Bundesministerium
des Innern

Bericht

des Bundesministeriums des Innern

zu den Auswirkungen des Urteils des Bundesverfassungsgerichts vom 24.04.2013, 1 BvR - 1215/07 (ATDG), auf die Zusammenarbeit und den Austausch von personenbezogenen Daten zwischen der Polizei und dem Verfassungsschutz

Stand: 24.10.2013

Inhalt

1. Einleitung

Der Erste Senat des Bundesverfassungsgerichts (BVerfG) hat am 24. April 2013 über die Verfassungsmäßigkeit des Antiterrordateigesetzes (ATDG) entschieden (1 BvR 1215/07). Danach ist die Antiterrordatei (ATD) in ihren Grundstrukturen verfassungsgemäß. Jedoch genügt sie hinsichtlich ihrer Ausgestaltung im Einzelnen den verfassungsrechtlichen Anforderungen nicht. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2014, dürfen die verfassungswidrigen Vorschriften unter bestimmten Maßgaben weiter angewendet werden.

Insbesondere die Aussagen des Urteils zum informationellen Trennungsprinzip sind bisher nicht Inhalt der Rechtsprechung des Bundesverfassungsgerichts gewesen. Inwieweit dieses informationelle Trennungsprinzip, das grundrechtlich hergeleitet ist, bestehende gesetzliche oder untergesetzliche Regelungen oder das Verwaltungshandeln berührt, muss im Einzelnen geprüft werden. Sein Inhalt lässt sich jedoch nur in einer Gesamtschau der Entscheidung bestimmen.

2. Inhalt der Entscheidung

Leitsätze:

1. Die Errichtung der Antiterrordatei als Verbunddatei verschiedener Sicherheitsbehörden zur Bekämpfung des internationalen Terrorismus, die im Kern auf die Informationsanbahnung beschränkt ist und eine Nutzung der Daten zur operativen Aufgabenwahrnehmung nur in dringenden Ausnahmefällen vorsieht, ist in ihren Grundstrukturen mit der Verfassung vereinbar.
2. Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendienste ermöglichen, unterliegen hinsichtlich des Grundrechts auf informationelle Selbstbestimmung gesteigerten verfassungsrechtlichen Anforderungen. Aus den Grundrechten folgt ein informationelles Trennungsprinzip, das diesen Austausch nur ausnahmsweise zulässt.
3. Eine Verbunddatei zwischen Sicherheitsbehörden wie die Antiterrordatei bedarf hinsichtlich der zu erfassenden Daten und ihrer Nutzungsmöglichkeiten einer hinreichend bestimmten und dem Übermaßverbot entsprechenden ge-

setzlichen Ausgestaltung. Das Antiterrordateigesetz genügt dem nicht vollständig, nämlich hinsichtlich der Bestimmung der beteiligten Behörden, der Reichweite der als terrorismusnah erfassten Personen, der Einbeziehung von Kontaktpersonen, der Nutzung von verdeckt bereitgestellten erweiterten Grunddaten, der Konkretisierungsbefugnis der Sicherheitsbehörden für die zu speichernden Daten und der Gewährleistung einer wirksamen Aufsicht.

4. Die uneingeschränkte Einbeziehung von Daten in die Antiterrordatei, die durch Eingriffe in das Brief- und Fernmeldegeheimnis und das Recht auf Unverletzlichkeit der Wohnung erhoben wurden, verletzt Art. 10 Abs. 1 und Art. 13 Abs. 1 GG.

Tenor:

1. a) § 1 Absatz 2 und § 2 Satz 1 Nummer 3 des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz) vom 22. Dezember 2006 (Bundesgesetzblatt I Seite 3409) sind mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes unvereinbar.

   b) § 2 Satz 1 Nummer 1 Buchstabe b hinsichtlich des Unterstützens einer unterstützenden Gruppierung und § 2 Satz 1 Nummer 2 des Antiterrordateigesetzes hinsichtlich des Merkmals „Befürworten“ sind mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes unvereinbar.

   c) § 5 Absatz 1 Satz 2 Nummer 1 a des Antiterrordateigesetzes ist mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes insoweit unvereinbar, als bei Recherchen in den erweiterten Grunddaten im Trefferfall Zugriff auf Informationen gemäß § 3 Absatz 1 Nummer 1 a des Antiterrordateigesetzes eröffnet wird.

   d) § 3 Absatz 1 Satz 1 Nummer 1 b und § 10 Absatz 1 des Antiterrordateigesetzes sind, soweit es an ergänzenden Regelungen nach Maßgabe der Gründe fehlt, mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes unvereinbar.

   e) § 2 Satz 1 Nummer 2 und § 10 Absatz 1 des Antiterrordateigesetzes sind im Übrigen nach Maßgabe der Gründe verfassungskonform auszulegen.

2. § 2 Satz 1 Nummern 1 bis 3, § 3 Absatz 1 Nummer 1, § 5 Absatz 1 und 2 sowie § 6 Absatz 1 und 2 des Antiterrordateigesetzes sind mit Artikel 10 Absatz

1 und Artikel 13 Absatz 1 des Grundgesetzes unvereinbar, soweit sie sich auf nicht gemäß § 4 des Antiterrordateigesetzes verdeckt gespeicherte Daten erstrecken, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren.

3. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2014 gelten die für mit dem Grundgesetz unvereinbar erklärten Vorschriften mit der Maßgabe fort, dass außerhalb des Eilfalls gemäß § 5 Absatz 2 des Antiterrordateigesetzes eine Nutzung der Antiterrordatei nur zulässig ist, sofern der Zugriff auf die Daten von Kontaktpersonen (§ 2 Satz 1 Nummer 3 des Antiterrordateigesetzes) und auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, ausgeschlossen und gewährleistet ist, dass bei Recherchen in den erweiterten Grunddaten im Trefferfall allein ein Zugang zu Informationen gemäß § 3 Absatz 1 Nummer 3 des Antiterrordateigesetzes gewährt wird; sobald danach die Möglichkeit des Zugriffs auf die Daten von Kontaktpersonen und auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, ausgeschlossen ist, dürfen diese auch für die Nutzung der Datei im Eilfall gemäß § 5 Absatz 2 des Antiterrordateigesetzes nicht mehr genutzt werden.
4. Im Übrigen wird die Verfassungsbeschwerde zurückgewiesen.
5. Die Bundesrepublik Deutschland hat dem Beschwerdeführer seine notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren zu erstatten.

3. Berichtsauftrag

Die Ständige Konferenz der Innenminister und -senatoren der Länder (IMK) hat auf ihrer 197. Sitzung am 23./24.05.2013 in Hannover unter TOP 36 die Auswirkungen des Urteils des BVerfG vom 24.04.13 (Az.: 1 BvR 1215/07) auf die Zusammenarbeit zwischen Nachrichtendiensten und der Polizei behandelt und hierzu folgenden Beschluss gefasst:

1. Die IMK nimmt die Feststellung im Urteil des Bundesverfassungsgerichts vom 24.04.13 - 1 BvR 1215/07 -, dass die Antiterrordatei in ihren Grundzügen mit dem Grundgesetz vereinbar ist, zur Kenntnis.
2. Sowohl die Bedrohung durch den internationalen islamistisch motivierten Terrorismus, als auch die Morde des rechtsterroristischen NSU machen deutlich, dass eine enge und vertrauensvolle Zusammenarbeit der Sicherheitsbehörden für die Bekämpfung von politisch motivierter Gewalt von zentraler Bedeutung ist.
3. Auch das GETZ und das GTAZ sind für den Informationsaustausch zu Gefahrenlagen und Gefährdungsbewertungen unerlässlich.
4. Soweit die Zusammenarbeit zwischen Polizei und Verfassungsschutz die Übermittlung von personenbezogenen Daten betrifft, muss entsprechend den Ausführungen des Bundesverfassungsgerichts geprüft werden, inwieweit - insbesondere im Hinblick auf gemeinsam geführte Dateien - weiterer Regelungsbedarf besteht.
5. Die IMK bittet das BMI, unter Beteiligung des AK II und AK IV, die Auswirkungen des Urteils in Bezug auf den Austausch von personenbezogenen Daten zwischen der Polizei und dem Verfassungsschutz zu prüfen und der IMK bis zur Herbstsitzung zu berichten.

Unter Bezugnahme auf Ziffer 5 dieses Beschlusses legt das Bundesministerium des Innern diesen Berichtsentwurf vor. AK II und AK IV waren bei der Erstellung des Berichts beteiligt und haben mitgewirkt.

4. Ergebnisse

4.1 Unmittelbare Auswirkungen des Urteils

Unmittelbare Auswirkungen entfaltet die Entscheidung des BVerfG nur im Rahmen ihrer Tenorierung und der tragenden Gründe, die sich naturgemäß auf den Gegenstand der zugrundeliegenden Verfassungsbeschwerde beschränken. Soweit das BVerfG einzelne Regelungen für mit der Verfassung unvereinbar oder nur nach bestimmten Maßgaben mit der Verfassung vereinbar erklärt hat (Nr. 1 und 2 des Urteilstenors), gelten die bisherigen Vorschriften bis zu einer Neuregelung, längstens bis zum 31.12.2014, fort. Bis zum Inkrafttreten der Neuregelung sind die in Nr. 3 des Urteilstenors festgelegten Maßgaben zu beachten.

4.1.1 Auswirkungen bis zum Inkrafttreten einer Neuregelung (Übergangsregelung)

Für die Übergangszeit bestimmt das BVerfG in Nummer 3 des Urteilstenors:

„Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2014, gelten die für mit dem Grundgesetz unvereinbar erklärten Vorschriften mit der Maßgabe fort, dass außerhalb des Eilfalls gemäß § 5 Absatz 2 des Antiterrordateigesetzes eine Nutzung der Antiterrordatei nur zulässig ist, sofern der Zugriff auf die Daten von Kontaktpersonen (§ 2 Satz 1 Nummer 3 des Antiterrordateigesetzes) und auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, ausgeschlossen und gewährleistet ist, dass bei Recherchen in den erweiterten Grunddaten im Trefferfall allein ein Zugang zu Informationen gemäß § 3 Absatz 1 Nummer 3 des Antiterrordateigesetzes gewährt wird; sobald danach die Möglichkeit des Zugriffs auf die Daten von Kontaktpersonen und auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, ausgeschlossen ist, dürfen diese auch für die Nutzung der Datei im Eilfall gemäß § 5 Absatz 2 des Antiterrordateigesetzes nicht mehr genutzt werden.“

4.1.1.1 Nutzung im Eilfall

Dies bedeutet zunächst, dass die ATD weiterhin uneingeschränkt genutzt werden kann, wenn die Voraussetzungen des Eilfalls nach § 5 Abs. 2 ATDG vorliegen, die Nutzung also „*aufgrund bestimmter Tatsachen zur Abwehr einer gegenwärtigen Ge-*

fahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, unerlässlich ist“ (§ 5 Abs. 2 Satz 1 ATDG).

Die eigentliche Eilfallregelung des § 5 Abs. 2 ATDG erfasst lediglich den Fall, dass eine Behörde nach einem Treffer in der ATD ohne die eigentlich erforderliche Zustimmung der datenbesitzenden Behörde auf die erweiterten Grunddaten der Person zugreifen möchte. Aufgrund dieses sehr engen Anwendungsbereichs ist seit Inbetriebnahme der ATD lediglich ein Eilfall vorgekommen.

Die Formulierung im Urteilstenor zielt allerdings erkennbar darauf ab, lediglich die gegenüber der einfachen Abfrage erhöhte materielle Schranke der Eilfallregelung wie oben zitiert auf die Nutzung der ATD insgesamt anzuwenden.

Im Ergebnis kann die ATD damit im Rahmen der Übergangsregelung unter den Voraussetzungen des Eilfalls weiter genutzt werden. Sobald die Möglichkeit des Zugriffs auf die Daten von Kontaktpersonen und auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, ausgeschlossen ist (hierzu sogleich unten, S. 9), dürfen diese auch für die Nutzung der Datei im Eilfall gemäß § 5 Ab. 2 ATDG nicht mehr genutzt werden.

4.1.1.2 Nutzung außerhalb des Eilfalls

Außerhalb des Eilfalls darf die ATD in der Übergangsphase genutzt werden, wenn sichergestellt ist, dass
(a) der Zugriff auf Daten von Kontaktpersonen sowie
(b) auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis [Art. 10 GG] und das Grundrecht auf Unverletzlichkeit der Wohnung [Art. 13 GG] herrühren ausgeschlossen ist und
(c) gewährleistet ist, dass bei Recherchen in den erweiterten Grunddaten nur Zugriff auf Daten nach § 3 Abs. 1 Nr. 3 ATDG gewährt wird (Nr. 3 des Urteilstenors).

