeschätzt werden (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 2). Weil die Rasterkriterien auch auf eine Vielzahl anderer nicht verantwortlicher Personen zutreffen können, ergibt sich nach der Rasterung ein Kreis von

Merkmalsträgern, aus dem der eigentliche Störer durch den Abgleich mit anderen (polizeifremden oder polizeilichen) Datenbeständen herausgefiltert werden muss. Die Auswertung der Daten ist zeitaufwändig und schwierig.

Die präventive Rasterfahndung stellt in Zeiten der Bedrohung durch den internationalen Terrorismus und durch die Erscheinungsformen der organisierten und schweren Kriminalität eine Ermittlungsmethode dar, mit der der Staat besondere Gefahrenlagen aufklären und abwehren kann. So hat das BVerfG in seiner Entscheidung zur Rasterfahndung betont, dass der Staat terroristischen Bestrebungen – etwa solchen, die die Zerstörung der freiheitlichen demokratischen Grundordnung zum Ziel haben und die planmäßige Vernichtung von Menschenleben als Mittel zur Verwirklichung dieses Vorhabens einsetzen – mit den erforderlichen rechtsstaatlichen Mitteln entgegentreten darf und muss (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 126).

III. Voraussetzungen für die Datenübermittlung (Abs. 1 und 2)

1. Nach **Abs. 1** kann die Polizei von öffentlichen und nicht öffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist. Mit einer Rasterfahndung wird notwendig der Grundsatz der Zweckbindung durchbrochen, denn die von öffentlichen oder nicht öffentlichen Stellen zu anderen Zwecken erhobenen Daten dürfen über die Rasterfahndung auch für die Gefahrenabwehr verwendet werden (Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 889, Rn. 531).

2. Adressaten des Herausgabeverlangens der Polizei sind öffentliche und nicht öffentliche Stellen. Zu den öffentlichen Stellen gehören insbesondere Behörden, Organe der Rechtspflege und andere öffentlich-rechtliche organisierte Einrichtungen einschließlich der sog. Beliehenen (vgl. § 2 Abs. 1 LDSG). Nicht öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts (vgl. § 2 Abs. 4 BDSG). Die Befugnis zur Übermittlung der Daten ergibt sich für öffentliche Stellen in Rheinland-Pfalz – sofern keine spezialgesetzliche Regelung vorhanden ist – aus den §§ 5 und § 7 LDSG bzw. im Falle der Übermittlung von besonderen Kategorien personenbezogener Daten (z. B. Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen oder religiöse Überzeugungen hervorgehen) aus § 19 Abs. 2 LDSG i. V. m. Art. 9 Abs. 2 Buchst. g DSGVO. Nicht öffentliche Stellen dürfen nach § 24 Abs. 1 Nr. 1 und Abs. 2 BDSG Daten übermitteln, soweit dies zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist und die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung nicht überwiegen. Ein

schutzwürdiges Interesse des Betroffenen am Ausschluss der Übermittlung besteht, wenn die zu übermittelnden Daten einem Berufsgeheimnis unterliegen. Da verdeckte Datenerhebungen in einem durch ein Berufsgeheimnis geschützten Vertrauensverhältnis i. S. d. §§ 53 Abs. 1 und 53a Abs. 1 StPO unzulässig sind, darf die Polizei die Herausgabe solcher Daten aber ohnehin nicht verlangen. Die repressive Rasterfahndung enthält in § 98a Abs. 5 i. V. m. § 95 Abs. 2 StPO eine hiervon abweichende Regelung. Danach dürfen auch Berufsgeheimnisträger um Datenübermittlung ersucht werden. Sie sind jedoch nicht verpflichtet, personenbezogene Daten, die einem Berufsgeheimnis unterliegen, zu übermitteln, sondern können selbst entscheiden, ob sie die Daten herausgeben oder nicht.

3. Das Verlangen der Polizei zur Herausgabe der begehrten Daten stellt einen Verwaltungsakt dar (Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, S. 893, Rn. 547). Gegenüber Behörden und juristischen Personen des öffentlichen Rechts darf der Verwaltungsakt gem. § 7 LVwVG aber nur vollstreckt werden, soweit dies durch Gesetz oder aufgrund eines Gesetzes besonders zugelassen ist. Da eine entsprechende Ermächtigung fehlt, kann die Herausgabe der Daten im Falle der Weigerung einer öffentlichen Stelle nicht im Wege des Verwaltungszwangs durchgesetzt werden.

