Stand: 22.08.2011

**Rahmenbeschluss Datenschutz: Umsetzungsbedarf und Verhältnis zu Ratsbeschluss Prüm und Rahmenbeschluss Schwedische Initiative**

**Beschlussvorschlag**

1. Der UARV nimmt den Bericht „Rahmenbeschluss Datenschutz: Umsetzungsbedarf und Verhältnis zu Ratsbeschluss Prüm und Rahmenbeschluss Schwedische Initiative“, Stand: **XX.XX**.2011, zur Kenntnis.

2. Zum Umsetzungsbedarf des Rahmenbeschlusses 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350, S. 60) – Rahmenbeschluss Datenschutz – stellt er fest:

   - Der Rahmenbeschluss Datenschutz ist nur auf Sachverhalte mit EU-Bezug, d.h. vor allem auf aus dem EU-Ausland übermittelte Daten, anwendbar. Soweit Daten ins EU-Ausland, an EU-Institutionen oder an Schengen-assoziierte Staaten übermittelt werden sollen, kommt er erst ab dem Zeitpunkt zum Tragen, zu dem die Daten tatsächlich übermittelt oder bereitgestellt werden.

   - Umsetzungsbedarf in den Polizeigesetzen der Länder ergibt sich insbesondere im Hinblick auf Beschränkungen der Verarbeitung von im Anwendungsbereich des Rahmenbeschlusses übermittelten Daten.

3. Die Datenschutzvorschriften des Ratsbeschlusses Prüm und des Rahmenbeschlusses Schwedische Initiative gehen dem Rahmenbeschluss Datenschutz im Wesentlichen vor. Soweit dort strengere Regelungen getroffen sind als im Rahmenbeschluss Datenschutz, muss eine gesonderte Umsetzung erfolgen.

4. Der UARV bittet den AK II, wie folgt zu beschließen:

   1. Der AK II nimmt den Bericht „Rahmenbeschluss Datenschutz: Umsetzungsbedarf und Verhältnis zu Ratsbeschluss Prüm und Rahmenbeschluss Schwedische Initiative“, Stand: **XX.XX**.2011, zur Kenntnis.

2. Zum Umsetzungsbedarf des Rahmenbeschlusses 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350, S. 60) – Rahmenbeschluss Datenschutz – stellt er fest:

   – Der Rahmenbeschluss Datenschutz ist nur auf Sachverhalte mit EU-Bezug, d.h. vor allem auf aus dem EU-Ausland übermittelte Daten, anwendbar. Soweit Daten ins EU-Ausland, an EU-Institutionen oder an Schengen-assoziierte Staaten übermittelt werden sollen, kommt er erst ab dem Zeitpunkt zum Tragen, zu dem die Daten tatsächlich übermittelt oder bereitgestellt werden.

   – Umsetzungsbedarf in den Polizeigesetzen der Länder ergibt sich insbesondere im Hinblick auf Beschränkungen der Verarbeitung von im Anwendungsbereich des Rahmenbeschlusses übermittelten Daten.

3. Die Datenschutzvorschriften des Ratsbeschlusses Prüm und des Rahmenbeschlusses Schwedische Initiative gehen dem Rahmenbeschluss Datenschutz im Wesentlichen vor. Soweit dort strengere Regelungen getroffen sind als im Rahmenbeschluss Datenschutz, muss eine gesonderte Umsetzung erfolgen.

4. Er bittet die IMK, wie folgt zu beschließen:

   1. Der IMK nimmt den Bericht „Rahmenbeschluss Datenschutz: Umsetzungsbedarf und Verhältnis zu Ratsbeschluss Prüm und Rahmenbeschluss Schwedische Initiative“, Stand: **XX.XX**.2011, zur Kenntnis.

   2. Zum Umsetzungsbedarf des Rahmenbeschlusses 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350, S. 60) – Rahmenbeschluss Datenschutz – stellt sie fest:

      – Der Rahmenbeschluss Datenschutz ist nur auf Sachverhalte mit EU-Bezug, d.h. vor allem auf aus dem EU-Ausland übermittelte Daten, anwendbar. Soweit Daten ins EU-Ausland, an EU-Institutionen oder an Schengen-assoziierte Staaten übermittelt werden sollen, kommt er erst ab dem Zeitpunkt zum Tragen, zu dem die Daten tatsächlich übermittelt oder bereitgestellt werden.

- Umsetzungsbedarf in den Polizeigesetzen der Länder ergibt sich insbesondere im Hinblick auf Beschränkungen der Verarbeitung von im Anwendungsbereich des Rahmenbeschlusses übermittelten Daten.

3. Die Datenschutzvorschriften des Ratsbeschlusses Prüm und des Rahmenbeschlusses Schwedische Initiative gehen dem Rahmenbeschluss Datenschutz im Wesentlichen vor. Soweit dort strengere Regelungen getroffen sind als im Rahmenbeschluss Datenschutz, muss eine gesonderte Umsetzung erfolgen.

# Rahmenbeschluss Datenschutz: Umsetzungsbedarf und Verhältnis zu Ratsbeschluss Prüm und Rahmenbeschluss Schwedische Initiative

Stand: 22.08.2011

# Inhaltsverzeichnis

## A. Anlass und Auftrag

Der Rahmenbeschluss 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350, S. 60) – Rahmenbeschluss Datenschutz (RB DS) – war nach seinem Artikel 29 bis zum 27.11.2010 in deutsches Recht umzusetzen. Seine Regelungen zu materiellen, verfahrensmäßigen und technischen Voraussetzungen der Datenverarbeitung betreffen auch das Polizeirecht der Länder.

Mit Umlaufbeschluss vom 12.11.2010 zum „Umsetzungsbedarf Ratsbeschluss Prüm und Schwedische Initiative“ hat der UARV unter Ziffer 6 eine Projektgruppe eingerichtet und sie beauftragt

> *„zu prüfen, in welchem Verhältnis die speziellen Datenschutzbestimmungen der von ihr bereits bewerteten Rechtsakte zu den allgemeinen Vorgaben des Rahmenbeschlusses 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, zu betrachten sind.“*

Der AK II hat dies mit Umlaufbeschluss vom 09.02.2011 zur Kenntnis genommen.

Die Projektgruppe hat als wesentlichen Bestandteil ihres Auftrags zunächst geprüft, welcher Umsetzungsbedarf sich in den Polizeigesetzen der Länder aus dem Rahmenbeschluss Datenschutz ergibt (C.) und anschließend das Verhältnis zu den Regelungen des Ratsbeschlusses Prüm und des Rahmenbeschlusses Schwedische Initiative bzw. dem aus diesen Rechtsakten resultierenden Umsetzungsbedarf geklärt (D.). Die wesentlichen Ergebnisse sind unter B. vorangestellt.

An der Arbeitsgruppe haben sich Niedersachsen (Vorsitz), Baden-Württemberg, Bayern, Hamburg, Schleswig-Holstein beteiligt. Ein Vertreter von BMI hat an den Sitzungen der Arbeitsgruppe teilgenommen.

## B. Wesentliche Ergebnisse

### I. Umsetzungsbedarf aus dem Rahmenbeschluss Datenschutz

Der Rahmenbeschluss Datenschutz (RB DS) enthält Regelungen zum Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit zwischen den Mitgliedstaaten der EU verarbeitet werden. Die Gesetzgebungskompetenz der Länder ist betroffen, soweit es um die Datenverarbeitung der Polizeien der Länder zur Gefahrenabwehr einschließlich der Verhütung oder Verhinderung von Straftaten geht.

Umsetzungsbedarf in Landesrecht besteht, soweit die Polizei- und Datenschutzgesetze der Länder nicht schon Regelungen enthalten, die den Anforderungen des RB DS gerecht werden. *Entsprechend dem begrenzten Anwendungsbereich des RB DS können die zu*

*treffenden Neuregelungen auf Sachverhalte mit EU-Bezug begrenzt werden*, d.h. auf Daten, die zur Verhinderung oder Verhütung von Straften

- aus dem EU-Ausland, von EU-Institutionen oder aus Schengen-assoziierten Staaten empfangen wurden oder
- ins EU-Ausland, an EU-Institutionen oder in Schengen-assoziierte Staaten zu übermitteln sind ab dem Zeitpunkt, zu dem sie tatsächlich übermittelt oder bereitgestellt werden.

Eine entsprechende Begrenzung führt zwar zu einer Verkomplizierung der Regelungsgefüge, hat aber den Vorteil, dass übermäßige Eingriffe in das bewährte Datenschutzregime des Polizeirechts der Länder vermieden werden. Zu überlegen ist allerdings, zumindest einzelne Vorschriften so umzusetzen, dass sie auf alle Sachverhalte mit Auslandsbezug anzuwenden sind und nicht nur auf die EU-Zusammenarbeit.

In folgenden Punkten besteht gesetzlicher Anpassungsbedarf oder könnten sich zumindest zur Klarstellung gesetzliche Regelungen empfehlen:

- *Kennzeichnungspflichten:* Um die Einhaltung der zur Umsetzung des RB DS zu schaffenden Regelungen zu gewährleisten, müssen aus dem EU-Ausland, von EU-Institutionen und aus Schengen-assoziierten Staaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit empfangene Daten gekennzeichnet werden.

- *Schutz besonderer Kategorien von Daten (Art. 6):* Besondere Kategorien von Daten sind bereits nach dem Verhältnismäßigkeitsprinzip besonders zu schützen. Eine klarstellende Regelung könnte die besondere Grundrechtsrelevanz der Verarbeitung solcher Daten betonen und eine Warnfunktion ausüben.

- *Unterrichtung des Empfängers bei unrechtmäßiger Datenübermittlung (Art. 8 Abs. 2:)* Dass der Empfänger zu unterrichten ist, wenn die Datenübermittlung unrechtmäßig war, lässt sich aus der landesrechtlich geregelten Verantwortung der übermittelnden Stelle für die Rechtmäßigkeit der Datenübermittlung ableiten. Eine ausdrückliche Regelung könnte jedoch zur Rechtssicherheit beitragen.