Ausweislich der Gründe ist Hintergrund für die Regelung, dass verhindert werden soll, dass bezüglich der vom BVerfG als sensibel eingestuften Daten (Erkenntnisse aus Eingriffen in Art. 10, 13 GG; erweiterte Grunddaten) eine automatisierte Über-

mittlung stattfindet, in der die datenbesitzende Behörde nicht mehr im Einzelfall prüfen kann, ob die Voraussetzungen nach den jeweils einschlägigen Übermittlungsvorschriften vorliegen. Dementsprechend ist mit „Zugriff“ offenbar die Erhebung von Daten anderer Behörden aus der ATD in Form des automatisierten Abrufs (§ 10 Abs. 1 BDSG) gemeint. Nicht erfasst sind hingegen das Einstellen von Daten sowie der Abruf von eigenen Daten (z.B. zur Überprüfung der Richtigkeit selbst eingestellter Daten, „Datenpflege“). Dies ist auch weiterhin uneingeschränkt zulässig. Ein Zugriff kann dabei sowohl dadurch ausgeschlossen werden, dass die Daten komplett gelöscht werden, oder dadurch, dass sie nur verdeckt im Sinne des § 4 ATDG eingestellt werden. Im Falle einer verdeckten Speicherung wird der Datensatz dergestalt eingestellt, dass eine suchende Behörde im Falle eines Treffers keine Treffermeldung erhält. Diese erhält nur die datenbesitzende Behörde, die dann im Einzelfall entscheiden muss, ob sie Kontakt zu der suchenden Behörde aufnimmt, wenn die rechtlichen Voraussetzungen hierfür erfüllt sind.

(a) Um den Zugriff auf Daten zu Kontaktpersonen auszuschließen, können diese mithin entweder komplett aus der ATD gelöscht werden oder verdeckt gespeichert werden. Dabei dürfen die Hauptpersonen, zu denen Kontaktpersonen existieren, trotz des Eintrags der Personaldaten im Feld nach § 3 Abs. 1 Nr. 1 b) oo) ATDG grundsätzlich im offenen Bestand bleiben. Lediglich der eigenständige Datensatz der Kontaktperson ist verdeckt einzustellen.

Gemäß § 2 Nr. 3 ATDG besteht auch für Kontaktpersonen eine Speicherpflicht, wenn die Tatbestandsvoraussetzungen vorliegen. Da die Übergangsregelung des BVerfG nur den Zugriff auf die Daten betrifft, bleibt diese Speicherpflicht bestehen.

Bei verständiger Auslegung des § 2 Nr. 3 ATDG im Lichte der Entscheidung des BVerfG dürfte allerdings im Rahmen der Übergangsregelung die Speicherpflicht hinsichtlich des Umfangs der zu den jeweiligen Kontaktpersonen zu speichernden Daten auf die vom BVerfG zitierten „wenigen Elementardaten“ beschränkt sein. Als Leitlinie können die unten stehenden Ausführungen zur möglichen Neuregelung der Speicherung von Kontaktpersonen herangezogen werden (S. 14).

(b) Entsprechendes gilt auch für personenbezogene Daten, die aus Eingriffen in die Grundrechte nach Art. 10 oder 13 GG herrühren. Dabei erachtet das BVerfG die verdeckte Speicherung derartiger Daten für zulässig (Rz. 228). Es muss lediglich durch die verdeckte Speicherung sichergestellt werden, dass die regelmäßig höheren Hürden für die Übermittlung dieser Daten im Einzelfall von der datenbesitzenden Behörde geprüft werden können.

Aus diesen Erwägungen folgt auch, dass sich die Pflicht zur verdeckten Speicherung nur auf die Daten des Personen-Datensatzes bezieht, die tatsächlich durch die entsprechende Maßnahme gewonnen wurden. Dies bedeutet, dass der Datensatz einer Person grundsätzlich offen gespeichert werden kann und nur der Zugriff auf die Daten innerhalb des Personen-Datensatzes, die aus dem Eingriff in Art. 10 oder 13 GG herrühren, verhindert werden muss. Soweit es technisch nicht möglich ist, nur einzelne Daten eines offenen Datensatzes verdeckt einzustellen, bieten sich zwei Möglichkeiten an: Der Personen-Datensatz wird einmal – ohne die entsprechenden Daten – im offenen Bestand eingestellt und noch einmal zusätzlich – mit den entsprechenden Daten - im verdeckten Bestand. Sind dagegen die Daten, die aus dem Eingriff in Art. 10 bzw. 13 GG herrühren, für das Auffinden der Person in der Datei nicht erheblich, kommt auch eine beschränkte Speicherung nach § 4 Abs. 1 Alt. 1 ATDG in Betracht, das heißt der Datensatz wird lediglich im offenen Bestand, aber ohne die entsprechenden zusätzlichen Daten eingestellt. In letzterem Falle stehen diese Einzelinformationen, z.B: Rufnummern der Person, dann allerdings auch nicht für die Suche zur Verfügung. Dies gilt auch für das Datenabgleichverfahren nach § 72a AufenthG.

Auch hinsichtlich der personenbezogenen Daten, die aus Eingriffen in Art 10 oder 13 GG herrühren, bleibt die Speicherpflicht nach § 2 ATDG, soweit nicht eine beschränkte Speicherung in Betracht kommt, während der Übergangsphase bestehen.

Unklar ist, was genau mit „Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren“ gemeint ist. Nach dem Wortlaut des Tenors wären prima facie sämtliche Daten betroffen, die durch Eingriffe in die Grundrechte aus Artikel 10 und 13 GG, also in die Unverletzlichkeit der Wohnung oder das Brief-, Post- oder Fernmeldegeheiminis, erlangt wurden. Im Tenor spricht das Gericht von „Daten, die aus Eingriffen in das Telekommu-

nikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren“, im Leitsatz von Daten, die „durch Eingriffe in das Brief- und Fernmeldegeheimnis und das Recht auf Unverletzlichkeit der Wohnung erhoben wurden“. In der Begründung ist schließlich überwiegend von Telekommunikations- und Wohnraumüberwachung die Rede. Das Postgeheimnis wird an keiner Stelle erwähnt.

In den Gründen nimmt das Gericht allerdings Bezug auf seine Rechtsprechung zu verdeckten Grundrechtseingriffen. Nur hierfür hat es bislang Kennzeichnungspflichten gefordert, da die besondere Schwere des Grundrechtseingriffs gerade auch dadurch begründet ist, dass der Betroffene von der Maßnahme allenfalls im Nachhinein erfährt. Damit wären insbesondere im Hinblick auf Art. 13 GG nur die verdeckten Eingriffe in Form der Wohnraumüberwachung erfasst, nur diese spricht das Gericht in den Urteilsgründen auch an (Rz. 225 f.). Auch in Rz. 226 ist von Daten, „die durch Telekommunikationsüberwachung, Wohnraumüberwachung oder auch Maßnahmen der strategischen Beschränkung (vgl. §§ 5 ff. G 10) gewonnen wurden die Rede.

Daten, die im Rahmen von offenen Eingriffen – also insbesondere im Zuge offener Wohnungsdurchsuchungen, aber auch durch Beschlagnahme von Briefen beim Betroffenen – erhoben wurden, erwähnt das Gericht in seiner Begründung hingegen nicht. Offenbar sind solche Eingriffe vom Gericht nicht gemeint.

Im Ergebnis ist daher im Rahmen der Neuregelung vorzusehen, dass Erkenntnisse aus verdeckten Eingriffen in Art. 10 und 13 GG, also aus Maßnahmen der Telekommunikations-, und Wohnraumüberwachung oder der Postbeschlagnahme beim Postdienstleister, nur verdeckt in der ATD zu speichern sind.

Dafür gelten die Ausführungen nach dem obiter dictum in Rz. 226 auch für vom Beschwerdeführer nicht gerügte Eingriffe in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, also insbesondere für Daten, die mittels der sog. Onlinedurchsuchung (für den Bund nur in § 20k BKAG vorgesehen) erlangt wurden.

(c) Schließlich muss bei Recherchen in den erweiterten Grunddaten gewährleistet sein, dass im Trefferfall allein ein Zugang zu Informationen gemäß § 3 Absatz 1

Nummer 3 ATDG, also einstellende Behörde, Aktenzeichen und ggf. VS-Grad, gewährt wird. Dies bedeutet, dass keine sog. *Inverssuche* über erweiterte Grunddaten dergestalt durchgeführt werden darf, dass allein durch die Eingabe von Suchbegriffen in den Feldern der erweiterten Grunddaten Namen von Verdächtigen ausgegeben werden. Hierzu ist die Suchfunktion entweder entsprechend umzuprogrammieren oder, wenn dieses technisch zu aufwändig ist, ggf. durch geeignete Maßnahmen ganz auszuschließen. Dies gilt ausweislich der Begründung lediglich für die Nutzung außerhalb des Eilfalls, unter den Voraussetzungen des Eilfalls bleibt auch die Inverssuche zulässig, R. 201.

4.1.1.3 Zwischenergebnis

Mit Verkündung der Entscheidung des BVerfG darf die ATD zunächst nur im Eilfall unter den materiellen Voraussetzungen des § 5 Abs. 2 ATDG abgefragt werden. Sobald die nachfolgenden Maßgaben erfüllt sind, darf die ATD bis zu einer Neuregelung, längstens bis zum 31.12.2014, genutzt werden:

a) Kein Zugriff auf Daten von Kontaktpersonen

b) Kein Zugriff auf personenbezogene Daten aus verdeckten Eingriffen in Artikel 10 oder 13 GG sowie in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (Onlinedurchsuchung)

c) Umprogrammierung der Inverssuche oder deren Ausschluss.

Alle übrigen, im Folgenden dargestellten Auswirkungen entfalten erst mit Ablauf der Übergangsfrist am 31.12.2014 ihre Wirkung, sofern nicht bis dahin eine Neuregelung in Kraft getreten ist.

4.1.2 Auswirkungen auf das ATDG

Sofern bis zum Ablauf der Übergangsfrist keine Neuregelung ergangen ist, treten die unter Nummern 1 und 2 des Urteils tenorierten Folgen in Kraft. Im Rahmen der Neuregelung sind die entsprechenden Vorgaben aus dem Urteilstenor zu berücksichtigen, wobei das BVerfG in seiner Entscheidung dem Gesetzgeber teilweise Umsetzungsspielräume belässt.

4.1.2.1 Unvereinbarkeit von § 1 Abs. 2 und § 2 Satz 1 Nr. 3 ATDG mit dem Grundgesetz

Gemäß Nr. 1 a) des Urteilstenors sind die §§ 1 Abs. 2 und 2 Satz 1 Nr. 3 ATDG mit dem Grundgesetz unvereinbar.

a) § 1 Abs. 2 gestattet es, im Benehmen mit dem BMI über die in Absatz 1 genannten Behörden hinaus weitere teilnehmende Behörden zu benennen. Mit Ablauf der Übergangsfrist sind die bislang durch die Errichtungsanordnung zur ATD, also durch Verwaltungsvorschrift benannten Behörden daher nicht mehr zum Zugriff auf die ATD berechtigt. Dies betrifft die weiteren Polizeivollzugsbehörden der Länder Bayern, Baden-Württemberg und Rheinland-Pfalz.

Ausweislich Rz. 144 der Urteilsgründe hat der Gesetzgeber im Rahmen der Neuregelung die Möglichkeit, diese Behörden per Gesetz durch Aufnahme in die Aufzählung des Absatz 1 zum Zugriff zu berechtigen, oder für die Benennung weiterer Behörden eine Verordnungsermächtigung nach den Vorgaben des Art. 80 GG im Gesetz vorzusehen.