4. Die Polizei kann die Übermittlung der Daten von bestimmten Personengruppen verlangen. Um welche Personengruppen es sich dabei handeln kann, ergibt sich mit Blick auf die Regelung in **Abs. 2 Satz 1**, die den Umfang der Übermittlungspflicht festlegt. Danach kann zur Rasterung nur die Übermittlung der Daten verlangt werden, die sich auf die Identifizierungsmerkmale einer Person (Name, Anschrift, Tag und Ort der Geburt) sowie auf im Einzelfall festzulegende Merkmale beziehen. Die weiteren im Einzelfall festzulegenden Merkmale richten sich nach dem Fahndungszweck und danach, nach welcher Personengruppe gefahndet wird (LT-Drs. 14/2287, S. 52). Bei der bundesweiten Rasterfahndung nach den Terroranschlägen vom 11. September 2001 ging es um das Auffinden von sog. Schläfern. Zu den in diesem Fall neben den Identifizierungsmerkmalen festgelegten weiteren Merkmalen gehörten beispielsweise Angaben zur Religionszugehörigkeit, zum Familienstand oder zur Studienfachrichtung. Obwohl Art und Inhalt der im Einzelfall festzulegenden Merkmale gesetzlich nicht näher eingegrenzt sind, hat das BVerfG die vergleichbare Regelung im nordrhein-westfälischen Polizeigesetz unter dem Aspekt der Normenbestimmtheit nicht beanstandet (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 101). Nach **Abs. 2 Satz 2** dürfen schließlich auch solche Daten übermittelt werden, die nicht den Rasterkriterien entsprechen, wenn ihre Aussonderung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Eine Verwendung dieser weiteren Daten ist nach **Abs. 2 Satz 3** unzulässig.

Die Beeinträchtigung der hiervon Betroffenen ist gering, denn der Polizei werden im Ergebnis nur die Daten bekannt, auf die sämtliche Rasterkriterien zutreffen (OVG Rheinland-Pfalz, Beschluss vom 22. März 2003 – 12 B 10331/02 – juris, Rn. 12).

5. Eine Rasterfahndung ist nur zulässig, wenn sie zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist. Hierbei handelt es sich – wie das BVerfG ausgeführt hat – um Schutzgüter von hohem verfassungsrechtlichen Gewicht (BVerfG, Beschluss vom 4 April 2006 – 1 BvR 518/02 – juris, Rn. 91). Bei der abzuwehrenden Gefahr muss es sich um eine konkrete Gefahr handeln, das heißt um eine Sachlage, bei der im konkreten Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die geschützten Rechtsgüter eintreten wird (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 144). Eine konkrete Gefahr in diesem Sinne kann auch eine Dauergefahr sein, bei der über einen längeren Zeitraum die hinreichende Wahrscheinlichkeit eines Schadenseintritts zu jedem Zeitpunkt vorliegt (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 146). In jedem Fall muss sich aber die für die Feststellung einer konkreten Gefahr oder einer Dauergefahr erforderliche Wahrscheinlichkeitsprognose auf Tatsachen beziehen. Vage Anhaltspunkte oder bloße Vermutungen ohne greifbaren, auf den Einzelfall bezogenen Anlass reichen nicht aus (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 145). Insbesondere darf eine Rasterfahndung angesichts der Schwere der mit ihr verbundenen Grundrechtsbeeinträchtigung nicht bereits im Vorfeld konkreter Gefahren ermöglicht werden (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 138). In Bezug auf die nach den Terroranschlägen vom 11. September 2001 bundesweit durchgeführte Rasterfahndung kam das BVerfG zu dem Ergebnis, dass die zur Annahme einer konkreten Gefahr erforderlichen Voraussetzungen nicht vorlagen. Vielmehr habe es sich nur um eine allgemeine Bedrohungslage gehandelt ohne tatsächliche Anhaltspunkte dafür, dass terroristische Anschläge vorbereitet werden oder sich in Deutschland Personen für Terroranschläge bereithalten, die in absehbarer Zeit in Deutschland selbst oder andernorts verübt werden sollen (BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – juris, Rn. 147, 156 ff.).

IV. Richterliche Entscheidung (Abs. 3)

1. Ursprünglich durfte die Maßnahme durch den Behördenleiter angeordnet werden. Seit der Novellierung der Vorschrift durch das Gesetz vom 15. Februar 2011 (GVBl. S. 26) bedarf sie jedoch einer richterlichen Entscheidung. Da die Rasterfahndung eine Vielzahl von Unbeteiligten betreffen kann, sollte durch den Richtervorbehalt der Grundrechtsschutz zusätzlich abgesichert werden (LT-Drs. 15/4879, S. 42). Wie bei anderen verdeckten Datenerhebungen mit hoher

Eingriffstiefe (§§ 29, 31, 31b bis 31e POG) ist das OVG Rheinland-Pfalz zuständig (vgl. Erl. VIII.1. zu § 29). Das OVG Rheinland-Pfalz entscheidet nach Maßgabe der Verwaltungsgerichtsordnung.