- *Bindung an Prüf- und Löschpflichten der übermittelnden Stelle (Art. 9):* Art. 9 verlangt die Beachtung von Prüf- und Löschpflichten der übermittelnden Stelle, wenn diese dem Empfänger mitgeteilt werden. Für eingehende Daten müssen entsprechende Regelungen geschaffen werden. Für ausgehende Daten erscheint eine gesetzliche Regelung nicht erforderlich, da durch den RB DS ein angemessenes Datenschutzniveau auch im empfangenden Mitgliedstaat gewährleistet ist.

  Eine Regelung kann gegebenenfalls gemeinsam mit den ähnlich gelagerten Bindungen aus Art. 12 und Art. 16 Abs. 2 erfolgen.

- *Dokumentierung und Protokollierung (Art. 10):* Die Polizeigesetze der Länder regeln Protokollierungspflichten v.a. bei der automatisierten Datenverarbeitung. Für die nicht automatisierte Übermittlung von Daten aus Dateien könnte eine klarstellende Rege-

lung erfolgen, allerdings ergeben sich entsprechende Pflichten bereits aus den allgemeinen Grundsätzen über die Aktenförmigkeit des Verwaltungshandelns.

- *Beschränkungen der Zweckänderung (Art. 11):* Nach Art. 11 dürfen Daten, die im Geltungsbereich des RB DS übermittelt wurden, ohne Zustimmung der übermittelnden Stelle nur

  - zur Verhütung von Straftaten, zur Strafverfolgung und Strafvollstreckung,
  - zur Verwendung in anderen justiziellen oder verwaltungsbehördlichen Verfahren, die mit dem der Übermittlung zugrunde liegenden Verfahren in Zusammenhang stehen, oder
  - zur Abwehr gegenwärtiger erheblicher Gefahren

  verwendet werden. Die Polizeigesetze der Länder sehen zumeist weitergehende Zweckänderungsmöglichkeiten vor. Für den Anwendungsbereich des RB DS ist die Zweckänderung zu beschränken und im Übrigen von der Zustimmung der übermittelnden Stelle abhängig zu machen.
  Die nach den Polizeigesetzen zulässige Verwendung von Daten zur Aus- und Fortbildung und zu statistischen Zwecken steht mit Art. 11 Abs. 2 in Einklang und muss nicht von einer Zustimmung der übermittelnden Stelle abhängig gemacht werden.

- *Wahrung von für die übermittelnde Stelle geltenden Verarbeitungsbeschränkungen (Art. 12):* Nach Art. 12 sind Vorgaben der übermittelnden Stelle zur Datenverarbeitung zu beachten. Für eingehende Daten muss eine entsprechende Bindung geregelt werden. Angesichts der besonderen Bedeutung besonderer Verarbeitungsbeschränkungen für die Grundrechtswahrung empfiehlt es sich, auch zu regeln, dass entsprechende Beschränkungen bei Datenübermittlungen ins Ausland mitzuteilen sind.

- *Beschränkung der Weiterleitung an Drittstaaten und internationale Einrichtungen (Art 13):* Eine Weiterleitung an Drittstaaten und internationale Einrichtungen darf nach Art. 13 nur mit Zustimmung der übermittelnden Stelle und nur zur Abwehr straftatenbezogener Gefahren erfolgen. Ohne Zustimmung darf eine Weiterleitung zur Abwehr unmittelbar bevorstehender erheblicher Gefahren erfolgen. Entsprechende Beschränkungen fehlen in den Polizeigesetzen der Länder bislang.
  Die Weiterleitung darf nach Art. 13 außerdem nur erfolgen, wenn in dem Drittstaat ein angemessenes Datenschutzniveau herrscht oder besondere Gründe die Übermittlung rechtfertigen. Die Polizeigesetze enthalten zum Teil bereits vergleichbare Regelungen; andernfalls sind entsprechende Vorschriften zu schaffen.
  Zu regeln ist außerdem die in Art. 13 vorgesehene Unterrichtung des Herkunfts-Mitgliedstaats über die Weiterleitung.
  Keiner gesetzlichen Regelung bedürfen hingegen die Erteilung der Zustimmung zur Weiterleitung von durch die Länderpolizeien ins Ausland übermittelten Daten und die Kriterien zur Bewertung des Datenschutzniveaus in dem Drittstaat.

- *Beschränkung der Weiterleitung an nicht-öffentlichen Stellen (Art. 14):* Die Weiterleitung an nicht-öffentliche Stellen ist von der Zustimmung der übermittelnden Stelle abhängig zu machen. Die Übermittlungszwecke sind zu beschränken auf die Abwehr straftatenbezogener Gefahren, die Abwehr sonstiger gegenwärtiger erheblicher Ge-

fahren oder die Abwehr schwerwiegender Beeinträchtigungen der Rechte Einzelner. Eine Weiterleitung an nicht öffentliche Stellen in Drittstaaten ist auszuschließen. Auch hier erscheint eine gesetzliche Regelung über die Erteilung der Zustimmung durch die Polizeien der Länder entbehrlich.

- *Unterrichtung der übermittelnden Stelle über die Datenverarbeitung (Art. 15):* Die Polizeigesetze der Länder sehen Auskunftsansprüche der übermittelnden Stelle bislang nicht vor. Da eine Information über die Datenverarbeitung mit einer Übermittlung personenbezogener Daten verbunden sein wird, ist eine spezielle Rechtsgrundlage erforderlich.

- *Absehen von der Information der betroffenen Person auf Ersuchen der übermittelnden Stelle (Art. 16):* Nach den Polizeigesetzen der Länder bestehen Unterrichtungspflichten nur für die verdeckte Datenerhebung. Ersuchen nach Art. 16, von einer Unterrichtung über den Empfang von Daten aus dem Ausland abzusehen, dürften daher für die Praxis keine große Bedeutung erlangen, sind aber auch nicht ausgeschlossen. Eine entsprechende Regelung sollte daher getroffen werden. Auch die Übermittlung entsprechender Zurückstellungsersuchen ins Ausland sollte geregelt werden, um der besonderen Bedeutung von Geheimhaltungserfordernissen Rechnung zu tragen.

- *Schriftlichkeit der Auskunftsverweigerung (Art. 17*): Soweit in den Ländern weder gesetzliche noch untergesetzliche Regelungen zur Schriftform bei der Verweigerung von Auskünften über die Datenverarbeitung bestehen, sollten entsprechende Regelungen getroffen werden.

- *Formerfordernisse bei der Ablehnung von Anträgen auf Berichtigung, Löschung oder Sperrung (Art. 18):* Nach Art. 18 muss die Ablehnung von Anträgen schriftlich erfolgen und mit einer Rechtsbehelfsbelehrung versehen werden. Dies entspricht zwar bereits der Praxis, an einer ausdrücklichen Regelung in den Polizeigesetzen der Länder fehlt es jedoch. Ob die Regelung in § 37 VwVfG zur Schriftform von Verwaltungsakten den Anforderungen genügt, ist fraglich, zumal auch streitig ist, ob die Ablehnung von Berichtigungs-, Löschungs- und Sperranträgen durch Verwaltungsakt erfolgt.

- *Schadensersatz bei unrichtiger Datenübermittlung (Art. 19):* Die Datenschutzgesetze der Länder sehen für Schadensersatzansprüche wegen unzulässiger nicht automatisierter Datenverarbeitung eine Exkulpationsmöglichkeit vor, die nach Art. 19 RB DS ausgeschlossen ist. Ob sich hieraus Umsetzungsbedarf ergibt, ist fraglich, da Art. 19 einen Nationalrechtsvorbehalt enthält, der sich auch auf die Exkulpationsmöglichkeit beziehen könnte.

- *Vorabkonsultation mit dem Landesbeauftragten für den Datenschutz (Art. 23):* Die Regelungen im Landesrecht zur Beteiligung des Landesbeauftragten für den Datenschutz sind unterschiedlich. Nach Art. 23 muss eine Vorab-Beteiligung erfolgen, wenn Dateien neu errichtet werden, besondere Kategorien von Daten verarbeitet werden oder sonst besondere Risiken bestehen.

## II. Verhältnis zum Ratsbeschluss Prüm und dem Rahmenbeschluss Schwedische Initiative

Nach Art. 28 RB DS gehen früher erlassene „spezifische Bestimmungen über die Verwendung von Daten durch den Empfängermitgliedstaat“ den Bestimmungen des RB DS vor. Unter diese Vorrangregelung fallen die einzelnen Vorschriften, die der Rahmenbeschluss Schwedische Initiative (RB SWI) über die weitere Verarbeitung von in seinem Geltungsbereich ausgetauschten Daten enthält. Der Ratsbeschluss Prüm (RatsB Prüm) mit seinen umfassenden Datenschutzbestimmungen für die auf seiner Grundlage ausgetauschten Daten kann insgesamt als dem RB DS vorgehende Spezialregelung betrachtet werden.

Sondervorschriften zur Umsetzung der Datenschutzbestimmungen des RatsB Prüm – für den eine Umsetzung im Landesrecht allerdings ohnehin nicht zwingend ist – und des RB SWI müssen jedoch nur noch insoweit geschaffen werden, als sie strengere Anforderungen stellen als der RB DS. Im Einzelnen ergibt sich für diejenigen Vorschriften, für die ein Umsetzungsbedarf bejaht wurde, folgendes Bild:

Im Anwendungsbereich des *RatsB Prüm* sind Sonderregelungen zu treffen zu

- Art. 14, strenge Zweckbindung und spezielle Löschungsregeln für Daten, die bei Großveranstaltungen übermittelt werden,
- Art. 26, strenge Zweckbindung für zum Datenabgleich übermittelte DNA-, Fingerabdruck- und Fahrzeugdaten,
- Art. 27, Zustimmung des Herkunftsmitgliedstaats bei jeder Weiterleitung (auch innerstaatlich oder an andere Mitgliedstaaten) und
- Art. 30, Dokumentation und Protokollierung des nicht automatisierten Empfangs von Daten.