Da sich die Benennung weiterer Polizeivollzugsbehörden in den Ländern, die dies praktiziert haben, bewährt hat, sollte eine entsprechende Verordnungsermächtigung vorgesehen werden.

b) § 2 Satz 1 Nr. 3 ATDG regelt die Speicherung der Kontaktpersonen. Auch diese fiele nach dem 31.12.2014 ersatzlos fort. Grund für die Verfassungswidrigkeit der Vorschrift ist ausweislich der Gründe, dass die im ATDG vorgesehene Einbeziehung

von Kontaktpersonen weder mit dem Bestimmtheitsgrundsatz noch mit dem Übermaßverbot vereinbar ist (Rz. 162 ff.). Es sei nicht vorhersehbar, wer in der Datei als Kontaktperson gespeichert werden könne. Das Gericht benennt hier insbesondere Personen aus dem privaten, beruflichen oder geschäftlichen Umfeld der terrorismusverdächtigen Hauptperson (Rz. 164). Daher ist die Speicherung derart weit gefasster Kontaktpersonen im Rahmen einer Neuregelung nur dergestalt zulässig, als diese mit nur wenigen Elementardaten nach § 3 Abs. 1 Nr. 1 b) oo) als Information zur eigentlichen Hauptperson gespeichert werden (Rz. 165).

Kontaktpersonen sind – so das Gericht – „nach dem Zweck der Datei nur insoweit von Interesse, als sie Aufschluss über die als terrorismusnah geltende Hauptperson vermitteln können. Hieran muss sich auch die gesetzliche Ausgestaltung orientieren." Mit Elementardaten sind demnach die für eine schnelle Identifizierung und Kontaktaufnahme erforderlichen Daten gemeint, also insbesondere Name, Anschrift, Geburtsdatum, telefonische oder sonstige Erreichbarkeiten. In den ATD-Gremien wird derzeit ein Katalog der Daten erarbeitet, die diese Kriterien erfüllen. Dieser sollte im Rahmen der Neuregelung berücksichtigt werden.

Die Speicherung „zu" der entsprechenden Hauptperson ist offenbar so gemeint, dass die Daten der Kontaktperson in das jeweilige Feld der zugehörigen Hauptperson entsprechend § 3 Abs. 1 Nr. 1 b) oo) ATDG eingetragen oder mit diesem verknüpft werden sollen.

Nicht vom Gericht ausgeführt wird, ob eine Speicherung von Kontaktpersonen in der hergebrachten Form zulässig bleibt, wenn der Kreis der zu speichernden Personen enger und damit vorhersehbar gefasst wird. Denkbar wäre beispielsweise eine Regelung nach dem Vorbild des § 2 Nr. 3 RED-G, der den Kreis der Kontaktpersonen auf Angehörige der rechtsextremistischen Szene beschränkt. Ausweislich Rz. 164 der Urteilsgründe kommt es letztlich darauf an, dass die Speicherung für den Betroffenen vorhersehbar sein muss, sei es, weil er um die extremistischen Aktivitäten seines Kontakts weiß, oder er dieselben extremistischen Bestrebungen verfolgt. Unter diesen Voraussetzungen wäre daher eine Speicherung von Kontaktpersonen auch als eigenständig recherchierbarer Datensatz zulässig, da der Personenkreis bestimmt ist und die Speicherung dieses enger gefassten Personenkreises im Hinblick auf die

damit verbundenen Ziele auch verhältnismäßig bleibt. Wie eine entsprechende Formulierung im ATDG aussehen könnte, müsste im Rahmen des Gesetzgebungsverfahrens erörtert werden; eine abgrenzbare „Szene“ die im Bereich des internationalen Terrorismus alle Formen des Terrorismus abdecken würde, existiert zwar nicht. Denkbar wäre aber beispielsweise in Anlehnung an § 72a Abs. 2 Satz 1 Nr. 4 AufenthG das Abstellen auf die Kenntnis der Kontaktperson von der Planung oder Begehung einer Straftat nach § 129a StGB bzw. § 129a i. V. m. § 129b StGB oder von der Ausübung, Unterstützung oder Vorbereitung rechtswidriger Gewalt.

4.1.2.2 Teilweise Unvereinbarkeit von § 2 Satz 1 Nr. 1 b) und Nr. 2 ATDG mit dem Grundgesetz

a) § 2 Satz 1 Nr. 1 b) ATDG ist insoweit mit dem Grundgesetz unvereinbar, als Voraussetzung für eine Speicherung bereits das Unterstützen einer den Terrorismus unterstützenden Gruppierung ist. Mit Ablauf der Übergangsfrist fiele daher dieses Merkmal weg.

Aus Rz. 149 der Urteilsgründe ergibt sich jedoch, dass im Rahmen einer Neuregelung die Beibehaltung des Merkmals des „Unterstützens“ dann möglich ist, wenn als Voraussetzung für das Vorliegen dieses Merkmals das Bestehen tatsächlicher Anhaltspunkte dafür gefordert wird, dass es sich um eine willentliche Förderung der den Terrorismus unterstützenden Aktivitäten solcher Gruppierungen handelt. Das Merkmal müsste im Rahmen der Neuregelung entsprechend ergänzt und damit eingegrenzt werden.

b) § 2 Satz 1 Nr. 2 ATDG ist insoweit mit dem Grundgesetz unvereinbar, als auch das bloße Befürworten von Gewalt umfasst ist, ohne dass es Anhaltspunkte gibt, dass die Personen tatsächlich Gewalt anwenden, unterstützen, vorbereiten oder hervorrufen. Die entsprechende Regelung fiele daher mit Ablauf der Übergangsfrist fort und wäre im Rahmen einer Neuregelung zu streichen oder durch eine engere Formulierung zu ersetzen, die entsprechende Anhaltspunkte voraussetzt. So führt das Gericht unter Rz. 161 ausdrücklich aus, dass der – vom Gesetzgeber in erster Linie intendierten - Aufnahme von Hasspredigern im Falle eines öffentlichen Anstachelns zu Hass und Gewalt keine verfassungsrechtlichen Bedenken entgegen stünden, sondern lediglich die insoweit überschießende Gesetzesformulierung zu weit sei.

4.1.2.3 Teilweise Unvereinbarkeit von § 5 Abs. 1 Satz 2 Nr. 1 a) ATDG mit dem Grundgesetz („Inverssuche“)

§ 5 Abs. 1 Satz 2 Nr. 1 a) ATDG ist mit dem Grundgesetz insoweit unvereinbar, als bei Recherchen in den erweiterten Grunddaten im Trefferfall Zugriff auf Informationen gemäß § 3 Abs. 1 Nr. 1 a) ATDG eröffnet wird (Rz. 198 f.). Derartige „Inverssuchen“ (s.o. S.12) sind bereits im Rahmen der Maßgaben für die Übergangszeit unzulässig. Wenn der Gesetzgeber [künftig] in diesem Umfang Daten in die Datei einzustellen anordnet, dürfen diese im Rahmen der Informationsanbahnung nur zur Ermöglichung eines Fundstellennachweises genutzt werden. Dementsprechend muss eine Nutzungsregelung so ausgestaltet sein, dass dann, wenn sich eine Recherche auch auf erweiterte Grunddaten erstreckt, nur das Aktenzeichen und die informationsführende Behörde angezeigt werden, nicht aber auch die korrespondierenden einfachen Grunddaten (Rz. 200).

4.1.2.4 Bedingte Unvereinbarkeit des § 3 Abs. 1 Satz 1 Nr. 1b und § 10 Abs. 1 ATDG

§ 3 Abs. 1 Satz 1 Nr. 1 b) und § 10 Abs. 1 ATDG sind mit dem Grundgesetz unvereinbar, soweit es an ergänzenden Regelungen nach Maßgabe der Gründe fehlt. Dies betrifft einerseits die Speicherung der erweiterten Grunddaten nach § 3 Abs. 1 Satz 1 Nr. 1 b), andererseits die eher deklaratorischen Ausführungen zur datenschutzrechtlichen Kontrolle in § 10 Abs. 1 ATDG.

a) Aus den Gründen ergibt sich hinsichtlich der erweiterten Grunddaten lediglich eine Maßgabe: Die Datenkategorien nach § 3 Abs. 1 Nr. 1 b) Buchst. gg), hh), ii), kk) und nn) (Volkszugehörigkeit, Religionszugehörigkeit, besondere Fähigkeiten, Tätigkeiten in sicherheitsempfindlichen Bereichen und besuchte Orte) sind im Gesetz selbst zu unbestimmt und weit definiert und bedürfen der Konkretisierung, wie sie derzeit im sogenannten Katalog-Manual vorgenommen wird, das als Verschlussache eingestuft ist und nur den teilnehmenden Behörden zur Verfügung steht. Zur Gewährleistung der notwendigen Transparenz verlangt das Gericht eine ergänzende Bestimmung, die eine nachvollziehbare Dokumentation und Veröffentlichung der Konkretisierung

gewährleistet (Rz. 187). Notwendig ist daher eine Pflicht, die entsprechenden Konkretisierungen beispielsweise in einer Verwaltungsvorschrift festzulegen und diese sowie Änderungen hieran in geeigneter Weise zu veröffentlichen.

Unklar ist die Rechtsfolge, wenn eine Regelung nicht rechtzeitig nach Fristablauf am 31.12.2014 in Kraft tritt. Der Tenor benennt den gesamten § 3 Abs. 1 Nr. 1 b) ATDG, also alle erweiterten Grunddaten, die Begründung beschränkt die verfassungsrechtliche Kritik hingegen auf die Datenkategorien nach Buchst. gg), hh), ii), kk) und nn). Es ist bei verständiger Würdigung davon auszugehen, dass im Falle der gesetzgeberischen Untätigkeit lediglich diese Datenkategorien nicht mehr verwendet werden dürften und gelöscht werden müssten, die übrigen erweiterten Grunddaten aber weiter genutzt werden könnten.

b) Hinsichtlich der datenschutzrechtlichen Aufsicht und Transparenz enthält die Begründung Ausführungen in den Rz. 214 bis 222. Konkrete Regelungen werden allerdings nur im Rz. 219 aE und Rz 222 gefordert. Im Übrigen belässt es das Gericht bei einer verfassungskonformen Auslegung des § 10 Abs. 1 ATDG (hierzu sogleich unten, S. 18) und dem Appell an die Datenschutzbeauftragten, für eine effektive kooperierende Kontrolle selbst zu sorgen (Rz. 216, 220).

Damit ergibt sich aus Nr.1 d) des Urteilstenors ein konkreter Regelungsbedarf hinsichtlich verpflichtender turnusmäßiger Datenschutzkontrollen etwa alle zwei Jahre (Rz. 217, 219 aE) sowie hinsichtlich einer regelmäßigen Berichtspflicht des BKA gegenüber Parlament und Öffentlichkeit (Rz. 222).

4.1.2.5 Verfassungskonforme Auslegung von § 2 Satz 1 Nummer 2 und § 10 Abs. 1 ATDG

§ 2 Satz 1 Nummer 2 und § 10 Absatz 1 ATDG sind im Übrigen nach Maßgabe der Gründe verfassungskonform auszulegen.
Dies bedeutet im Hinblick auf § 2 Satz 1 Nr. 2 ATDG, dass die unbestimmten Rechtsbegriffe der „rechtswidrigen Gewalt“ sowie des „Hervorrufens“ solcher Gewalt eng auszulegen sind, also beispielsweise nicht der weite Gewaltbegriff des § 240 StGB zugrundegelegt werden kann (Rz. 150) und ein willentliches Hervorrufen von Gewalt vorliegen muss (Rz. 152).

Zu § 10 Abs. 1 ATDG fordert das Gericht im Hinblick auf das Zusammenspiel der Kontrollbefugnisse der Datenschutzbeauftragten von Bund und Ländern sowie der G10-Kommission, dass es den Kontrollinstanzen gestattet sein muss, kontrollierend zusammenzuwirken, und der Gesetzgeber eine kontrollierende Kooperation ermöglichen muss (Rz. 216).

Mit den Instrumenten der Amtshilfe nach Art. 35 Abs. 1 GG, §§ 4 ff. VwVfG des Bundes und der Auftragsdatenverarbeitung nach § 11 BDSG stehen den Kontrollinstanzen die notwendigen Rechtsgrundlagen für eine Zusammenarbeit zur Verfügung. Diese zu nutzen stellt das BVerfG in die Verantwortung der beteiligten Stellen (Rz. 220). Das Bundesministerium des Innern beabsichtigt, eine Kooperation des BfDI mit den Datenschutzbeauftragten der Länder bei der Ausübung der Kontrolle zu unterstützen. Einzelne Datenschutzbeauftragte haben bereits angekündigt, gemeinsame Kontrollen durchführen zu wollen.