2. Nach **Abs. 3 Satz 4** ist der Landesbeauftragte für den Datenschutz und die Informationsfreiheit über die Anordnung einer Rasterfahndung zu unterrichten. Diese Unterrichtungspflicht ist dem Umstand geschuldet, dass die Mehrzahl der von der Datenübermittlung an die Polizei betroffenen Personen nicht über die Maßnahme unterrichtet werden muss, da nach Abs. 5 Satz 1 alle zum Abgleich übermittelten Daten sowie alle im Zusammenhang mit dem Abgleich zusätzlich angefallen Daten zu löschen sind, sobald sie für den festgelegten oder einen anderen zulässigen Zweck nicht mehr benötigt werden. Werden personenbezogene Daten unverzüglich nach Beendigung der Maßnahme gelöscht, unterbleibt gem. § 40 Abs. 6 Nr. 3 POG die Unterrichtung, sodass nach § 40 Abs. 5 Satz 1 POG grundsätzlich nur die Personen unterrichtet werden, gegen die nach Abschluss der Rasterfahndung weitere Maßnahmen ergriffen werden. Mit der Unterrichtung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit wird sichergestellt, dass eine neutrale Instanz von dem Ausmaß der mit einer Rasterfahndung verbundenen Datenerhebung Kenntnis erlangt.

3. Nach **Abs. 3 Satz 5** kann die Maßnahme bei Gefahr im Verzug vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten mit der Befähigung für das vierte Einsteigsamt angeordnet werden. Die richterliche Entscheidung ist dann unverzüglich nachzuholen.

V. Kennzeichnung, Zweckänderung (Abs. 4)

1. Abs. 4 Satz 1 normiert eine besondere Kennzeichnungspflicht für die aus einer Rasterfahndung erlangten Daten. Mit der Kennzeichnung bleibt erkennbar, dass die Daten aus einer Rasterfahndung stammen. Hierdurch wird sichergestellt, dass die in Abs. 4 Satz 3 geregelten besonderen Anforderungen an eine zweckändernde Verwendung der Daten umgesetzt werden können. Nach **Abs. 4 Satz 2** ist die Kennzeichnung nach einer Übermittlung durch die Empfänger aufrechtzuerhalten.

2. Abs. 4 Satz 3 legt fest, unter welchen Voraussetzungen eine zweckändernde Verwendung der Daten zulässig ist. Nach dem Grundsatz der hypothetischen Datenneuerhebung ist eine Zweckänderung zulässig, wenn die neue Nutzung der Daten zum Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen können (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – juris, Rn. 288). Ausreichend, aber für eine Zweckänderung auch erforderlich, ist, dass sich aus den

erhobenen Daten konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter ergeben (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – juris, Rn. 290). Nach **Abs. 4 Satz 3 Nr. 1** dürfen die Daten zu Zwecken der Strafverfolgung verwendet werden, wenn sich aus ihnen konkrete Ermittlungsansätze zur Verfolgung von Straftaten von erheblicher Bedeutung ergeben, die nach der Strafprozessordnung eine Rasterfahndung rechtfertigen. Mit dieser Regelung wird den verfassungsrechtlichen Anforderungen an eine Zweckänderung Rechnung getragen. Nach **Abs. 4 Satz 3 Nr. 2** dürfen die Daten zu einem anderen präventiven Zweck verarbeitet werden, wenn dies zur Abwehr einer dringenden Gefahr im Sinne des Abs. 1 erforderlich ist. Mit dem Erfordernis einer dringenden Gefahr verlangt der Gesetzgeber mehr als verfassungsrechtlich geboten war, denn das BVerfG lässt hinsichtlich des Konkretisierungsgrades der Gefahrenlage Abstriche zu (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – juris, Rn. 289). Statt einer dringenden Gefahr hätte auch eine auf „mittlere Sicht" drohende Gefahr ausgereicht.

3. Die Vorschrift enthält keine ausdrückliche Pflicht zur Dokumentation der Zweckänderung. Gleichwohl ist die Zweckänderung, die einen eigenen Grundrechtseingriff darstellt, zu dokumentieren, damit sie später nachvollzogen und gegebenenfalls überprüft werden kann.

VI. Löschung, verfahrenssichernde Regelungen (Abs. 5)

1. Abs. 5 Satz 1 legt fest, dass die übermittelten und die im Zusammenhang mit dem Abgleich zusätzlich angefallenen Daten zu löschen und die Unterlagen zu vernichten sind, wenn der Zweck der Maßnahme erreicht ist oder sich zeigt, dass er nicht erreicht werden kann. Diese Löschungspflicht gilt jedoch nicht, soweit die Daten für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind.

2. Nach **Abs. 5 Satz 2** ist die getroffene Maßnahme zu dokumentieren. Die Dokumentation ist gem. **Abs. 5 Satz 3** gesondert aufzubewahren und durch technische und organisatorische Maßnahmen zu sichern. Sie ist gem. **Abs. 5 Satz 4** sechs Monate nach der Benachrichtigung nach § 40 Abs. 5 POG zu löschen. Ist die Datenschutzkontrolle nach § 41b POG noch nicht beendet, ist die Dokumentation gem. **Abs. 5 Satz 5** bis zu ihrem Abschluss aufzubewahren. Die Dauer der Aufbewahrungsfrist für die Löschungsprotokolle entspricht den Anforderungen des BVerfG, wonach die Frist so bemessen sein muss, dass die Protokolle bei typisierender Betrachtung nach der Benachrichtigung der Betroffenen und im Rahmen der nächsten periodisch anstehenden Kontrolle durch die oder den Datenschutzbeauftragten(n) noch vorliegen (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 272).