Art. 28 mit seinen allgemeinen Grundsätzen zur Richtigkeit, Aktualität und Speicherdauer bedarf hingegen neben den zur Umsetzung des RB DS ergehenden Regelungen keiner gesonderten Umsetzung.

Der *RB SWI* erfordert Sonderregelungen für den Datenschutz zu Art. 8 Abs. 3, der strengere Regelungen zur Zweckbindung enthält als Art. 11 RB DS. Insbesondere darf eine Zweckänderung im Anwendungsbereich des RB SWI auch zur Verhütung von Straftaten nur mit Zustimmung der übermittelnden Stelle erfolgen. Außerdem ist die Auskunftserteilung an die übermittelnde Stelle in Art. 8 Abs. 4 Satz 5 SWI nur zu Zwecken der Datenschutzkontrolle erlaubt und unterliegt damit engeren Bindungen als die Auskunftserteilung nach Art. 15 RB DS.

# C. Landesrechtlicher Umsetzungsbedarf aus dem Rahmenbeschluss Datenschutz

Zur Rechtsnatur von Rahmenbeschlüssen als umsetzungsbedürftige Rechtsakte und zum Fortbestehen der Umsetzungspflicht auch nach Inkrafttreten des Vertrages von Lissabon wird auf die Ausführungen in dem Bericht „Umsetzungsbedarf Ratsbeschluss Prüm und

Schwedische Initiative, Stand: 05.01.2011“, Anlage 2, Ziffn. II und III verwiesen. Nach einer Übergangsfrist von fünf Jahren ab Inkrafttreten des Vertrags von Lissabon am 01.12.2009 unterliegen die nach Titel VI des aufgrund des Vertrags von Nizza vom 26.02.2001 geänderten Vertrags über die Europäische Union (konsolidierte Fassung: Amtsblatt der Europäischen Gemeinschaften C 325/1 vom 24.12.2002 – EUV a.F. – ) erlassenen Rechtsakte den allgemeinen Vorschriften und damit auch dem Vertragsverletzungsverfahren. Wird ein Rechtsakt vor Ablauf der Fünfjahresfrist geändert, unterliegt er bereits ab diesem Zeitpunkt den allgemeinen Vorschriften (Art. 10 Abs. 1 bis 3 des Protokolls über die Übergangsbestimmungen, ABl. C 306, S. 159).

Die Umsetzung von EU-Rechtsakten in deutsches Recht erfolgt im Rahmen der für die jeweilige Sachmaterie bestehenden Gesetzgebungskompetenzen. Soweit daher der Rahmenbeschluss Datenschutz Regelungen trifft, die der Gesetzgebungskompetenz der Länder unterfallen, ist das Landesrecht anzupassen.

## I. Betroffenheit der Polizeigesetze der Länder

### 1. Anwendungsbereich und Regelungsgehalt des RB Datenschutz

Der Rahmenbeschluss trifft Regelungen zum Datenschutz für die Verarbeitung von Daten durch Polizei und Justiz im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen gem. Titel VI des Vertrages über die Europäische Union in der bis zum 01.12.2009 geltenden Fassung (Art. 1 Abs. 1 RB DS).

#### a) Verarbeitung von Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit

Gemäß seinem Art. 1 Abs. 2 ist der Anwendungsbereich des RB DS nur eröffnet, wenn

> „…personenbezogene Daten zum Zweck der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen
>
> a) zwischen Mitgliedstaaten übermittelt oder bereitgestellt werden oder wurden;
>
> b) von Mitgliedstaaten an Behörden oder an Informationssysteme, die aufgrund von Titel VI. des Vertrags über die Europäische Union errichtet worden sind, übermittelt oder ihnen bereitgestellt werden oder wurden;
>
> c) von Behörden oder Informationssystemen, die aufgrund des Vertrags über die Europäische Union oder des Vertrags zur Gründung der Europäischen Gemeinschaft errichtet worden sind, an die zuständigen Behörden der Mitgliedstaaten übermittelt oder ihnen bereitgestellt werden oder wurden.“

#### aa) Keine Anwendung auf rein innerstaatliche Sachverhalte

Der Rahmenbeschluss ist auf rein innerstaatliche Sachverhalte nicht anwendbar. Der solchermaßen beschränkte Anwendungsbereich des Rahmenbeschlusses bewegt sich innerhalb der bisherigen Rechtsetzungskompetenz der Europäischen Union gemäß Titel VI EUV a.F. Gemäß Art. 29 EUV a.F. verfolgt die Union das Ziel, den Bürgern in einem Raum der Freiheit, der Sicherheit und des Rechts ein hohes Maß an Sicherheit zu bieten. Nach Art. 29 erster Anstrich dient diesem Ziel eine engere Zusammenarbeit der Polizei-, Zoll- und anderer zuständiger Behörden in den Mitgliedstaaten, sowohl unmittelbar als auch unter Einschaltung des Europäischen Polizeiamts (Europol), nach den Art. 30 und 32. Rahmenbeschlüsse, die der Rat gemäß Art. 34 Abs. 2 lit. b EUV a.F. zur Angleichung

der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten annehmen konnte, waren in ihrem Anwendungsbereich auf das Verständnis von Titel VI als Zusammenarbeit der zuständigen Behörden in den Mitgliedstaaten beschränkt. Dies dürfte im Übrigen auch für die heutige Rechtslage gemäß Art. 16 Abs. 2 i.V. m. Art. 87 AEUV gelten, da sich Unionsrecht zum Datenschutz nach Art. 16 Abs. 2 Satz 1 AEUV nur auf Tätigkeiten beziehen darf, die in den Anwendungsbereich des Unionsrechts fallen. Hierzu gehören polizeiliche Sachverhalte ohne grenzüberschreitende Dimension gem. Art. 87 gerade nicht.

Dementsprechend sind die Vorschriften des Rahmenbeschlusses so auszulegen, dass sie nur unter der Voraussetzung eines Datenaustauschs mit dem EU-Ausland oder mit Datenbanken der EU anwendbar sind, nicht jedoch auf innerstaatliche Sachverhalte ohne direkten Bezug zum EU-Ausland. Das bedeutet insbesondere, dass die Vorgaben des Rahmenbeschlusses erst von dem Zeitpunkt an gelten, zu dem Daten tatsächlich bereitgestellt oder übermittelt werden, und nicht schon im Hinblick auf einen möglichen späteren Datenaustausch von Anfang an anzuwenden sind. Soweit dies im Einzelnen zu Auslegungsschwierigkeiten führt, wird darauf bei den einzelnen Vorschriften des Rahmenbeschlusses einzugehen sein.

**bb) Datenübermittlung zwischen Mitgliedstaaten**

In Art. 1 Abs. 2 lit. a RB DS wird wie auch in anderen Vorschriften des Rahmenbeschlusses auf die Mitgliedstaaten Bezug genommen. Nach den Erwägungsgründen 45 bis 47 gilt der Rahmenbeschluss jedoch auch für die Schengen-assoziierten Staaten. Insoweit wird auf die Ausführungen in dem Bericht „Umsetzungsbedarf Ratsbeschluss Prüm und Schwedische Initiative, Stand: 05.01.2011“, Anlage 2 (VI.1.a.(b)) verwiesen.

**cc) Behörden oder Informationssysteme, die aufgrund des EUV oder des EGV errichtet worden sind**

Nach Art. 1 Abs. 2 lit. b und c RB DS ist auch der Datenaustausch mit Behörden oder Informationssystemen, die aufgrund des EUV oder des EGV errichtet worden sind – z.B. Europol oder das Schengener Informationssystem – vom Anwendungsbereich des Rahmenbeschlusses erfasst. In Art. 2 Buchst. h werden als „zuständige Behörden“ im Sinne des Rahmenbeschlusses allerdings neben den zuständigen Behörden der Mitgliedstaaten nur „durch Rechtsakte, die der Rat gemäß Titel VI des Vertrages über die Europäische Union erlassen hat, errichtete Agenturen oder Einrichtungen“ genannt. Diese Definition ist für die Anwendung der folgenden Artikel, in denen nur auf „zuständige Behörden“ abgestellt wird, maßgeblich. Die abweichende Formulierung des Art. 1 Abs. 2 lit. b und c RB DS verdeutlicht, dass die Vorschriften des Rahmenbeschlusses auch dann gelten, wenn Abruf oder Bereitstellung von Daten auch über ein nach dem EUV oder dem EGV errichtetes Informationssystem erfolgen können.

**dd) Straftaten**

Fraglich ist, ob der Begriff der Straftat in Art. 1 Abs. 2 RB DS eng auszulegen ist und sich nur auf Straftaten i.S.d. deutschen Strafrechts bezieht oder auch Übertretungen umfasst, die das deutsche Recht als Ordnungswidrigkeiten einordnet. Für Art. 29 EUV a.F., der die Ziele der Zusammenarbeit in Strafsachen nach Titel VI des EUV a.F. beschreibt, wird teilweise vertreten, dass er neben Verbrechen und Vergehen im Sinne des deutschen Strafrechts auch Ordnungswidrigkeiten erfasst (Böse in: Schwarze, EU-Kommentar,

2. Aufl. 2009, Art. 29 EUV, Rn. 4; a.A.: Groeben/ Schwarze/ Wasmeier/Jour-Schröder, EUV/EGV, Art. 29, Rn. 21 ff.). Dies entspricht auch dem Verständnis in verschiedenen anderen Mitgliedstaaten. Diese weite Auslegung des Straftatenbegriffs könnte auch auf den RB DS übertragen werden.
Allerdings enthalten andere Rechtsakte der EU und völkerrechtliche Verträge, deren Anwendungsbereich sich auch auf Ordnungswidrigkeiten erstrecken soll, hierzu ausdrückliche Regelungen (z.B. Art. 5 des Rahmenbeschlusses zur gegenseitigen Anerkennung von Geldstrafen und Geldbußen, Art. 3 des EU-Rechtshilfeübereinkommens, Art. 49 des Schengener Durchführungsübereinkommens).
Dass der RB DS keine entsprechende Klausel enthält, spricht dafür, den in Art. 1 Abs. 2 RB DS verwendeten Straftatenbegriff eng auszulegen.