4.1.2.6 Bedingte Unvereinbarkeit der §§ 2 Satz 1 Nr. 1 bis 3, § 3 Abs. 1 Nr. 1, § 5 Abs. 1 und 2 sowie § 6 Abs. 1 und 2 ATDG

§ 2 Satz 1 Nummern 1 bis 3, § 3 Absatz 1 Nummer 1, § 5 Absatz 1 und 2 sowie § 6 Absatz 1 und 2 ATDG sind mit dem Grundgesetz unvereinbar, soweit sie sich auf nicht gemäß § 4 ATDG verdeckt gespeicherte Daten erstrecken, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren.

Für Datenerhebungen, die in die Grundrechte der Art. 10 Abs. 1 und Art. 13 Abs. 1 GG eingreifen, gelten angesichts deren besonderen Schutzgehalts in der Regel besonders strenge Anforderungen. Diese gesteigerten Anforderungen wirken nach der Rechtsprechung des Bundesverfassungsgerichts auch in den Anforderungen für die Weitergabe und Zweckänderung der hierdurch gewonnen Daten fort. So darf etwa die Schwelle für die Übermittlung von Daten, die im Rahmen strafprozessualer Maßnahmen durch eine Wohnraumüberwachung erlangt wurden, nicht unter diejenige abgesenkt werden, die bei der Gefahrenabwehr für entsprechende Eingriffe gilt, da durch eine Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden nicht unterlaufen werden dürfen. Ebenso ist eine

Weitergabe von Telekommunikationsdaten, die nur unter besonders strengen Bedingungen abgerufen werden dürfen, nur dann an eine andere Stelle zulässig, wenn sie zur Wahrnehmung von Aufgaben erfolgt, derentwegen ein Zugriff auf diese Daten auch unmittelbar zulässig wäre. Dem entspricht, dass Daten, die aus gewichtigen Eingriffen in Art. 10 Abs. 1 oder Art. 13 Abs. 1 GG stammen, zu kennzeichnen sind (BVerfG vom 14.07.1999 – 1 BvR 2226/94 – Rz. 168 (G10-Befugnisse des BND); BVerfG vom 3.3.2004 – 1 BvF 3/92 (Post- und Fernmeldeüberwachung durch ZKA); BVerfG vom 3.3.2004 - 1 BvR 2378/98 – Rz. 339 (akustische Wohnraumüberwachung); BVerfG vom 2.3.2010 – 1 BvR 256/08 - Rz. 267 (Vorratsdatenspeicherung)). Die Erkennbarkeit solcher Daten soll die Beachtung der spezifischen Grenzen für die Datennutzung auch nach deren etwaiger Weiterleitung an andere Stellen sicherstellen (Rz. 225).

Wie das Gericht in Rz. 227 f. ausführt, müsste eine gesetzliche Regelung daher vorschreiben, dass derartige personenbezogene Daten nur verdeckt eingestellt werden dürfen, damit die einstellende Behörde im Trefferfall einzelfallbezogen prüfen kann, ob die Übermittlung der Erkenntnisse auch aus Eingriffen in Art. 10 oder 13 GG im konkreten Fall zulässig wäre oder nicht. Eine automatisierte Ausgabe im Rahmen einer Treffermeldung an die suchende Behörde wäre damit ausgeschlossen.

Wie oben ausgeführt, erstreckt sich das Gebot der verdeckten Speicherung von Daten auf personenbezogene Daten, die durch verdeckte Eingriffe in Art. 10 oder 13 GG oder das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewonnen wurden, also durch Telekommunikationsüberwachung, Brief- oder Postbeschlagnahme beim Dienstleister oder Wohnraumüberwachung. Dabei genügt es, die jeweiligen Einzeldaten zu verdecken oder den Datensatz beschränkt einzustellen. Eine verdeckte Speicherung des gesamten Personendatensatzes ist grundsätzlich nicht erforderlich.

Sollte eine derartige Regelung nicht zustande kommen, wären § 2 Satz 1 Nr. 1 bis 3, § 3 Abs. 1 Nr. 1, § 5 Abs. 1 und 2 sowie § 6 Abs. 1 und 2 ATDG nach Ablauf der Übergangsfrist nicht mehr mit dem Grundgesetz vereinbar und damit nicht mehr anwendbar. Dies betrifft die Vorschriften zur Speicherung von Daten in der ATD (§ 2 Satz 1, § 3 Abs. 1 Nr. 1), zum Zugriff auf die Daten (§ 5 Abs. 1 und 2) und zur weite-

ren Verwendung (§ 6 Abs. 1 und 2). Sofern daher der Gesetzgeber bis zum 31.12.2014 keine entsprechende Regelung vorsieht, kann ab 01.01.2015 die gesamte ATD nicht mehr genutzt werden.

Praktisch umgesetzt wird diese Vorgabe bereits im Rahmen der Übergangsmaßgaben.

4.2 Mittelbare Auswirkungen des Urteils auf die Zusammenarbeit von Polizei und Verfassungsschutz

Ausweislich Rz. 232 der Urteilsgründe will das Gericht dem Gesetzgeber durch die Übergangsfrist bis zum 31.12.2014 die Möglichkeit geben *„zu prüfen, ob er im Zusammenhang mit der Neuregelung des ATDG auch eine Überarbeitung von Bestimmungen anderer Gesetze, die den angegriffenen Vorschriften ähnlich sind, sowie eventuell von Datenübermittlungsvorschriften einzelner Sicherheitsbehörden für angezeigt hält*“. Hieraus ergibt sich ein Prüfauftrag, der über den Verfahrensgegenstand – das ATDG – hinausgeht. Zu prüfen sind ausweislich der Begründung einerseits Vorschriften, die den im Tenor für verfassungswidrig erklärten Vorschriften ähnlich sind sowie Übermittlungsvorschriften zwischen Sicherheitsbehörden.

4.2.1 Auswirkungen auf das RED-G

Vorschriften, die den angegriffenen Vorschriften ähnlich sind, enthält das Rechtsextremismus-Datei-Gesetz (RED-G), das in wesentlichen Teilen dem ATDG nachgebildet ist. Der Rechtsextremismusdatei (RED) kommen im Phänomenbereich des gewaltbezogenen Rechtsextremismus im Wesentlichen die gleichen Funktionen zu wie der ATD im Hinblick auf den internationalen Terrorismus. Anders als beim ATDG treten die Regelungen des RED-G, auch wenn sie den für verfassungswidrig erklärten ATDG-Vorschriften entsprechen, nicht zum 01.01.2015 automatisch außer Kraft. Da sie in diesen Fällen aber materiell verfassungswidrig wären, könnten sie mit den im BVerfGG vorgesehenen Verfahren angegriffen werden. Ohne verfassungskonforme Neuregelung dürften sie nach dem 31.12.2014 auch keine hinreichende Rechtsgrundlage mehr für ein hierauf basierendes Handeln der Behörden darstellen. Im Einzelnen:

4.2.1.1 Teilnahme weiterer Behörden (§ 1 Abs. 2)

Die Regelung des § 1 Abs. 2 RED-G ist mit § 1 Abs. 2 ATDG, soweit das BVerfG die Regelung beanstandet hat, wortgleich. Auch hier sollte daher zukünftig eine Verordnungsermächtigung vorgesehen werden (s. oben S. 14).

4.2.1.2 Kontaktpersonen (§ 2 Satz 1 Nr. 3 RED-G)

Die Regelung zu den zu speichernden Kontaktpersonen unterscheidet sich von der für verfassungswidrig erklärten Vorschrift des ATDG. Kontaktpersonen dürfen in der RED einschränkend nur dann gespeichert werden, wenn sie den Sicherheitsbehörden „*aufgrund von Tatsachen als Angehörige der rechtsextremistischen Szene bekannt sind.*“ Hierdurch wird der Kreis der betroffenen Personen gegenüber der ATD deutlich eingeschränkt, da die Person nicht nur in einem dauerhaften, nicht flüchtigen Kontakt zu einer Hauptperson stehen muss, sondern selbst ein „*Funktionär oder Mitglied einer rechtsextremistischen Gruppierung … oder sonst als Angehörige der rechtsextremistischen Szene bekannt“* sein muss (amtl. Begründung, BT-Drs. 17/8672, S. 13).

Durch diese Einschränkung ist ausgeschlossen, dass rein private, geschäftliche oder berufliche Kontakte genügen, um in der RED gespeichert zu werden. Nur wer selber der rechtsextremistischen Szene angehört, muss damit rechnen, als Kontaktperson gespeichert zu werden. Hinsichtlich dieser Zugehörigkeit genügt auch nicht eine bloße Vermutung, sondern sie muss den zuständigen Behörden aufgrund von Tatsachen bekannt sein, also beispielsweise der Mitgliedschaft in einer rechtsextremistischen Gruppierung oder der regelmäßigen Teilnahme an rechtsextremistischen Veranstaltungen.

Damit greift die Kritik, die das BVerfG an der weiteren Fassung des § 2 Satz 1 Nr. 3 ATDG geübt hat (Rz. 164), hinsichtlich der RED gerade nicht. Vielmehr ist es nach § 2 Satz 1 Nr. 3 RED-G für den Betroffenen vorhersehbar, dass er als Angehöriger der rechtsextremistischen Szene, auch wenn er selbst keinen Gewaltbezug aufweist, möglicherweise als Kontaktperson gespeichert werden kann. Durch die gewählte

Formulierung genügt die Vorschrift, wie ausgeführt, sowohl dem Bestimmtheitsgrundsatz als auch dem Verhältnismäßigkeitsprinzip.

Damit ist die Regelung des § 2 Satz 1 Nr. 3 RED-G verfassungskonform und bedarf keiner Änderung.

4.2.1.3 § 2 Satz 1 Nr. 1 b) und Nr. 2 RED-G („Befürworter von Gewalt“ und „Unterstützer von Unterstützern“).

a) Eine dem § 2 Satz 1 Nr. 1 b) ATDG (Unterstützung von Gruppierungen) entsprechende Regelung gibt es im RED-G nicht, insoweit ergibt sich auch kein Änderungsbedarf.

b) § 2 Satz 1 Nr. 2 RED-G unterscheidet sich vom beanstandeten § 2 Satz 1 Nr. 2 ATDG insoweit, als gerade das vom BVerfG beanstandete Tatbestandsmerkmal des „Befürwortens von Gewalt“ nicht enthalten ist. Auch insoweit ergibt sich daher kein Änderungsbedarf.

c) Die Hinweise des Gerichts zur verfassungskonformen Auslegung des Begriffs des „Hervorrufens rechtswidriger Gewalt“ gelten auch für das RED-G.

4.2.1.4 § 5 Abs. 1 Satz 2 Nr. 1 a) (Inverssuche) und § 7 (erweiterte Datennutzung) RED-G

a) § 5 Abs. 1 Satz 2 Nr. 1 a) RED-G ist mit der entsprechenden Vorschrift im ATDG wortgleich. Insoweit ist diese ebenso wie die ATDG-Vorschrift zu ändern.

b) Darüber hinaus schließt auch die Definition der erweiterten Datennutzung in § 7 Abs. 2 RED-G nicht aus, dass im Rahmen derartiger Projekte durch die Eingabe allein von erweiterten Grunddaten die Daten zu bestimmten Personen ausgegeben werden können. Dies ist ausweislich des Urteils (Rz. 198 f.) grundsätzlich nicht zulässig. Allerdings bleibt eine Inverssuche dann verfassungsrechtlich zulässig, wenn die Voraussetzungen, unter denen sie gesetzlich gestattet wird, hinreichend eng gefasst sind (Rz. 203). So genügte dem Gericht die Einschränkung auf Zwecke zum Schutz von Leib, Leben, Gesundheit oder Freiheit von Personen sowie von Sachen

von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, in § 5 Abs. 2 ATDG.

Auch ist § 7 RED-G hinsichtlich der Tatbestandsvoraussetzungen deutlich enger gefasst als § 5 Abs. 1 ATDG. Voraussetzung ist, dass die Nutzung der Daten im Rahmen eines bestimmten Projekts zur Sammlung und Auswertung von Informationen über konkrete rechtsextremistische Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten, oder zur Verfolgung gewaltbezogener rechtsextremistischer Straftaten im Einzelfall erforderlich ist, um weitere Zusammenhänge aufzuklären. § 7 Abs. 1 Satz 3 enthält hinsichtlich der Verhütung oder Verfolgung von Straftaten zudem einen abschließenden Katalog, der sich auf Straftaten beschränkt, die einen Gewaltbezug enthalten. Durch diesen Katalog sowie die Einschränkung auf rechtsextremistische Bestrebungen, die Gewalttaten ausüben oder vorbereiten, ist sichergestellt, dass als Zweck nur die Abwehr von Gefahren für oder Verfolgung von Straftaten gegen Leib, Leben oder Freiheit von Personen in Betracht kommen.