**b) Ganz oder teilweise automatisierte Verarbeitung von Daten**

Eine weitere Beschränkung des Anwendungsbereichs ergibt sich aus Art. 1 Abs. 3 des Rahmenbeschlusses. Danach gilt dieser Rahmenbeschluss für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Diese Vorschrift ist wortgleich mit Art. 3 Abs. 1 der Datenschutzrichtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995. Insoweit ist in dem Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder, soweit diese für öffentliche Stellen gelten, weiter, denn diese Gesetze regeln unterschiedlich Anforderungen an die Verarbeitung in Akten und Datenträgern[1], jedoch unabhängig davon, ob die Daten unter Einsatz von Datenverarbeitungsanlagen oder in nichtautomatisierten Dateien verarbeitet werden (vgl. § 1 Abs. 2 Nr. 1 BDSG).

## 2. Gesetzgebungskompetenz der Länder

Die Länder haben die Gesetzgebungskompetenz, soweit es um die Datenverarbeitung zur Gefahrenabwehr einschließlich der Verhütung oder Verhinderung von Straftaten durch die Polizeien der Länder geht. Die ausschließliche Gesetzgebungskompetenz des Bundes für die internationale Verbrechensbekämpfung (Art. 73 Abs. 1 Nr. 10 GG) umfasst zwar nicht nur die Strafverfolgung, sondern auch die Verhütung von Straftaten (str.), ermächtigt den Bund jedoch nur, die Zusammenarbeit mit dem Ausland in verfahrensmäßiger Hinsicht zu regeln. Materielle Regelungen über die Datenübermittlung ins Ausland und über die Verarbeitung von aus dem Ausland erhaltenen Daten sind von dem Kompetenztitel nicht umfasst. Dementsprechend enthalten die Polizeigesetze der Länder eigene Vorschriften über den Datenaustausch mit dem Ausland (vgl. im Einzelnen die Ausführungen in dem Bericht Umsetzungsbedarf Ratsbeschluss Prüm und Schwedische Initiative, Anlage 1, Ziff. V.1.).
Mittelbar gilt das Polizeirecht auch für die zu präventiven Zwecken erfolgende Verarbeitung von Daten, die zu Zwecken der Strafverfolgung erhoben und gespeichert wurden, da der Bund für diesen Bereich von seiner konkurrierenden Gesetzgebungskompetenz für das gerichtliche Verfahren aus Art. 74 Abs. 1 Nr. 1 GG keinen abschließenden Gebrauch gemacht hat (§ 481 StPO: Verwendung von repressiven Daten zu präventiven Zwecken nach Polizeirecht; §§ 483 ff. StPO: Verwendung von in Mischdateien gespeicherten Daten nach Polizeirecht). Abschließend bundesgesetzlich geregelt ist allerdings die Datenübermittlung ins Ausland zu Zwecken der Strafverfolgung, auch soweit es sich um zu präventi-

[1] Gola/Schomerus, BDSG, § 3 Rn. 16.

ven Zwecken erhobene oder gespeicherte Daten oder um Daten in Mischdateien handelt (IRG und völkerrechtliche Verträge).

## II. Umsetzungsbedarf im Hinblick auf die Einzelregelungen des RB DS

Die Polizei- und Datenschutzgesetze der Länder enthalten bereits jetzt Regelungen über die Verarbeitung von personenbezogenen Daten, die den Vorgaben des RB Datenschutz in weiten Bereichen entsprechen. Gleichwohl ergeben sich auch einige Abweichungen. Soweit das Landesrecht strengere Regelungen vorsieht als der Rahmenbeschluss, hat die Arbeitsgruppe eine Absenkung des Schutzniveaus nicht geprüft, da der Erlass strengerer Regelungen den Mitgliedstaaten gem. Art. 1 Abs. 5 RB DS ausdrücklich unbenommen bleibt. Soweit die landesrechtlichen Schutzvorkehrungen hinter denen des Rahmenbeschlusses zurückbleiben, müssen sie jedoch an den Rahmenbeschluss angepasst werden.
Der Anwendungsbereich des RB DS ist auf die Übermittlung und Bereitstellung von Daten für das EU-Ausland einschließlich der Schengen-assoziierten Staaten oder für EU-Institutionen und die Verarbeitung der von dort erhaltenen Daten beschränkt (s.o. I.1.a). Entsprechend beschränkt ist auch die Umsetzungspflicht. Die Mitgliedstaaten sind allerdings nicht gehindert, auch andere, vom Rahmenbeschluss nicht erfasste Sachverhalte den entsprechenden Regelungen zu unterwerfen. Hier ist vor allem zu überlegen, ob die nach dem Rahmenbeschluss zu treffenden Regelungen auf andere Sachverhalte mit nicht den Bereich der EU betreffenden Auslandsbezug erstreckt werden sollten. Eine vollständige Anpassung der polizeirechtlichen Datenschutzvorschriften, auch soweit sie keinen Auslandsbezug aufweisen, erscheint jedenfalls nicht erforderlich. Eine beschränkte Umsetzung erfordert zwar eine Reihe von Sonderregelungen für die Verarbeitung von aus dem Ausland erhaltenen Daten und wird deshalb zu einer Verkomplizierung der Regelungsgefüge führen. Eine auf Sachverhalte mit Auslandsbezug beschränkte Umsetzung hat jedoch den Vorteil, dass für den größeren Teil der Datenverarbeitungsvorgänge, der keinen Auslandsbezug aufweist, die bewährten Regelungen unverändert fort gelten können.

Soweit zur Umsetzung des Rahmenbeschlusses Vorschriften geschaffen werden, die nur im Anwendungsbereich des Rahmenbeschlusses – d.h. nur für den Datenverkehr mit dem EU-Ausland einschließlich der Schengen-assoziierten Staaten – gelten sollen, müssen Kennzeichnungspflichten geschaffen werden, die eine Einhaltung der entsprechenden Vorschriften ermöglichen.

### 1. Artikel 3 – Grundsatz der Rechtmäßigkeit, Verhältnismäßigkeit und der Zweckbindung

Mit den Grundsätzen der Rechtmäßigkeit, Verhältnismäßigkeit und der Zweckbindung einschließlich allgemeiner Vorgaben zur Zulässigkeit von Zweckänderungen enthält Art. 3 grundlegende Anforderungen an die Verarbeitung von personenbezogenen Daten. Die Polizeigesetze der Länder gehen von den gleichen Grundsätzen aus (z.B. §§ 38 und 39 Nds. SOG). Zur Rechtmäßigkeit der Datenverarbeitung enthalten die Polizeigesetze zwar keine ausdrücklichen Vorschriften, dieses Erfordernis ergibt sich jedoch bereits aus dem

rechtsstaatlichen Grundsätzen des Vorrangs des Gesetzes. Ein Umsetzungsbedarf ergibt sich aus Art. 3 daher nicht. Auf die Frage, inwieweit Art. 3 in Anbetracht des begrenzten Anwendungsbereichs des RB DS und der spezielleren Regelungen in Art. 11 überhaupt eigenständige Bedeutung zukommt, kommt es daher nicht an.

## 2. Artikel 4 – Berichtigung, Löschung und Sperrung

Auch die in Art. 4 enthaltenen Vorschriften über die Berichtigung, Löschung und Sperrung von Daten finden in den Polizei- und Datenschutzgesetzen der Länder ihre Entsprechung. Nach Art. 4 Abs. 1 sind Daten zu berichtigen und zu aktualisieren; dem entspricht die Berichtigungspflicht z.B. aus § 17 NDSG. Wie Art. 4 Abs. 2 und 3 RB DS sehen die Polizeigesetze vor, dass Daten zu löschen oder zu sperren sind, wenn sie zu den Zwecken, zu denen sie erhoben oder verarbeitet wurden, nicht mehr benötigt werden (z.B. § 39 a Nds. SOG). Nach Art. 4 Abs. 2 Satz 2 dürfen zu löschende Daten in einem gesonderten Datenbestand archiviert werden; nach Erwägungsgrund 13 genügt zur Trennung der Datenbestände allerdings auch eine entsprechende Verwendungsbeschränkung innerhalb einer Datenbank. Die Archivierung von unter fachlichen Gesichtspunkten nicht mehr benötigten Daten ist in den Archivgesetzen der Länder geregelt (z.B. § 17 Abs. 1 Satz 2 NDSG i.V.m. NArchG). Art. 4 Abs. 4 verweist für in gerichtlichen Akten und Dokumenten enthaltene Daten auf die nationalen Prozessordnungen.
Umsetzungsbedarf ergibt sich aus Art. 4 nicht.

## 3. Artikel 5 – Festlegung von Löschungs- und Prüffristen

Nach Art. 5 sind Prüf- und Löschfristen vorzusehen und verfahrensrechtlich abzusichern. Prüfristen regelt z.B. in § 47 Nds. SOG; allerdings nur für personenbezogene Daten, die in einer Datei gespeichert sind. Daneben sind auch die Aufbewahrungsfristen der Aktenordnungen Löschfristen i.S.v. Art. 5. Eine spezielle verfahrensrechtliche Absicherung von Löschfristen ist auf gesetzlicher Ebene nicht erfolgt; hier gelten lediglich die allgemeinen Regelungen wie die datenschutzrechtlichen Vorschriften über technische und organisatorische Maßnahmen, die Pflicht zur Bestellung von behördlichen Datenschutzbeauftragen und die Kontroll- und Beanstandungsrechte der Landesbeauftragten für den Datenschutz. Den Anforderungen des Art. 5 genügen jedoch die bestehenden Regelungen in Errichtungsanordnungen sowie die technischen Vorkehrungen für automatisierte Wiedervorlagen. Ein Umsetzungsbedarf ergibt sich nicht.

## 4. Artikel 6 – Verarbeitung besonderer Kategorien personenbezogener Daten

### a) Regelungsgehalt

Art. 6 enthält eine besondere Beschränkung für die Verarbeitung von Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben. Daten dieser Kategorien dürfen nur verarbeitet werden, wenn dies „unbedingt notwendig“ ist und das innerstaatliche Recht einen angemessenen Schutz gewährleistet.

**b) Landespolizeigesetzliche Regelungen**

Vergleichbare Regelungen sind in fast allen Polizei- und Ordnungsgesetzen der Länder nicht enthalten. Vielmehr wird grundsätzlich in den Landesdatenschutzgesetzen bei deren Regelungen zur Verarbeitung besonderer personenbezogener Daten eine Einschränkung des Anwendungsbereichs in der Weise vorgenommen, dass die formulierten Beschränkungen nicht für die Bereiche Gefahrenabwehr und Verfolgung von Straftaten gelten (z.B. § 33 LDSG BW, Art. 15 Abs. 7 und 8 DSG BY i.V.m Art 49 PAG BY, § 5 Abs. 1 S. 3 HmbDSG, § 11 Abs. 5 LDSG SH; ähnlich § 28 Abs. 6 - 9 BDSG). Nur in Mecklenburg-Vorpommern wurde im Rahmen der Änderung des Sicherheits- und Ordnungsgesetzes im März 2011 eine Regelung für die polizeiliche Verarbeitung der besonderen personenbezogenen Daten aufgenommen (§ 27 Abs. 4 SOG MV).

Die unter Art. 6 fallenden besonderen Kategorien personenbezogener Daten sind in der polizeilichen Arbeit häufig betroffen. Beispielsweise wird die rassische und ethnische Herkunft als Datum verarbeitet bei Straftaten gegen oder durch Ausländer, die politische Meinung bei Staatsschutzdelikten, die religiöse Überzeugung bei Ermittlungen zum islamischen Extremismus, Gesundheitsdaten bei Infektionsgefahren für Polizeibeamte oder Daten über das Sexualleben bei Exhibitionismus und Vergewaltigung.

**c) Umsetzungsbedarf**

Trotz des Fehlens ausdrücklicher Regelungen in den Polizeigesetzen der Länder zieht Art. 6 keinen zwingenden Umsetzungsbedarf nach sich. Durch Schaffung von klarstellenden Regelungen könnte jedoch die besondere Bedeutung der in Art. 6 genannten Daten hervorgehoben werden.

**aa) Unbedingte Notwendigkeit der Verarbeitung**

Gegenüber dem 2005 in den Bundesrat eingebrachten Rahmenbeschluss-Vorschlag wurde die Regelung des Art. 6 von einem grundsätzlichen Verbot der Verarbeitung besonderer personenbezogener Daten zu der jetzigen Fassung abgemildert.
Im Rahmenbeschlussvorschlag für die Bundesratsunterrichtung hatte Art. 6 noch folgenden Wortlaut gehabt:

„**Artikel 6**
**Verarbeitung besonderer Kategorien personenbezogener Daten**

1. Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.
2. Absatz 1 findet keine Anwendung,
   – wenn die Verarbeitung gesetzlich vorgeschrieben und unabdingbar für die Erfüllung der rechtmäßigen Aufgaben der betreffenden Behörde im Hinblick auf die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten ist oder die betroffene Person ausdrücklich ihre Einwilligung zu der Datenverarbeitung erteilt hat, und
   – wenn die Mitgliedstaaten für spezifische Fälle geeignete Garantien vorsehen, beispielsweise eine Beschränkung des Datenzugriffs auf das für die rechtmäßige, die Datenverarbeitung rechtfertigende Verarbeitung zuständige Personal.“

In der geltenden Fassung des Art. 6 wird die Verarbeitung der besonderen personenbezogenen Daten nunmehr an einen qualifizierten Zulässigkeitsmaßstab gebunden, der sowohl die unbedingte Notwendigkeit als auch die Gewährleitung innerstaatlichen Schutzes

statuiert. Das der ursprünglichen Regelung noch eigene strenge Regel-Ausnahme-Verhältnis besteht dagegen nicht.

Die Prüfung der unbedingten Notwenigkeit ist kein den Ländergesetzen fremder Aspekt. Vielmehr hat bereits jetzt im Rahmen der Verhältnismäßigkeitsprüfung eine Beachtung besonderer Arten von Daten stattzufinden, wenn diese einen speziellen Grundrechtsschutz für die Betroffenen aufweisen oder dem Privat- und Intimbereich zuzuordnen sind. Dass jeweils eine Abwägung stattzufinden hat, ergibt sich aus den Grundsätzen der Erforderlichkeit („Datenverarbeitung nur, soweit und solange dies zur Aufgabenwahrnehmung erforderlich ist“) sowie der Datensparsamkeit.
Besondere Abwägungsaspekte auf Seiten der Betroffenen sind für alle in Art. 6 genannten Kategorien gegeben und führen bereits zur Einschränkung der Datenverarbeitung:
- für die Kategorie rassische und ethnische Herkunft vor dem Hintergrund von Art. 3 Abs. 3 GG
- für die religiöse oder philosophische Überzeugung aufgrund von Art. 4 GG
- für die Gewerkschaftszugehörigkeit angesichts von Art. 9 Abs. 3 GG
- für Gesundheit und Sexualleben durch die Betroffenheit des Privat- bzw. Intimbereich der Betroffenen, d.h. des Kernbereichs der Persönlichkeit und damit des Kernbereichs des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG).

**bb) Angemessener Schutz durch innerstaatliches Recht**
Der als zweite Voraussetzung in Art. 6 geforderte angemessene innerstaatliche Schutz bedeutet nicht, dass für die besonderen Arten von Daten neue, sonst nicht zur Anwendung kommende Schutzmechanismen entwickelt werden müssen. Vielmehr ist es erforderlich, aber auch ausreichend, die möglichen Schutzmaßnahmen (z.B. beschränkter Nutzerkreis, Vorgesetztenkontrolle, kurze Prüffristen) jeweils auf die Dateien, in denen die besonderen Arten von Daten verarbeitet werden, spezifisch anzupassen. Für diese Auslegung der Voraussetzung „angemessener Schutz“ spricht auch die oben unter aa) zitierte frühere „strengere“ Fassung von Art. 6, in der es hieß:

> „[Die Datenverarbeitung ist nicht untersagt,]
> – wenn die Mitgliedstaaten für spezifische Fälle geeignete Garantien vorsehen, beispielsweise eine Beschränkung des Datenzugriffs auf das für die rechtmäßige, die Datenverarbeitung rechtfertigende Verarbeitung zuständige Personal.“

Angesichts der Verhältnismäßigkeitsprüfung, die den Grundrechtsschutz oder Kernbereich des Rechts auf informationelle Selbstbestimmung zu berücksichtigen hat, werden in der Praxis der Länder für deren Staatsschutz-/ Extremismus-/ u.ä.-Dateien bereits spezifische angepasste Nutzungs- und Datenschutzregelungen vorgesehen und in deren Errichtungsanordnungen bzw. Verfahrensverzeichnissen sowie Datenschutz- und Sicherheitskonzepten beschrieben. Ergänzt wird der Schutz durch die bestehenden Rechte der Betroffenen (Auskunft, Löschung, Schadensersatz usw.) einschließlich der Anrufung der Gerichte (Art. 19 Abs. 4 GG) und die zur Verfahrenssicherung vorgesehene Vorabkonsultation in Art. 23 des hiesigen Rahmenbeschlusses, der in den Ländergesetzen bereits eine vergleichbare Umsetzung gefunden hat (vgl. Ausführungen bei Art. 23).

**cc) Klarstellende Regelung**

Eine Art. 6 umsetzende Regelung erscheint nicht erforderlich. Gegebenfalls kann jedoch eine deklaratorische Umsetzung für förderlich erachtet werden, die dann den Wortlaut des Art. 6 aufgreift oder auf die entsprechenden landesdatenschutzrechtlichen Regelungen Bezug nimmt und deren Anwendungsbereich erweitert. Eine Einschränkung auf den Anwendungsbereich des Rahmenbeschlusses, d.h. auf die Datenübermittlung und -bereitstellung zwischen Mitgliedstaaten, wäre allerdings bei einer Umsetzung nur schwer möglich, denn alle Daten könnten potenziell im weiteren Verarbeitungsverlauf Inhalt von Übermittlungen an andere Staaten sein. In § 27 Abs. 4 des SOG MV wurde eine allgemein für die Polizei geltende Vorschrift zum Umgang mit den besonderen Arten personenbezogener Daten gewählt.

## 5. Artikel 7 – Automatisierte Einzelentscheidungen

Art. 7 enthält Sondervorschriften für automatisierte Einzelentscheidungen. Zahlreiche Ländergesetze enthalten für den allgemeinen Datenschutz, nicht aber für den Polizeibereich vergleichbare ausdrückliche Verbotsregelungen für automatisierte, nachteilige Entscheidungen, u.a. Art. 15 Abs. 6 DSG BY, § 5a HmbDSG, § 10a NDSG i.V.m. § 48 Nds. SOG, § 19 LDSG SH. Bundesgesetzlich bestehen Regelungen in § 6a BDSG oder § 114 Abs. 4 BBG. Keine Regelungen enthält u.a. das LDSG BW.