Zwar ist § 7 gegenüber der Eilfallregelung insoweit deutlich weiter gefasst, dass der Zugriff auf die Daten für diesen Zweck nicht unerlässlich im Sinne eines Eilfalles sein muss. Dies wird in § 7 allerdings insoweit kompensiert, als die Nutzung nur im Rahmen von befristeten Projekten zulässig ist, die jeweils auf Antrag zu genehmigen sind. Im Rahmen des Genehmigungsverfahrens besteht die Möglichkeit, die Voraussetzungen für eine Datenübermittlung zu prüfen und ggf. den Datenbestand für das Projekt sowie die Art und Weise der Datenauswertung zu begrenzen, um für den jeweiligen Einzelfall den Vorgaben der fachgesetzlichen Übermittlungsvorschriften sowie des informationellen Trennungsprinzips zu genügen.

Damit ergibt sich für § 7 RED-G kein Änderungsbedarf.

4.2.1.5 § 3 Abs. 1 Satz 1 Nr. 1 b (erweiterte Grunddaten) und § 10 Abs. 1 (Berichtspflichten).

a) Die Vorschriften des § 3 Abs. 1 Satz 1 Nr. 1 b) gg) (besondere Fähigkeiten), ii) (sicherheitsempfindliche Tätigkeit), und ll) (besuchte Orte) RED-G entsprechen den

beanstandeten Regelungen in der ATD (Buchst. ii), kk), nn)). Diesbezüglich ist daher auch eine konkretisierende Verwaltungsvorschrift vorzusehen und zu veröffentlichen (s. oben S. 17). Regelungen, die dem § 3 Abs. 1 Satz 1 Nr. 1 b) gg) und hh) ATDG entsprechen, gibt es im RED-G nicht. Die nicht im ATDG enthaltene Datenkategorie „besuchte rechtsextremistische Konzerte und sonstige Veranstaltungen“ nach § 3 Abs. 1 Satz 1 Nr. 1 b) Buchst. qq) RED-G ist hingegen gegenüber der Kategorie der „besuchten Orte“ klar und eng genug gefasst und bedarf keiner zwingenden Konkretisierung.

b) Die Vorgaben des Gerichts zu den verpflichtenden turnusmäßigen Datenschutzkontrollen sowie den Berichtspflichten des BKA beziehen sich auf die Datei insgesamt und sind daher ohne weiteres auf das RED-G zu übertragen. Dasselbe gilt für die Ausführungen zur Gewährleistung einer Kooperation bei der Datenschutzkontrolle.

4.2.1.6 Verdeckte Speicherung von Daten aus Eingriffen in Art. 10, 13 GG

Analog zur ATD ist schließlich vorzusehen, dass zukünftig personenbezogene Daten, die durch verdeckte Eingriffe in Art. 10 oder 13 GG oder das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewonnen wurden, nur verdeckt oder beschränkt eingestellt werden (s. oben S. 19).

4.2.1.7 Verhältnismäßigkeit der RED als solcher

Ein wesentlicher Unterschied zur ATD besteht schließlich in der Zielrichtung der Datei. Während die Speicherung von personenbezogenen Daten in der ATD der Aufklärung oder Bekämpfung des internationalen Terrorismus dient, woran nach dem Urteil des BVerfG ein gewichtiges öffentliches Interesse besteht (R. 175), dient die RED der Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus, also ggf. auch der Verhütung oder Verfolgung von Straftaten, die zwar einen Gewaltbezug aufweisen, aber gegenüber terroristischen Taten weniger schwer wiegen. Allerdings war die Einrichtung der RED die unmittelbare Reaktion auf die Aufdeckung der Straftaten des sog. „Nationalsozialistischen Untergrunds“. Diese hat deutlich gemacht, dass gerade im Phänomenbereich Rechtsextremismus die Täter zunächst mit einfa-

cheren Gewaltdelikten aufgefallen sind, um anschließend von den Behörden über mehrere Jahre unbemerkt eine beispielslose Reihe von terroristischen Morden zu begehen. Vor diesem Hintergrund liegt die etwas weitere Zielrichtung der Bekämpfung des gewaltbezogenen Rechtsextremismus ebenfalls in einem gewichtigen öffentlichen Interesse.

4.2.2 Auswirkungen auf die Übermittlungsvorschriften

Während es beim RED-G angesichts des oftmals gleichen Wortlauts auf der Hand liegt, dass die angegriffenen Vorschriften sich auch hier wiederfinden und im ähnlichen Umfang mit der Verfassung vereinbar oder nicht vereinbar sind, ist der Prüfauftrag des BVerfG im Hinblick auf die Übermittlungsvorschriften deutlich vager: Der Gesetzgeber soll prüfen, ob er *eventuell* die Änderung von Datenübermittlungsvorschriften *einzelner* Sicherheitsbehörden *für angezeigt* hält.

Damit wird der Prüfauftrag sprachlich gleich dreifach abgeschwächt: Anpassungen kann es offenbar auch nach Auffassung des Gerichts nur möglicherweise geben, wenn beträfen sie nur einzelne Vorschriften, und die eventuellen Anpassungen sind auch nicht geboten oder erforderlich, was der übliche Sprachgebrauch für eine verfassungswidrige Vorschrift wäre, sondern lediglich möglicherweise angezeigt.

4.2.2.1 Informationelles Trennungsprinzip

Hintergrund für diesen Prüfauftrag sind die Ausführungen des Gerichts zum von ihm so benannten „informationellen Trennungsprinzip“ (LS 2, Rz. 123), das vom Gericht im Hinblick auf die unterschiedlichen Aufgaben und Befugnisse von Polizeibehörden einerseits und Nachrichtendiensten andererseits aus dem Grundrecht auf informationelle Selbstbestimmung abgeleitet wird (Rz. 122, 123). Während der Polizei überwiegend die klassischen Aufgaben auf den Gebieten der Gefahrenabwehr und Strafverfolgung zukommen, gehört zu den Aufgaben der Verfassungsschutzbehörden die Sammlung und Auswertung von Informationen über verfassungsfeindliche Bestrebungen, über sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht, über Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden und über Bestrebungen gegen den Gedanken der Völkerverständigung (§ 3 Abs. 1 BVerfSchG), um Gefahren für diese Rechtsgüter frühzeitig zu erkennen und – ggf. im Zusammenwirken mit der Polizei – zu verhindern.

So finden sich in den Urteilsgründen immer wieder Ausführungen dazu, dass Nachrichtendienste unter geringeren Voraussetzungen Informationen erheben dürfen als Polizei- und Strafverfolgungsbehörden, demgegenüber letzteren aber die schwereren Eingriffsbefugnisse im Hinblick auf Leib, Leben und Freiheit einer Person zustehen. Auch erfolge die Informationserhebung der Nachrichtendienste grundsätzlich verdeckt, während die Polizei – jedenfalls im Grundsatz – offen vorgeht.

So führt das BVerfG unter anderem aus, dass das Eingriffsgewicht der ATD insbesondere dadurch erhöht sei, dass der Informationsaustausch zwischen „*Sicherheitsbehörden mit zum Teil deutlich verschiedenen Aufgaben und Befugnissen ermöglicht*“ werde, „*insbesondere (…) zwischen Nachrichtendiensten und Polizeibehörden“* (Rz. 112).

Weiter erläutert das Gericht: „*Die Aufgliederung der Sicherheitsbehörden nach fachlichen und föderalen Gesichtspunkten entfaltet damit für den Datenschutz auch eine besondere grundrechtliche Dimension. Dass Informationen zwischen den verschiedenen Sicherheitsbehörden nicht umfassend und frei ausgetauscht werden, ist nicht Ausdruck einer sachwidrigen Organisation dieser Behörden, sondern von der Verfassung durch den datenschutzrechtlichen Grundsatz der Zweckbindung grundsätzlich vorgegeben und gewollt.*“ (Rz. 113).

Im Ergebnis handelt es sich damit beim „informationellen Trennungsprinzip“ um eine Konkretisierung des schon im Volkszählungsurteil entwickelten Zweckbindungsprinzips. Dies wird aus der Herleitung in den Rz. 113 und 114 besonders deutlich, in denen das Gericht sehr häufig die Begriffe „Zweckbindung“ oder „Zweckänderung“ verwendet.

Besonderes Augenmerk legt das Gericht auf die Datenübermittlung durch die Nachrichtendienste an die Polizeibehörden für ein mögliches „operatives Tätigwerden: Der Austausch von Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden muss deshalb grundsätzlich einem herausragenden öffentlichen Interesse dienen, das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebot stehen, rechtfertigt (Rn. 123). Mit „operativem Tätigwerden“ ist dabei offenbar ein Tätigwerden ge-

meint, das mit einem schwerwiegenden Grundrechtseingriff verbunden ist, wie es üblicherweise durch die Polizei erfolgt, namentlich die Anwendung von unmittelbarem Zwang (Rz. 120). Demgegenüber sei die durch die ATD ermöglichte bloße „Informationsanbahnung“ von einem deutlich geringerem Eingriffsgewicht (Rz. 127).

Der Austausch von Daten für ein mögliches operatives Tätigwerden muss nach den Urteilsgründen dann einem herausragenden öffentlichen Interesse dienen, wenn der „*Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebote stehen“*, erfolgt. „*Die Eingriffsschwellen für die Erlangung der Daten dürfen hierbei nicht unterschritten werden*“ (Rz. 123). Für Datenübermittlungen zwischen den Nachrichtendiensten und der Polizei bedeutet dies, dass sich entsprechende Übermittlungsregelungen *„jedenfalls (…) nicht mit vergleichbar niederschwelligen Voraussetzungen wie der Erforderlichkeit für die Aufgabenwahrnehmung oder der Wahrung öffentlicher Sicherheit begnügen*“ dürfen (Rz. 126 aE). Dies bedeutet im Ergebnis, dass bei der Beurteilung von Übermittlungsvorschriften einerseits danach differenziert werden muss, ob die Informationsübermittlung ein operatives Tätigwerden zum Ziel hat, zum anderen, ob die Informationen unter erleichterten Bedingungen erlangt wurden, die der empfangenden Behörde nicht zur Verfügung stünden. Mit letzterem sind offenbar insbesondere die nachrichtendienstlichen Mittel der Informationsgewinnung im Sinne des § 8 Abs. 2 BVerfSchG gemeint, also „Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen“ (vgl. auch Rz. 117).

Hieraus folgt, dass insbesondere die Übermittlung von Nachrichtendiensten an Polizeien einer Überprüfung bedarf, ob diese den Grundsätzen des informationellen Trennungsprinzips genügen, wie sie das Gericht aufgestellt hat. Gegenstand der Prüfung müssen die in der Entscheidung ausgeführten Kriterien für den Austausch von Daten zwischen Nachrichtendiensten und Polizei sein:

- Die Aufhebung der Datentrennung zwischen Nachrichtendiensten und Polizeibehörden ist nur ausnahmsweise zulässig (Rz. 123).
- Die Übermittlung mit dem Ziel eines operativen polizeilichen Tätigwerdens von Informationen, die mit nachrichtendienstlichen Mitteln gewonnen wurden, bedarf

einer höheren Rechtfertigung als der bloßen Aufgabenwahrnehmung oder der Wahrung der öffentlichen Sicherheit (Rz. 123, 126).

- Der Austausch von Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden muss grundsätzlich einem herausragenden öffentlichen Interesse dienen, das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebot stehen, rechtfertigt (Rz. 123).
- Die Eingriffsschwellen für die Erlangung der Daten durch die empfangende Behörde dürfen dabei nicht unterlaufen werden (Rz. 123).

Wie genau die Schwelle für eine Übermittlung nachrichtendienstlicher Erkenntnisse an Polizeibehörden mit dem Ziel eines operativen Tätigwerdens formuliert werden muss, gibt das Gericht nicht vor. Es formuliert in Rz. 126 lediglich, wann die Übermittlungsschwelle unterschritten würde. Bei einer Gesamtschau der Ausführungen insbesondere unter den Rz. 116 bis 123 ergibt sich aber, dass das Gericht erkennbar auf die unterschiedlichen Schwellen für ein Tätigwerden von Polizeibehörden einerseits und Nachrichtendiensten andererseits abstellt. Nachrichtendienste dürfen bereits im Vorfeld von Gefährdungslagen Aufklärung betreiben, ohne dass es eines konkreten Gefahrverdachts bedarf (Rz. 116 ff.), haben demgegenüber aber keine operativen Befugnisse. Polizeibehörden haben hingegen operative Befugnisse einschließlich der Möglichkeit, Maßnahmen auch mit Zwang durchzusetzen; Voraussetzung für die Ausübung dieser Befugnisse ist aber in der Regel, dass Anhaltspunkte für einen Tatverdacht oder eine Gefahr vorliegen (Rz. 120).