Umsetzungsbedarf besteht jedoch nicht. Es ist anzunehmen, dass die hiesige Regelung von der Parallelvorschrift aus Art. 15 der Richtlinie 95/46/EG für den Datenschutz der sog. Ersten Säule geprägt wurde. Während für dessen Themenfelder Anwendungsbeispiele bestehen bzw. bestanden, wie z.B. bei Entscheidungen über Bankkredite mittels Online-Verfahrens oder bei der Bewerberauswahl über elektronisch generierte Rankings, sind solche im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen nicht gegeben. Vielmehr gehen Entscheidungen mit nachteiligen Rechtsfolgen immer auf das Tätigwerden einer natürlichen Person, die die Daten bewertet und eine Entscheidung trifft, zurück. Dass dies so ist, wird durch die Verfassungsgrundsätze aus Art. 1 Abs. 3 GG (Grundrechtsbindung der vollziehenden Gewalt und Rechtsprechung) und Art. 103 Abs. 1 GG (Anspruch auf rechtliches Gehör) abgesichert.

## 6. Artikel 8 – Überprüfung der Qualität der übermittelten oder bereitgestellten Daten

Art. 8 stellt zur Gewährleistung der Qualität von übermittelten oder bereitgestellten Daten vier Forderungen auf:

- So soll die Behörde, soweit möglich, vor Übermittlung die Datenqualität prüfen (Abs. 1 Sätze 1 und 2) und
- nach Möglichkeit bei der Übermittlung Informationen zur Beurteilung der Datenqualität durch den Empfänger beifügen (Abs. 1 Satz 3).
- Ohne Einschränkung „nach Möglichkeit“ sind Daten, die ohne Ersuchen zugegangen sind, auf ihre Speichernotwendigkeit zu prüfen (Abs. 1 Satz 4) und es besteht
- die Pflicht, bei festgestellter Unrichtigkeit oder Unrechtmäßigkeit unverzügliche Mitteilung an den Empfänger machen. Dieser ist verpflichtet, die Daten zu berichtigen, zu löschen oder zu sperren (Abs. 2).

**a) Qualitätssicherung und –prüfung (Abs. 1 Satz 1 und 2)**
Vergleichbar detaillierte ländergesetzliche Regelungen zur bestehen nicht. Vielmehr werden die möglichen Rechtsfolgen für die Verarbeitung unrichtiger Daten im Wege von Lösch-, Sperr- und Berichtigungspflichten bzw. -ansprüchen (vgl. Ausführungen zu Art. 4) geregelt. Hiermit verbunden und als „angemessene Maßnahme“ im Sinne von Satz 1 anzusehen sind insbesondere die detaillierten ländergesetzlichen Regelungen zu den Prüffristen von Daten (vgl. Ausführungen zu Art. 5), durch die eine regelmäßige Richtigkeitskontrolle - schon im Eigeninteresse der Polizei - sichergestellt wird.

In der Aufzählung in Art. 8 Abs. 1 Satz 1 kommt dem Begriff „unvollständig“ nur als Unterfall von „unrichtig“ Sinn zu. Nur wenn der unvollständige Datenbestand Anlass gibt, von Fehlern bei seiner Verarbeitung auszugehen, ist die Rechtsfolge auf Unterlassung der Übermittlung folgerichtig. Andernfalls wären Ergänzungen der unvollständigen Daten oder Hinweise auf die Unvollständigkeit je nach Einzelfall die Folge. Als Unterfall des Begriffs „unrichtig“ reiht sich „unvollständig“ dann ebenso ein wie die dritte Aufzählung „nicht mehr aktuell“.

Umsetzungsbedarf besteht für Art. 8 Abs. 1 Satz 1 und 2 nicht, da, wie erwähnt, mit den Prüffristen / -pflichten angemessene Maßnahmen zur Richtigkeitskontrolle bestehen. Zudem ist der Praxis des Auslandsdatenverkehrs die Einzelfallprüfung eigen, die sich insbesondere mit der Zulässigkeit der Anfrage und mit dem Umfang an Daten, die zur Verfügung gestellt werden können, befasst, dabei aber zugleich auch erkennbare Zweifel an der Datenqualität aufgreifen kann und wird. In Art. 8 Abs. 1 Satz 2 wird insofern auch nochmals darauf abgestellt, dass die Qualitätskontrolle nur „soweit praktisch möglich“ erfüllt werden muss.

**b) Beifügen von Informationen zur Plausibilitätsprüfung (Abs. 1 Satz 3)**
Zur zweiten Anforderung aus Art. 8, der Übermittlung von Informationen, die es dem Empfänger gestatten, Richtigkeit, Vollständigkeit, Aktualität und Zuverlässigkeit zu beurteilen, kann es sich nach dem Grundsatz der Datensparsamkeit nur um solche Informationen handeln, mit denen nicht ein „Mehr“ an personenbezogenen Daten übermittelt wird, als erfragt ist (und zulässig übermittelt werden darf).
Solche Informationen für die Qualitätsbeurteilung könnten daher insbesondere nur das Speicherdatum des Datensatzes oder der Kurzsachverhalt sein, der in den länderpolizeilichen Auskunftssystemen zumindest in den Fällen mittlerer und schwerer Kriminalität erfasst ist (sog. T-Gruppe) und bereits in der derzeitigen Praxis Bestandteil von Übermittlungen ist. Bislang beziehen sich Übermittlungen an andere Mitgliedstaaten, für die die Länder die Daten liefern, zumeist noch weniger auf Gefahren- oder Ermittlungserkenntnisse als auf Katalogdaten wie Wohnsitz oder Telefonanschluss und sind dann mit dem Speicherdatum als Zusatzinformation verbindbar.

Mit Blick auf die auch hier enthaltene Einschränkung zur Informationsbeifügung „nach Möglichkeit“ wird vorgeschlagen, von einer gesetzlichen Umsetzung abzusehen, aber ggf. in Verwaltungsvorschriften oder Dienstanweisungen entsprechende Regelungen mit aufzunehmen.

**c) Prüfpflicht bei unverlangt übermittelten Daten (Abs. 1 Satz 4)**

In Art. 8 Abs. 1 Satz 4 wird die Pflicht statuiert, bei Datenerhalt ohne vorheriges Ersuchen zu prüfen, ob die Daten für den übermittelten Zweck benötigt werden. Insoweit implizieren bereits die Datenschutzgrundsätze der Erforderlichkeit und der Rechtmäßigkeit der Datenverarbeitung (vgl. auch Art. 3) die landespolizeiliche Prüfung, ob und inwieweit erhaltene Daten im eigenen System verarbeitet werden können. Ein Umsetzungsbedarf besteht nicht.

Eine Zweckbindungsregelung enthält Satz 4 dabei nicht, da der Fokus der Regelung, wie für den gesamten Art. 8, auf der Prüfpflicht liegt.

**d) Folgen bei Übermittlung unrichtiger Daten und bei unrechtmäßiger Übermittlung (Abs. 2)**

Art. 8 Abs. 2 enthält die vierte Anforderung, dass eine unverzügliche Nachmeldung an den Empfänger zu erfolgen hat, wenn die Unrichtigkeit der Daten oder die Unrechtmäßigkeit der Übermittlung festgestellt wird. Dieser ist verpflichtet, die Daten zu berichtigen, zu löschen oder zu sperren.

Anders als bei Abs. 1 lässt sich hier für den neben die Unrichtigkeit tretenden Grund der Unrechtmäßigkeit nicht argumentieren, dass es sich bei „unrechtmäßig“ um einen Unterfall des Begriffs „unrichtig“ handelt, auch wenn Art. 8 im Schwerpunkt den Umgang mit unrichtigen Daten regelt. Einen Aspekt der unrechtmäßigen Übermittlung greift vielmehr Art. 8 Abs. 1 Satz 4 zur „Übermittlung ohne Ersuchen“ auf. Zugleich ist in Art. 8 Abs. 2 ein Verweis auf Art. 4 enthalten, in dem ebenfalls neben der Unrichtigkeit als Berichtigungs-, Lösch- oder Sperrgrund auf die Rechtmäßigkeit der Datenerhebung oder -verarbeitung abgestellt wird.

**aa) Unverzügliche Mitteilung an den Empfänger**

Ländergesetzlich wird eine vergleichbare Mitteilungspflicht bei Unrichtigkeit im Zusammenhang mit den Themen Berichtigung, Sperrung und Löschung geregelt, entweder in den allgemeinen Datenschutzgesetzen, z.B. §§ 22 Abs. 2, 23 Abs. 5, 24 Abs 5 LDSG BW, § 17 Abs. 4 NDSG, § 28 LDSG SH oder im Polizeirecht, Art. 45 Abs. 1 Satz 3 PAG BY und § 24 Abs. 5 HmbPolDVG. Die festgestellte „Unrechtmäßigkeit“ der Datenübermittlung als Mitteilungsanlass findet sich im Wortlaut nicht.

In den Länderregelungen wird - mit abweichenden Formulierungen - i.d.R. zugleich eine Einschränkung der Mitteilungspflicht im Sinne einer Verhältnismäßigkeitsprüfung statuiert, nach der mit Blick auf die Wahrung der Betroffeneninteressen (oder die Aufgabenerfüllung der verantwortlichen Stelle) oder einen unverhältnismäßigen Aufwand eine Berichtigung des Empfängers ggf. unterbleiben kann.

Derartige Einschränkungen nach der Verhältnismäßigkeit enthält Art. 8 Abs. 2 nicht. Angeführt werden kann allerdings, dass der Grundsatz der Verhältnismäßigkeit auch ein Grundsatz des Europarechts ist. Als zentraler Abwägungsaspekt für die Empfängerbenachrichtigungen wird in den Ländergesetzen die Wahrung der schutzwürdigen Interessen des Betroffenen herausgestellt, die in gleicher Weise Kernzweck des deutschen und des europäischen Datenschutzes sind.

Den Aspekt der unrechtmäßigen Datenübermittlung regeln die Ländergesetze, wie gesagt, bei der Benachrichtigungspflicht der Datenempfänger nicht mit. Insoweit kann „nur" darauf abgestellt werden, dass die allgemeine Verantwortung für die Datenübermittlers in den Landesgesetzen geregelt wird, z.B. in § 41 PolG BW: „Bei der Übermittlung personenbezogener Daten trägt die übermittelnde Stelle die Verantwortung für deren Zulässigkeit" (ähnlich in § 18 Abs. 4 S. 1 HmbPolDVG, § 11 NDSG, § 191 LVwG SH). Dazu, so ist argumentierbar, gehört es, dass der verantwortliche Übermittler die nachträglich festgestellte Unrechtmäßigkeit seiner Übermittlung zu bereinigen versucht, um den Fehler nicht zu perpetuieren und sich (weiteren) Haftungsansprüchen auszusetzen.

**bb) Berichtigung, Löschung, Sperrung nach Art. 4**

Zu den Rechtsfolgen Berichtigen, Löschen oder Sperren sind Ausführungen bei Art. 4 erfolgt. Eine eigenständige Funktion des Verweises in Art. 8 Abs. 2 auf Art. 4 ist, über eine Konkretisierung der Rechtsfolgenwahl zwischen Berichtigung, Löschung und Sperrung hinaus, allerdings nicht ersichtlich. Insoweit sieht Art. 4 für den Fall unrichtiger Daten vorrangig die Berichtigung, bei unrechtmäßiger Übermittlung vorrangig die Rechtsfolge Löschung vor.

Landesrechtlich bestehen Lösch-, Sperr- und Berichtigungspflichten, die sprachlich typischerweise die „Unzulässigkeit der Speicherung" voraussetzen (vgl. auch bei Art. 3 Grundsatz der Rechtmäßigkeit).
Nicht zu vertiefen, aber ebenfalls zu diesem Kontext gehörig ist die streitige Frage, ob und unter welchen Voraussetzungen ggf. rechtswidrig erhobene Daten verwendet werden können und ob ihre weitere Verarbeitung stets „unzulässig" wäre, d.h. die Löschung oder Sperrung nach sich ziehen muss (sog. „fruit of the poisonous tree doctrine").

**cc) Umsetzungsbedarf**

Als gut vertretbar wird es angesehen, von einer Umsetzung für Art. 8 Abs. 2 Satz 1 und 2 aus den genannten Gleichstellungsgründen mit dem bestehenden Landesrecht abzusehen. Wenn zur Sicherstellung der Empfängerbenachrichtigung (Satz 1) und Löschung (Satz 2) eine klarstellende Regelung erfolgen soll, könnte dies auf untergesetzlicher Ebene im Wege einer Verwaltungsvorschrift oder Dienstanweisung geschehen. Gleichförmige Abwägungs- und Anwendungsergebnisse können auf diesem Wege ebenso sichergestellt werden wie die Unverzüglichkeit der Benachrichtigung und eine Berichtigung, Löschung oder Sperrung als Empfänger.

## 7. Artikel 9 – Fristen

Nach Art. 9 Abs. 1 kann die übermittelnde Behörde die für sie geltenden Prüf- und Löschfristen auch für den Empfänger der Daten verbindlich machen, indem sie die Fristen nach dort mitteilt. Der Empfänger hat sich an diese Fristen zu halten, wenn die Daten nicht für laufende Ermittlungen, die Strafverfolgung oder die Strafvollstreckung benötigt werden. Ansonsten gilt für den Empfänger das eigene innerstaatliche Recht (Abs. 2).

Die Polizeigesetze der Länder enthalten bislang keine entsprechenden Regelungen.

Für ausgehende Daten enthält Art. 9 Abs. 1 Satz 1 eine Kann-Regelung, aufgrund derer es nicht nur im einzelnen Übermittlungsfall, sondern bereits allgemein zur Frage einer landesrechtlichen Umsetzung möglich ist, sich für oder gegen eine Fristenbindung des Empfängers zu entscheiden. Gegen eine Umsetzung der Kann-Regelung könnte u.a. sprechen, dass mit dem vorliegenden Rahmenbeschluss bereits sichergestellt wird, dass alle Datenempfänger angemessene Prüf- und Speicherfristen vorsehen (vgl. insbesondere Art. 5). Ebenfalls dürfte eine Änderung und Verschärfung der polizeilichen Praxis nicht intendiert sein.

Umsetzungsbedarf ist allerdings für eingehende Daten gegeben, d.h. soweit es Art. 9 Abs. 1 S. 2 und die Bindung der eigenen Landespolizei als empfangende Stelle an die vom Übermittler angegebenen Fristen betrifft.

Eine umsetzende Regelung - hier als Beispiel der Umsetzung beider Teilaspekte - könnte lauten:

> *„Der empfangenden Stelle können die innerstaatlich geltenden Fristen für die Aufbewahrung der Daten mitgeteilt werden, nach deren Ablauf auch der Empfänger die Daten zu löschen oder zu sperren oder zu prüfen hat, ob sie noch benötigt werden.*
> *Durch die übermittelnde Stelle angegebene Fristen sind zu beachten. Dies gilt nicht, wenn die Daten bei Fristablauf zur Verhütung oder Verfolgung einer Straftat oder zur Strafvollstreckung benötigt werden.“*

Weitere bindende Hinweise des Übermittlers an den Empfänger enthalten neben Art. 9 auch Art. 12, 14 und 16, jedoch mit Unterschieden in der Ausformung der Regelungen. So handelt es sich u.a. bei Art. 12 im Gegensatz zu Art. 9 nicht um eine Kann-Regelung bei der Übermittlung von innerstaatlichen Verarbeitungsbeschränkungen; im Fall von Art. 14 Abs. 2 sind andere Übermittlungsvorgänge - an nicht-öffentliche Stellen - betroffen und bei Art. 16 Abs. 2 wird auf Vorgänge gestellt, in denen das Ersuchen um Nicht-Information der betroffenen Personen vom Übermittlungsvorgang ggf. zeitlich getrennt erfolgen kann (vgl. die Ausführungen zu diesen Vorschriften).

## 8. Artikel 10 – Protokollierung und Dokumentierung

Nach Art. 10 sind Datenübermittlungen zu protokollieren oder zu dokumentieren und die entsprechenden Protokolldateien auf Verlangen der zuständigen Kontrollstelle vorzulegen.

### a) Dokumentationspflicht (Abs. 1)

#### aa) Regelungsgehalt

Die hier verwendeten Begriffe Protokollieren und Dokumentieren beziehen sich typischerweise für das Protokollieren auf die automatisierte Datenverarbeitung und für das Dokumentieren auf die nicht-automatisierte Verarbeitung. Vergleichbare Begriffe des Protokollierens, aktenkundig Machens oder Dokumentierens verwenden die Ländergesetze - tendenziell mit der Protokollierung als Unterfall der anderen zwei - ohne dass eine strenge Begriffstrennung erfolgen würde. Auch für Art. 10 ist eine Begriffstrennung nicht erforderlich, da dieselbe Rechtsfolge statuiert wird.

Protokollieren und Dokumentieren zum Zwecke der Datenschutzkontrolle bezieht sich auf die übermittelten Daten, Anlass und Zeitpunkt der Übermittlung sowie die verantwortlichen Beteiligten. Unten im Abschnitt D. II. 2. ist beim Vergleich zum Ratsbeschluss Prüm zu Art. 30 Ratsbeschluss Prüm näher ausgeführt, dass sich der Protokollierungs- bzw. Dokumentationsumfang an der insoweit ausführlicheren Regelung in Art. 30 Abs. 1 Ratsbeschluss Prüm orientieren kann. Die Grundsätze der Datensparsamkeit und die Zugangsbeschränkung, z.B. auf Administratoren, und (technische) Sicherung der Protokolldateien bzw. Dokumentationen sind ergänzend zu beachten.

**bb) Landespolizeigesetzliche Regelungen**

Die Vorgabe, dass jede Datenübermittlung zu protokollieren ist, enthalten die Ländergesetze typischerweise im Zusammenhang mit der Regelung zum automatisierten Abrufverfahren, so u.a. Art. 46 Abs. 2 BY PAG, § 194 Abs.1 LVwG, § 42 Abs. 2 Nds.SOG, während andere Ländergesetze Vorgaben zu (zumindest) geeigneten Stichprobenverfahren machen, z.B. § 42 Abs. 5 PolG BW und § 27 Abs. 1 Satz 4 HmbPolDVG.

Die Datenübermittlung an andere Staaten ist noch von der konventionellen Übermittlung geprägt und der automatisierte Abruf i.d.R. ausgeschlossen. Technisch wäre eine Vollprotokollierung einfach realisierbar und ist in der Arbeit mit Dateien, z.B. länderpolizeilichen Auskunftssystemen oder Schnittstellen zu INPOL auch bereits üblich.

Das Dokumentieren bzw. aktenkundig Machen wird als landesgesetzliche Vorgabe im Zusammenhang mit der Datenübermittlung nur in Teilen ausdrücklich geregelt, z.B. in § 40 Abs. 1 Satz 2 SOG NI für Übermittlungen mit Zweckänderung oder in § 191 Abs. 4 LVwG SH für jede Übermittlung personenbezogener Daten, sofern das Ersuchen nicht mündlich vorgetragen wird und zur Person bereits schriftliche Unterlagen bestehen. Für die öffentliche Verwaltung besteht eine Pflicht zur Aktenführung aber bereits auch dann, wenn dies nicht ausdrücklich bestimmt ist (BVerfG, Beschluss vom 06.06.1983, NJW 1983, 2135 - stRspr.). Diese Pflicht wird durch die drei Gebote der Vollständigkeit, Aktenmäßigkeit und der wahrheitsgetreuen Aktenführung ausgefüllt. Die Aktenführung dient als Erkenntnisquelle für das Verwaltungshandeln und als Grundlage für die Nachprüfung der Verwaltungsentscheidungen durch übergeordnete Behörden und Gerichte. Im Zusammenhang mit dem - andernfalls nicht erfüllbaren - Akteneinsichtsrecht nach § 29 VwVfG wird die vorausgesetzte Pflicht zur Aktenführung / Dokumentation ebenfalls deutlich.