Dabei stellt das Gericht hinsichtlich der Schwelle offenbar nicht auf die tatsächlich – und ggf. in den Fachgesetzen sehr unterschiedlich – geregelten Erhebungsvoraussetzungen ab, sondern auf die jeweils verfassungsrechtlich gebotene Schwelle (vgl. auch Rz. 228). Da seine Argumentationslinie grundrechtlich – nicht kompetenzrechtlich – basiert ist, ist die verfassungsbezogene Anknüpfung auch zwingend, denn der einfache Gesetzgeber kann nicht grundrechtliche Anforderungen normieren. Daher wäre es unverständlich, wenn eine Spontanübermittlung einer Verfassungsschutzbehörde in unterschiedliche Bundesländer aus grundrechtlicher Sicht unterschiedlichen Anforderungen unterliegen sollte. Der Eingriffsakt der Verfassungsschutzbehörde ist derselbe. Zu erwägen sein könnte allenfalls, dass der Eingriff als nicht erforderlich zu

qualifizieren wäre, wenn der Empfänger die Information nicht verwenden dürfte, weil er sie selbst mit dem von der Verfassungsschutzbehörde verwendeten Mittel nach Landesrecht nicht hätte erheben dürfen. Dies ist vorgängig eine Frage der Auslegung des Landesrechts. Solche Auslegung erschiene allerdings generell fernliegend. Es gibt keinen derartigen allgemeinen Datenschutzgrundsatz. Umgekehrt erscheint völlig unstreitig, dass beispielsweise Informationen, die eine Stelle aufgrund bestehender Zeugenpflichten erlangt hat, auch an Stellen weitergeben dürfte, gegenüber denen solche Pflichten nicht bestehen (vgl. etwa StPO); es werden insoweit typischerweise nur Zweckbegrenzungen getroffen. Weitergehende Einschränkungen sind im Fachrecht die Ausnahme (z.B. Steuergeheimnis), die normenklarer Regelung bedarf.

Damit ist Voraussetzung für eine Übermittlung von mittels nachrichtendienstlicher Methoden erlangter Erkenntnisse an Polizeibehörden, dass diesbezüglich ein Anfangsverdacht im Sinne des § 160 Abs. 1 StPO, eine konkrete Gefahr im Sinne der einschlägigen polizeirechtlichen Regelungen oder eine sonstige Befugnis vorliegt, die ein polizeiliches Tätigwerden im Vorfeld der Gefahr gestattet.

Ein Unterlaufen der Eingriffsschwellen ist insbesondere dann denkbar, wenn für die entsprechende Datenerhebung für die Polizeibehörden von Verfassung wegen höhere Schwellen als der Anfangsverdacht oder Gefahrverdacht gelten. Als Beispiel kann hier die Telekommunikationsüberwachung für Zwecke der Strafverfolgung genannt werden, da dieses Ermittlungsinstrument nur statthaft ist, wenn ein durch bestimmte Tatsachen begründeter Verdacht einer auch im Einzelfall schweren und in einem vom Gesetzgeber abschließend aufgestellten Katalog enthaltenen Straftat vorliegt, was zudem im Rahmen der Anordnung durch einen richterlichen Beschluss festgestellt werden muss. Eine Übermittlung von personenbezogenen Daten, die durch nachrichtendienstliche Telekommunikationsüberwachungsmaßnahmen nach dem Artikel 10-Gesetz gewonnen wurden, zur Verfolgung minder schwerer Straftaten an die zuständige Strafverfolgungsbehörde wäre damit insoweit unzulässig, wie es dem einfachen Gesetzgeber von Verfassung wegen verschlossen wäre, die empfangende Stelle zur Erhebung dieser Informationen mit dem eingesetzten Mittel (der TKÜ) zu befugen. Insoweit ist zunächst also zu bedenken, dass der Katalog des §100a StPO möglicherweise nicht abschließend den verfassungsrechtlich zulässigen Rahmen strafverfahrensrechtlicher Telekommunikationsüberwachung bezeichnet.

Durch die Formulierung, die Schwellen dürften nicht „unterlaufen“ werden, hat das Gericht bereits deutlich gemacht, dass es für die Übermittlungsschwellen nicht auf eine Eins-zu-eins-Abbildung der bestehenden einfachgesetzlichen Erhebungsschwellen ankommt. Im Übrigen können Schwellen der Erhebung durch Übermittlung im unmittelbaren Sinn nur dann unterlaufen werden, wenn der Eingriffsgegenstand derselbe ist. Für die grundrechtliche Würdigung ist dabei von Bedeutung, dass typische verdeckte Erhebungsmittel, für die auch Polizeien über Befugnisse verfügen (wie die Telekommunikationsüberwachung oder längerfristige Observation) Erforschungseingriffe sind, die nicht gezielt die erforderlichen Informationen erheben, sondern mit hoher Streubreite, u.U. über Monate, in breite Lebenswelten der Privatheit eindringen (nicht nur beim nachrichtendienstlichen, sondern ebenso beim polizeilichen Einsatz). In der Relation des Erkenntnisvolumens erbringen diese Maßnahmen typischerweise nur in sehr untergeordnetem Umfang relevante Erkenntnisse. Dieser Eingriffstypizität trägt der einfache Gesetzgeber durch entsprechend hohe Eingriffschwellen Rechnung. Diese Verhältnismäßigkeitsrelation wäre auf den Übermittlungsvorgang nur dann zu übertragen, wenn das gesamte Erkenntnisaufkommen der Maßnahme – also das komplette Rohdatenvolumen einer TKÜ – übermittelt werden würde. Dies ist in der Zusammenarbeit der Nachrichtendienste mit den Polizeien jedoch nicht der Fall. Tatsächlich geht der Übermittlung die Auswertung voraus, die strikt das Relevante vom Irrelevanten trennt. Der Übermittlungsgegenstand hat demnach gerade nicht mehr die Streuung, die die Erhebungsschwelle mit veranlasst hat, sondern ist gezielt auf das zur Erfüllung der Empfängeraufgaben Erforderliche beschränkt. Ein solcher Übermittlungseingriff in die informationelle Selbstbestimmung ist unter grundrechtlichen sowie Verhältnismäßigkeitserwägungen wesentlich anders zu bewerten, als der zugrunde liegende Erhebungseingriff. Angesichts der unterschiedlichen Eingriffstiefe wäre es danach auch nicht von Verfassung wegen zu beanstanden, wenn für die Übermittlung der bereits erforderlichkeitsgefilterten Informationen niedrigere Schwellen gelten würden, als für die Ausforschungserhebung, die in breitem, weit überwiegenden Umfang Informationen einschließt, die zur weiteren Aufgabenwahrnehmung nicht erforderlich sind. Bei unterschiedlichen Gegenständen des Datenumgangs ist ausgeschlossen, den Übermittlungseingriff mit dem Erhebungseingriff gleichzusetzen. Dann kann die Übermittlung auch nicht die Erhebungsschwelle unterlaufen.

4.2.2.2 Zwischenergebnis

Die Überprüfung der Übermittlungsvorschriften kann sich damit im Wesentlichen auf die Vorschriften zur Übermittlung von Informationen von Nachrichtendiensten an Polizeibehörden beschränken, da das vom BVerfG beschriebene Gefälle zwischen erleichterten Erhebungsbefugnissen und operativen Eingriffsbefugnissen nur in dieser Richtung besteht. Die Regelungen auf Bundesebene finden sich dabei im BVerfSchG sowie im G10-Gesetz. MAD-Gesetz und BND-Gesetz verweisen insoweit lediglich auf das BVerfSchG.

Die Vorschriften müssen folgende Kriterien erfüllen:
a) Die Übermittlung personenbezogener Daten, die mit nachrichtendienstlichen Mitteln gewonnen wurden, mit dem Ziel eines operativen polizeilichen Tätigwerdens ist nur zulässig, wenn der Verdacht einer Straftat, eine Gefahr oder eine sonstige Befugnis, die ein polizeiliches Tätigwerden im Vorfeld der Gefahr gestattet, vorliegen.
b) Wenn für die Form der Informationsbeschaffung verfassungsrechtlich höhere materielle Schwellen geboten sind, dürfen diese nicht unterlaufen werden.
c) Die Durchbrechung dieses Trennungsprinzip durch die Übermittlung von personenbezogenen Daten, die durch Nachrichtendienste unter (gegenüber den der empfangenden Polizeibehörde zustehenden Befugnissen) erleichterten Bedingungen gewonnen wurden, muss grundsätzlich einem herausragenden öffentlichen Interesse dienen.
d) Keiner über die Vorgaben des allgemeinen Zweckbindungsprinzips hinausgehenden Voraussetzungen bedarf hingegen die Übermittlung von personenbezogenen Daten, die offen oder gar aus öffentlich zugänglichen Quellen gewonnen wurden.
e) Dasselbe gilt für die Übermittlung von Polizei- und Strafverfolgungsbehörden an die Verfassungsschutzbehörden. Da und soweit der Polizei keine erleichterten Möglichkeiten der Datenerhebung und den Verfassungsschutzbehörden keine operativen Befugnisse in Form der Ausübung unmittelbaren Zwangs zustehen, genügt hier die Erforderlichkeit für die Aufgabenerfüllung als Übermittlungsvoraussetzung.
f) Auch die Übermittlung durch Verfassungsschutzbehörden an andere öffentliche Stellen, die keine operativen Befugnisse wie die Polizei haben, ist unverändert möglich. Diese können schon dem Grundgedanken nach nicht vom Trennungsprinzip

erfasst werden, da dieses nur zwischen Verfassungsschutzbehörden und Polizei- und Strafverfolgungsbehörden besteht.

4.2.2.3 Änderungsbedarf im BVerfSchG

Im BVerfSchG regeln die §§ 19 und 20 die Übermittlung von Daten an Polizeibehörden.

a) § 19 Abs. 1 BVerfSchG regelt allgemein die Datenübermittlung an inländische öffentliche Stellen. Danach darf das Bundesamt für Verfassungsschutz personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt. Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

Damit sind auch Polizei- und Strafverfolgungsbehörden von der Regelung umfasst, auch soweit die Datenübermittlung mit dem Ziel der operativen Aufgabenerfüllung erfolgt. Voraussetzung für die Datenübermittlung ist, dass dies zur Erfüllung der Aufgaben (des BfV) erforderlich ist oder der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt.

Soweit die Übermittlung zum Schutz der freiheitlich demokratischen Grundordnung erfolgt, handelt es sich letztlich nicht um eine zweckändernde Übermittlung, da die Daten bereits zu diesem Zweck erhoben wurden, so dass das informationelle Trennungsprinzip als Ausprägung des Zweckbindungsgebots nicht greift. Auch steht der Schutz der freiheitlichen demokratischen Grundordnung zweifelsfrei in einem herausragenden öffentlichen Interesse. Dasselbe gilt für die Übermittlung zum Zweck der Aufgabenerfüllung des BfV. Allerdings ist in diesem Fall nicht ausgeschlossen, dass auch eine solche Übermittlung zugleich operative Maßnahmen der Polizeibehörden auslöst – nämlich dann, wenn die beobachteten Bestrebungen in eine konkrete Gefahrenlage übergehen.

Problematisch ist die Voraussetzung der *Zwecke der öffentlichen Sicherheit*. Nach dem Wortlaut der Norm ist damit eine Übermittlungsschwelle definiert, die nach den Ausführungen in Rz. 126 der Entscheidung nicht mehr genügen soll.

Die Norm kann aber verfassungskonform ausgelegt werden. Die vom BVerfG festgestellte Maßgabe, dass Übermittlungsbefugnisse Erhebungsschwellen nicht unterlaufen dürfen, muss bei verfassungskonformer Anwendung dazu führen, dass kumulativ neben den Übermittlungsvoraussetzungen auch die empfängerseitigen Erhebungsvoraussetzungen zu prüfen sind. Dazu können als normenklare Grundlage de lege lata nur die jeweiligen Fachgesetze für die empfangende Stelle herangezogen werden. Soweit Polizei- oder Strafverfolgungsbehörden personenbezogene Daten erheben dürfen, erfordern diese Erhebungsbefugnisse aber in aller Regel zumindest einen Tat- oder Gefahrverdacht (vgl. § 20b Abs. 1 BKAG, der eine Erhebung nur zur Erfüllung der Aufgaben des BKA nach § 4a Abs. 1 BKAG gestattet, wobei § 4a Abs. 1 BKAG als Aufgaben die Abwehr von Gefahren des internationalen Terrorismus sowie die Verhütung von Straftaten im Sinne des § 129a StGB definiert). Ein solcher konkreter Verdacht ist nach den Ausführungen des Gerichts auch die verfassungsrechtlich gebotene Erhebungsschwelle für Übermittlungen von mit nachrichtendienstlichen Mitteln gewonnenen personenbezogenen Daten. Dabei muss die übermittelnde Stelle allerdings keine zusätzlichen Ermittlungen anstellen; Prüfungsmaßstab kann allein die Bewertung des Verfassungsschutzes auf der Grundlage seiner Informationsbasis sein.

Daher ist für mit nachrichtendienstlichen Mitteln gewonnene Erkenntnisse eine Übermittlung an Polizeibehörden mit dem Ziel eines operativen polizeilichen Tätigwerdens nach § 19 Abs. 1 BVerfSchG nur zulässig, wenn dies zur Verfolgung von Straftaten oder zur Abwehr von Gefahren notwendig ist oder eine sonstige Befugnis ein polizeiliches Tätigwerden im Vorfeld der Gefahr gestattet.

Des Weiteren dürfen möglicherweise höhere Erhebungsschwellen der empfangenden Behörde nicht unterlaufen werden. Dabei entsteht nach der Entscheidung des BVerfG ein Stufenverhältnis:

- Bei personenbezogenen Daten aus allgemein zugänglichen Quellen bedarf es keiner weiteren Voraussetzungen. Dasselbe gilt für Erkenntnisse aus kurzfristigen Observationen, die nach StPO und Gefahrenabwehrrecht ebenfalls keinen besonderen rechtlichen Voraussetzungen unterliegen.
- Bei personenbezogenen Daten, die durch nachrichtendienstliche Mittel im Sinne des § 8 Abs. 2 BVerfSchG erlangt wurden, ist danach zu differenzieren, welche Instrumente der verdeckten Informationsbeschaffung nach der StPO bzw. dem Gefahrenabwehrrecht mit diesen Mitteln vergleichbar sind und ob diese ggf. höheren verfassungsrechtlich gebotenen Schwellen begegnen. In diesen Fällen müssen grundsätzlich diese höheren Schwellen auch für die Übermittlung vom Nachrichtendienst an die Polizei erfüllt sein.
    - Bei personenbezogenen Daten aus offenen Quellen, die auch die Polizei- und Strafverfolgungsbehörden im Rahmen der jeweiligen Generalklauseln erheben dürften, bedarf es keiner weiteren Voraussetzungen.
    - Auch sind Aussagen von Vertrauens- oder Gewährspersonen im Rahmen eines Strafverfahrens grundsätzlich mit Aussagen von Zeugen oder Anzeigeerstattern vergleichbar und bedürfen daher keiner höheren Schwellen als denen des Anfangsverdachts (vgl. BGHSt 41, 42). Die Tatsache, dass Vertrauenspersonen aus einer anderen Motivation heraus aussagen und in der Regel nur der V-Mann-Führer als Zeuge vom Hörensagen zur Verfügung steht, ist bei der Beurteilung der Glaubwürdigkeit des Zeugen sowie der Glaubhaftigkeit der Zeugenaussage entsprechend zu berücksichtigen. In den Polizeigesetzen unterliegt der Einsatz von Vertrauenspersonen hingegen teilweise höheren Hürden, die dann auch im Falle der Übermittlung beachtet werden müssten, vgl. § 20g Abs. 2 Nr. 4 BKAG.
    - Längerfristige Observationen sowie Bild- und Tonaufzeichnungen sind sowohl nach der StPO als auch den Polizeigesetzen von Bund und Ländern nur unter höheren rechtlichen Voraussetzungen zulässig (§§ 163 f StPO, 20g Abs. 2 Nr. 1 für längerfristige Observationen, §§ 100f, 100h StPO bzw. 20g Abs. 2 Nr. 2 BKAG für Ton- und Bildaufnahmen). Aufgrund des für den Betroffenen intensiveren Grundrechtseingriffs durch solche Maßnahmen, ist hier eine höhere Übermittlungsschwelle vermutlich auch verfassungsrechtlich angezeigt.

- Maßnahmen, die aufgrund ihrer Eingriffsintensität besonders hohen verfassungsrechtlich gebotenen Hürden unterliegen, sind schließlich solche der Telekommunikationsüberwachung. Soweit Nachrichtendienste Erkenntnisse aus Eingriffen in Art. 10 GG haben, richtet sich deren Übermittlung allerdings nach dem Artikel 10-Gesetz. Dieses sieht für die Übermittlung von Erkenntnissen aus G10-Maßnahmen eigene Übermittlungsvorschriften vor, die denen des BVerfSchG als lex specialis vorgehen und wesentlich höhere Hürden für die Übermittlung vorsehen (hierzu näher unten S. 38).

Damit genügt die materielle Regelung zur Datenübermittlung an Polizeibehörden des § 19 Abs. 1 BVerfSchG grundsätzlich den Erfordernissen des informationellen Trennungsprinzips. Allerdings erschließt sich dieser Regelungsgehalt nicht alleine aus der Lektüre des § 19 Abs. 1 BVerfSchG, sondern nur in der Gesamtschau mit der jeweils einschlägigen Erhebungsbefugnis der empfangenden Stelle und müsste in Umsetzung des Urteils ggf. durch entsprechende Anwendungserlasse für die Anwender handhabbarer ausgestaltet werden.

Insoweit wäre eine Änderung des § 19 Abs. 1 BVerfSchG zwar nicht verfassungsrechtlich geboten, rechtspolitisch aber wünschenswert. Dabei sollte auch der rechtspolitischen Empfehlung der Bund-Länder-Kommission Rechtsterrorismus zur Harmonisierung der Übermittlungsregelungen Rechnung getragen werden. Die derzeitige verfassungskonforme Auslegung ist darauf verwiesen, das jeweilige Landesfachrecht heranzuziehen. Übermittelt das BfV ohne Ersuchen an Polizeien verschiedener Länder, kann das dazu führen, dass dies an unterschiedlichen Voraussetzungen zu messen ist. Dies läuft dem sachgerechten Harmonisierungsanliegen zuwider. Eine einheitliche bundesgesetzliche Regelung muss sich dabei nicht am kleinsten gemeinsamen Nenner des Landesrechts, sondern lediglich an der von Verfassung wegen zu fordernden Erhebungsschwelle orientieren. Letztlich steht dabei wieder die konkrete Verhältnismäßigkeitsabwägung zur Übermittlungsregelung im Vordergrund, da die Übermittlung ungefilterter Rohdaten vollständig lebensfremd ist und dafür folglich auch keine Befugnis benötigt wird.

Bei der Ausgestaltung einer Neuregelung ist darauf zu achten, dass diese handhabbar ist und neben der Wahrung des Trennungsprinzips auch das Ziel im Auge behält, den Informationsaustausch zwischen Polizei- und Verfassungsschutzbehörden dort, wo er geboten ist, zu intensivieren und nicht unsachgemäß zu behindern.

b) Eine weitere Übermittlungsregelung an Polizeibehörden enthalten die §§ 20 Abs. 1 und 21 Abs. 1 BVerfSchG. Im Gegensatz zu § 19 BVerfSchG enthalten diese Regelungen sogar Übermittlungspflichten. Voraussetzung für eine Übermittlung ist nach § 20 Abs. 1 (auf den § 21 insoweit verweist) allerdings, dass tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Verhinderung oder Verfolgung von Staatsschutzdelikten erforderlich ist. Damit ist die durch das informationelle Trennungsprinzip gefordert Übermittlungsschwelle gewahrt.

4.2.2.4 Änderungsbedarf im Artikel 10-Gesetz

Personenbezogene Daten, die aus Beschränkungen nach dem Artikel 10-Gesetz (G 10) gewonnen wurden, unterliegen dem besonderen Datenregime des Artikel 10-Gesetzes. Dies sieht die Möglichkeit der Übermittlung derartiger Erkenntnisse an Polizei- oder Strafverfolgungsbehörden in den §§ 4 Abs. 4 und 7 Abs. 4 G 10 vor. Voraussetzung ist jeweils, dass die Übermittlung der Verhinderung, Aufklärung oder Verfolgung von Straftaten dient und entweder tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der in § 3 Abs. 1 und 1a genannten Straftaten plant oder begeht, oder bestimmte Tatsachen den Verdacht begründen, dass jemand eine sonstige in § 7 Abs. 4 Satz 1 genannte Straftat plant oder begeht. Die in §§ 3 Abs. 1 und 1a sowie § 7 Abs. 4 Satz 1 genannten Straftaten sind bis auf die §§ 83, 305a StGB, 20 Abs. 1 Nr. 1 bis 4 VereinsG, § 35 AWG und § 95 Abs. 1 Nr. 8 AufenthG Katalogstraftaten nach § 100a StPO, so dass im Falle der Übermittlung die materiellen Voraussetzungen für diese gegeben sind.

Hinsichtlich der §§ 83, 305a StGB, 20 VereinsG, 35 AWG und 95 AufenthG muss im Einzelfall geprüft werden, ob diesbezüglich noch die verfassungsrechtlich gebotene Schwelle für eine Übermittlung gewahrt bleibt. Der Straftatenkatalog des § 100a StPO ist durch einfaches Gesetz formuliert und nicht verfassungsrechtlich fest vorgegeben. Die Festlegung eines abweichenden Katalogs im Artikel 10-Gesetz durch

den Gesetzgeber ist – insbesondere im Hinblick auf die Tatsache, dass dieser wesentlich beschränkter und auf die Aufgaben der nach dem Artikel 10-Gesetz befugten Behörden zugeschnitten ist – verfassungsrechtlich nicht ausgeschlossen. Voraussetzung ist, dass die einzelnen Straftaten in ihrem Unwertgehalt mit den schweren Straftaten, wie sie im Katalog des § 100a StPO aufgezählt sind, vergleichbar sind.

4.2.2.5 Eilbefugnisse

Abseits des oben beschrieben Stufenverhältnisses, das nach Herkunft der Erkenntnisse differenziert, müssen aber auch Spontanübermittlungen im Eilfall möglich bleiben. Das BVerfG hat zur Eilfallregelung des § 5 Abs. 2 ATDG ausgeführt, dass die Beschränkung des Nutzungszwecks auf den Schutz von besonders hochwertigen Rechtsgütern, namentlich zum Schutz von Leib, Leben, Gesundheit oder Freiheit von Personen sowie von Sachen mit erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist eine hinreichend hohe Eingriffsschwelle darstellt, die auch die Übermittlung von Erkenntnissen aus verdeckten Eingriffen in Art. 10 oder 13 GG rechtfertigt (Rz. 203). Auch im Übrigen ist, wie oben ausgeführt, eine Durchbrechung des Trennungsprinzips möglich, wenn dies einem herausragenden öffentlichen Interesse dient.

Betrachtet man die bestehenden Übermittlungsvorschriften des Artikel 10-Gesetzes, so stellt man fest, dass es an einer solchen allgemeinen Übermittlungsbefugnis zur Abwehr schwerer Gefahren fehlt. Die Schaffung einer solchen allgemeinen Übermittlungsbefugnis insbesondere für Zufallserkenntnisse, aus denen sich die konkrete Gefahr für besonders hochwertige Rechtsgüter ergibt und ein unverzügliches Eingreifen der zuständigen Polizeibehörden erforderlich macht, sollte daher im Rahmen der Novellierung des Artikel 10-Gesetzes ebenfalls vorgesehen werden.

4.2.3 Auswirkungen auf die Arbeit in gemeinsamen Zentren

Keine Aussage trifft das BVerfG, ob und inwieweit auch der Informationsaustausch zwischen Nachrichtendiensten und Polizeibehörden in den gemeinsamen Zentren (GTAZ, GAR, GETZ und CyberAZ) von der Entscheidung betroffen ist. Die Arbeit des GTAZ, die eng mit der Nutzung der ATD verbunden ist, war Gegenstand sowohl des schriftsätzlichen Vortrags im Verfassungsbeschwerdeverfahren als auch der mündlichen Verhandlung. Gleichwohl hat das BVerfG in Rz. 232 eine Überarbeitung lediglich der Vorschriften, die den angegriffenen Vorschriften im ATDG ähnlich sind, sowie eventuell Datenübermittlungsvorschriften einzelner Sicherheitsbehörden erwähnt. Dies bedeutet im Umkehrschluss, dass das BVerfG Änderungsbedarf hinsichtlich der gemeinsamen Zentren – die ihre Arbeit nicht auf Grund eigener gesetzlicher Regelungen, sondern auf der Grundlage der bestehenden Übermittlungsvorschriften erledigen – nicht gesehen hat. Dies ergibt sich auch aus den Urteilsgründen, und zwar sowohl hinsichtlich der Übermittlungsvorschriften als auch der datenschutzrechtlichen Aufsicht.

4.2.3.1 Übermittlungsvorschriften

a) Soweit im Hinblick auf das informationelle Trennungsprinzip Anpassungen in den gesetzlichen Übermittlungsvorschriften ergeben, gelten diese natürlich unmittelbar auch für die Zentren, da die allgemeinen Übermittlungsvorschriften die Grundlage der Zusammenarbeit sind.

b) Darüber hinaus ergibt sich für die Übermittlung von Daten innerhalb der Zentren letztlich eine ähnliche Einschätzung, wie sie das Gericht für die ATD gefunden hat. Der Austausch in den Zentren dient zum einen der Informationsanbahnung, also der Klärung, welche Behörden hinsichtlich eines konkreten Falls ebenfalls über Informationen verfügen oder aufgrund ihrer örtlichen Zuständigkeit informiert werden müssten. Hierin sieht das BVerfG jedenfalls in Bezug auf die ATD einen nur geringen Grundrechtseingriff (Rz. 124 f.). Unabhängig davon müssen auch für die Übermittlung von Daten im Rahmen der Informationsanbahnung die Voraussetzungen der einschlägigen Übermittlungsvorschriften erfüllt sein. Dabei ist die Schwelle für die Zusammenarbeit in den Zentren nach bestehendem Recht schon insoweit höher, als die Tatbestandsvoraussetzungen der Übermittlungsbefugnisse – und im Gegenzug

auch der Erhebungsbefugnisse – bezüglich aller im Zentrum bzw. der jeweiligen Arbeitsgruppe tätigen Behörden erfüllt sein müssen. Ist dies nicht der Fall, kann ein personenbezogenes Datum nur in einem kleineren Kreis ausgetauscht werden.

Darüber hinaus findet ein Austausch von Daten über die Informationsanbahnung hinaus zur unmittelbaren Nutzung für die Aufklärung und Bekämpfung des Terrorismus statt. Dieser ist dann nur unter den Voraussetzungen der einzelnen Übermittlungsvorschriften zulässig, die wiederum ihrerseits den verfassungsrechtlichen Anforderungen genügen müssen (Rz. 126). Diese Aussagen des BVerfG zur ATD können unmittelbar auf die Arbeit in den Zentren übertragen werden mit der Maßgabe, dass hinsichtlich jeder beteiligten Behörde die Voraussetzungen der Übermittlungsvorschriften erfüllt sein müssen.

4.2.3.2 Datenschutzkontrolle

Wie auch bei der ATD besteht bei den Zentren die Besonderheit, dass Landes- und Bundesbehörden regelmäßig Informationen austauschen, so dass die datenschutzrechtliche Kontrollbefugnis zwischen den verschiedenen Bundes- und Landesbeauftragten für den Datenschutz aufgeteilt ist. Diesbezüglich hat das Gericht aber wie ausgeführt lediglich vorgegeben, dass der Gesetzgeber eine Kooperation der einzelnen Datenschutzbeauftragten ermöglichen muss. Die Ausübung und Ausgestaltung dieser kontrollierenden Kooperation hat das Gericht grundsätzlich den betroffenen Datenschutzbeauftragten aufgegeben. Die zuständigen Landesdatenschutzbeauftragten haben teilweise bereits entsprechende Prüfungen im Nachgang des Urteils angekündigt.

Wie ausgeführt bestehen mit den Regelungen zur Amtshilfe und zur Auftragsdatenverarbeitung die notwendigen Instrumente, um den Beauftragten eine effektive Kooperation zu ermöglichen. Insoweit besteht ebenso wie bei der ATD kein gesetzgeberischer Handlungsbedarf.

4.2.1 Auswirkungen auf projektbezogene gemeinsame Dateien

Die Übermittlung personenbezogener Daten zwischen Nachrichtendiensten und Polizeibehörden kann auch im Rahmen projektbezogener gemeinsamer Dateien z.B. nach § 9a BKAG oder § 22a BVerfSchG erfolgen.

Anders als bei der ATD ist das Speichern personenbezogener Daten in einer solchen gemeinsamen Datei allerdings nur zulässig, wenn für jedes Datum die Übermittlung nach den jeweils einschlägigen Übermittlungsvorschriften an alle an der Datei beteiligten Behörden zulässig ist (§ 9a Abs. 2 BKAG, § 22a Abs. 2 BVerfSchG).

Insofern wirken sich Änderungen an den Übermittlungsvorschriften bzw. deren verfassungskonformer Auslegung unmittelbar auf die Befugnis aus, personenbezogene Daten in gemeinsamen Dateien zu speichern. Ein eigenständiger Änderungsbedarf für § 9a BKAG oder § 22a BVerfSchG ergibt sich darüber hinaus allerdings nicht.

5. Zusammenfassung der Ergebnisse

In Folge der Entscheidung des BVerfG vom 24.04.2013 ergibt sich im Hinblick auf die Zusammenarbeit und den Austausch von personenbezogenen Daten zwischen der Polizei und dem Verfassungsschutz unmittelbarer gesetzgeberischer Änderungsbedarf im ATD-Gesetz sowie in weiten Teilen entsprechender gesetzgeberischer Änderungebedarf im RED-Gesetz.

Weiterhin sind die Vorschriften für die Übermittlung von Verfassungsschutz- an Polizeibehörden verfassungskonform auszulegen. Diesbezüglich empfiehlt das Bundesministerium des Innern ebenfalls eine klarstellende Regelung, um die Einheitlichkeit und Handhabbarkeit der Übermittlungsvorschriften zu gewährleisten.

Darüber hinaus gehender Regelungsbedarf, insbesondere im Hinblick auf die Zusammenarbeit in den gemeinsamen Zentren sowie die Vorschriften zu projektbezogenen gemeinsamen Dateien, folgt aus dem in der Entscheidung entwickelten informationellen Trennungsprinzip nicht.

Bis zum Inkrafttreten der Neuregelung, längstens bis zum 31.12.2014, kann die ATD nach Maßgabe der Übergangsregelung des BVerfG genutzt werden.

5.1 Änderungsbedarf im ATDG

- Für die Benennung weiterer Polizeivollzugsbehörden im Sinne des § 1 Abs. 2 ATDG ist künftig eine Verordnungsermächtigung vorzusehen.
- Der Kreis der in der Datei zu speichernden Kontaktpersonen ist entweder in geeigneter Weise einzuschränken oder der zu den Kontaktpersonen zu speichernde Datenkranz ist auf wenige, zu Identifizierung notwendigen Elementardaten zu beschränken.
- Das Merkmal des „Unterstützens“ einer den Terrorismus unterstützenden Gruppierung in § 2 Satz 1 Nr. 1 b) ATDG ist dahingehend einzuschränken, dass es sich um eine willentliche Förderung der den Terrorismus unterstützenden Aktivitäten der Gruppe handeln muss.

- Das Merkmal des „Befürwortens“ von Gewalt ist in § 2 Satz 1 Nr. 2 ATDG ist dahingehend einzuschränken, dass es Anhaltspunkte geben muss, dass die Person tatsächlich Gewalt anwenden, unterstützen, vorbereiten oder hervorrufen will.
- § 5 Abs. 1 Satz 2 Nr. 1 a) ATDG ist dahingehend zu ergänzen, dass bei einer Suche nur in den erweiterten Grunddaten („Inverssuche“) im Trefferfall nur Zugriff auf die Informationen gemäß § 3 Abs. 1 Nr. 3 ATDG gewährt werden darf.
- Hinsichtlich der Datenkategorien nach § 3 Abs. 1 Nr. 1 b) Buchst. gg), hh), ii), kk) und nn) ist eine Konkretisierung durch eine veröffentlichungspflichtige Verwaltungsvorschrift vorzusehen.
- Es ist eine verpflichtende turnusmäßige Datenschutzkontrolle alle zwei Jahre vorzusehen.
- Es ist eine Regelung vorzusehen, dass personenbezogene Daten innerhalb eines Datensatzes, die durch verdeckte Eingriffe on Art. 10 oder 13 GG oder das Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewonnen wurden, nur verdeckt oder beschränkt gespeichert werden.

5.2 Änderungsbedarf im RED-G

- Für die Benennung weiterer Polizeivollzugsbehörden im Sinne des § 1 Abs. 2 RED-G ist künftig eine Verordnungsermächtigung vorzusehen.
- Die Möglichkeit einer Inverssuche ist in § 5 Abs. 1 Satz 2 Nr. 1 a) RED-G wie im ATDG einzuschränken. Kein Änderungsbedarf besteht bezüglich der Möglichkeit zur erweiterten Nutzung nach § 7 RED-G, da die diesbezüglichen hohen rechtliche Eingriffsschwellen den verfassungsrechtlichen Anforderungen genügen.
- Hinsichtlich der Datenkategorien nach § 3 Abs. 1 Nr. 1 b) Buchst. gg), ii) und ll) ist eine Konkretisierung durch eine veröffentlichungspflichtige Verwaltungsvorschrift vorzusehen.
- Es ist eine verpflichtende turnusmäßige Datenschutzkontrolle alle zwei Jahre vorzusehen.
- Es ist eine Regelung vorzusehen, dass personenbezogene Daten innerhalb eines Datensatzes, die durch verdeckte Eingriffe on Art. 10 oder 13 GG oder das

Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewonnen wurden, nur verdeckt oder beschränkt gespeichert werden.

- Kein analoger Änderungsbedarf besteht hinsichtlich der Regelungen zu Kontaktpersonen, Befürworten von Gewalt und Unterstützer von Gruppierungen, da diesbezügliche Regelungen von vornherein enger gefasst wurden als im ATDG oder gar nicht in das RED-G übernommen wurden.

5.3 Verfassungskonforme Auslegung von § 19 Abs. 1 BVerfSchG

§ 19 Abs. 1 BVerfSchG ist dahingehend verfassungskonform auszulegen, dass eine Übermittlung von mit nachrichtendienstlichen Mitteln gewonnener personenbezogener Daten an Polizeibehörden mit dem Ziel eines operativen polizeilichen Tätigwerdens nur zulässig ist, wenn dies zur Verfolgung von Straftaten oder zur Abwehr von Gefahren notwendig ist oder eine sonstige Befugnis ein polizeiliches Tätigwerden im Vorfeld der Gefahr gestattet und die für die empfangende Behörde geltenden Erhebungsschwellen nicht unterlaufen werden.

6. Weiteres Vorgehen

Auf Basis des vorliegenden Berichts wird das BMI einen Gesetzentwurf erarbeiten und die betroffenen Bundesressorts sowie die Länder beteiligen.

Die vom Gericht als verfassungswidrig erkannten Regelungen müssen im ATDG bis zum 31.12.2014 geändert werden, da sie ansonsten außer Kraft treten und die ATD als Konsequenz ab dem 01.01.2015 nicht mehr genutzt werden kann (vgl. Ausführungen S. 21).

Ebenfalls bis dahin ist das RED-G zu novellieren. Zwingender Änderungsbedarf in anderen Vorschriften ergibt sich aus der Entscheidung des BVerfG nicht, das BMI wird allerdings prüfen, ob weitere rechtliche Anpassungen sinnvollerweise mit der Gesetzesnovelle verbunden werden können.

7. Beschlussvorschlag

Der IMK wird vorgeschlagen, bei ihrer Herbstsitzung 2013 folgenden Beschluss zu fassen:

Die IMK nimmt den vom Bundesministerium des Innern unter Beteiligung des AK II und AK IV vorgelegten Bericht zu den Auswirkungen des Urteils des Bundesverfassungsgerichts vom 24.04.2013, 1 BvR - 1215/07 (ATDG) in Bezug auf den Austausch von personenbezogenen Daten zwischen der Polizei und dem Verfassungsschutz zur Kenntnis.