**cc) Umsetzungsbedarf**

Daher erscheint es gut vertretbar, für Art. 10 Abs. 1 auf eine Umsetzungsregelung zu verzichten.
Alternativ könnte eine klarstellende Regelung gewählt werden, so wie dies z.T. zur Betonung der Aktendokumentation beim Einsatz besonderer Datenerhebungsmittel, wie z.B. beim Einsatz Automatischer Kennzeichenlesesysteme, geschieht (vgl. § 22a Abs. 1 Satz 4 PolG BW). Anbieten würde sich dann z.B. eine - ggf. zusätzlich den Anwendungsbereich des Rahmenbeschlusses nochmals benennende - Formulierung: „Jede Übermittlung ist zu dokumentieren.“, wobei sich das Dokumentieren, wie gesagt, als Oberbegriff für protokollieren und (in Papierform) dokumentieren darstellt.

**b) Einsichtsrechte der Kontrollstelle (Abs. 2)**

Bezüglich Art. 10 Abs. 2 sind die Einsichtsrechte der Landesbeauftragten für den Datenschutz in die Protokolle und Dokumentationen bereits landesgesetzlich gesichert, § 29 Abs. 1 LDSG BW, Art. 32 Abs. 1 DSG BY, § 23 Abs. 5, 6 HmbDSG, § 22 NDSG, § 41 LDSG SH.

Zur Dauer der Speicherung der Protokoll- und Dokumentationsdaten und ihrer Verfügbarmachung an die Kontrollstelle werden durch den Rahmenbeschluss keine Vorgaben gemacht.

## 9. Artikel 11 – Verarbeitung personenbezogener Daten, die von einem anderen Mitgliedstaat übermittelt oder bereit gestellt wurden

Art. 11 legt den Mitgliedsstaaten Verwendungsbeschränkungen auf. Er regelt, für welche anderen Zwecke als diejenigen, für welche die personenbezogenen Daten übermittelt oder bereit gestellt wurden, diese grundsätzlich noch verarbeitet werden dürfen. Damit wird einerseits eine Durchbrechung des Zweckbindungsgrundsatzes, anderseits aber auch eine ausdrückliche Beschränkung vorgenommen.

Art. 11 gilt für die Verarbeitung in dem Mitgliedstaat, dem die Daten übermittelt oder bereit gestellt wurden, und umfasst auch die Weiterübermittlung an andere öffentliche Stellen des empfangenden Mitgliedstaats. Für die Weiterleitung an die zuständigen Behörden in Drittstaaten oder an internationale Einrichtungen ist Art. 13 und für die Übermittlung von Daten an nicht-öffentliche Stellen in Mitgliedstaaten ist Art. 14 spezieller.

**a) Voraussetzungen der Verarbeitung für andere Zwecke (Satz 1)**

Art. 11 Satz 1 sieht vor, dass personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaates übermittelt oder bereitgestellt wurden, unter den Voraussetzungen des Art. 3 Abs. 2 nur für bestimmte, in den Art. 11 Satz 1 lit. a-c genannte andere Zwecke als diejenigen, für die sie übermittelt oder bereitgestellt wurden, weiter verarbeitet werden dürfen. Andernfalls – also für die Verarbeitung zu jedem anderem Zweck – wäre gemäß Art. 11 Satz 1 lit. d die vorherige Zustimmung des übermittelnden Mitgliedstaates oder die Einwilligung der betroffenen Person erforderlich. Es ist folglich zu prüfen, was im Einzelnen unter den in Art. 11 Satz 1 lit. a-c genannten Zwecken zu verstehen ist und ob die Landespolizeigesetze eine Beschränkung der Datenverarbeitung zu den derart herausgearbeiteten Zwecken vorsehen oder darüber hinausgehen.

**aa) Voraussetzungen des Art. 3 Abs. 2**

Allen in den Art. 11 Satz 1 lit. a-c genannten Zwecken ist aufgrund des Wortlauts zunächst gemein, dass die weitere Datenverarbeitung die Vorgaben des Art. 3 Abs. 2 beachten muss, der insoweit eine Ausprägung des Verhältnismäßigkeitsgrundsatzes darstellt.

**bb) Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder Vollstreckung von strafrechtlichen Sanktionen**

Die weitere Datenverarbeitung ist gemäß Art. 11 Satz 1 lit. a zulässig zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder Vollstreckung von strafrechtlichen Sanktionen, bei denen es sich nicht um die Straftaten oder Sanktionen handelt, für die sie übermittelt oder bereitgestellt wurden. Für letztere fehlt es bereits an der Zweck-

änderung. Die Einschränkung, dass es sich dabei nicht um die Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder Sanktionen handelt, für die die Daten seinerzeit übermittelt oder bereitgestellt wurden, dient daher insoweit der Klarstellung, erscheint aber entbehrlich.
Das Bundesministerium des Innern hat in seinen Anwendungshinweisen zum BKAG eine verkürzte Formulierung gewählt. Danach ist eine Verwendung von aus Mitgliedstaaten übermittelten Daten zur Verhütung oder Verfolgung von Straftaten oder Vollstreckung von strafrechtlichen Sanktionen zulässig.
Die Landesgesetze sehen eine Zweckänderung zur Verhütung von Straftaten regelhaft vor. So heißt es beispielsweise in § 14 Abs. 1 Satz 2 HmbPolDVG: Die Nutzung einschließlich einer erneuten Speicherung und einer Veränderung zu einem anderen polizeilichen Zweck ist zulässig, soweit die Polizei die Daten zu diesem Zweck erheben dürfte (vgl. auch § 39 Abs. 1 Nds. SOG, § 37 Abs. 2 Satz 2 PolG BW, Art. 37 Abs. 2 Satz 2 BY PAG, § 188 Abs. 1 Satz 3 LVwG). § 1 Abs. 1 HmbPolDVG definiert drei Aufgabenbereiche im Rahmen der polizeilichen Datenverarbeitung (Gefahrenabwehr i.S.d. § 3 HmbSOG, vorbeugende Bekämpfung von Straftaten, Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen). Da aus der Zuweisung von Aufgaben noch nicht die Befugnis zum Einsatz von Mitteln folgt, die zu einer rechtlichen Belastung des Bürgers führt (vgl. Schenke, Polizei- und Ordnungsrecht, 6. Auflage 2009, Rn. 36), ist auf diejenigen Normen zurückzugreifen, die eine Datenerhebung zum Zwecke der Straftatenverhütung erlauben. Die Befugnis zur Datenerhebung zum Zwecke der Verhütung von Straftaten ergibt sich in unterschiedlichen Befugnisnormen (vgl. z.B. § 6 Nr. 6, § 9 Abs. 1 Nr. 2, § 10 Abs. 1 HmbPolDVG; § 179 Abs. 2 LVwG; § 31 Abs. 2, § 34 Abs. 1 Nr. 2 Nds. SOG; Art. 31 Abs. 1 Nr. 1 BY PAG; § 20 Abs. 2, 3 Nr. 1 PolG BW).
Damit stünden die Landespolizeigesetze im Einklang mit den Vorgaben des Rahmenbeschlusses, soweit sie auch eine Nutzungsänderung zum Zwecke der Verhütung von Straftaten erlauben. Die Ländergesetze dürften jedoch insgesamt weiter gefasst sein, denn sie erlauben eine Zweckänderung regelhaft, wenn die Polizei die Daten zu diesem Zweck erheben dürfte (vgl. § 14 Abs. 1 Satz 2 HmbPolDVG, Art. 37 Abs. 2 Satz 2 BY PAG, § 188 Abs. 1 Satz 2 LVwG, § 37 Abs. 2 S. 2 PolG BW, § 39 Abs. 1 Nds. SOG). Dies geht über die Zweckbeschränkung des Art. 11 Satz 1 lit. a hinaus und bedürfte insoweit der Begrenzung.

**cc) Andere justizielle und verwaltungsbehördliche Verfahren**

Art. 11 Satz 1 lit. b erlaubt die Durchbrechung des Zweckbindungsprinzips, wenn die übermittelten oder bereitgestellten personenbezogenen Daten für andere justizielle und verwaltungsbehördliche Verfahren, die mit der Verhütung, Ermittlung, Feststellung oder Strafverfolgung von Straftaten oder Vollstreckung von strafrechtlichen Sanktionen unmittelbar zusammenhängen, verwendet werden.
Fraglich ist zunächst, welche Verfahren darunter zu verstehen sind. Den Erwägungsgründen lässt sich in Nr. 21 insoweit nur entnehmen, dass die Weiterverarbeitung von personenbezogenen Daten für Verwaltungsverfahren auch die Tätigkeiten von Regulierungs- oder Aufsichtsbehörden in diesen Verfahren umfasst. Konkrete Auslegungshinweise ergeben sich jedoch, wenn man die gleichlautende Formulierung in Art. 23 Abs. 1 lit. b des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der

Europäischen Union (EU-RhÜbk) in den Blick nimmt.[2] Denn eine Erklärung für die dort verwendete Formulierung ergibt sich wiederum aus dem Erläuternden Bericht zu dem EU-RhÜbk. Sonstige justizielle und verwaltungsbehördliche Verfahren, die mit der Strafverhütung, -ermittlung, -feststellung oder -verfolgung unmittelbar zusammenhängen, können danach beispielsweise folgende Fälle sein:

- Verfahren in Handelssachen in Zusammenhang mit einem betrügerischen Bankrott,
- Verfahren betreffend den Entzug des Sorgerechts in Zusammenhang mit einem Strafverfahren wegen Kindesmisshandlung,
- Verfahren betreffend den Entzug eines Waffenscheins in Zusammenhang mit einem Strafverfahren wegen eines Gewaltdelikts mit Waffen (vgl. Erläuternder Bericht zu dem Übereinkommen vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (2000/C/379/02, S. 27)).

Beispiele für mit Strafverfahren zusammenhängende justizielle Verfahren dürften sich auch aus § 14 Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) ergeben. Dort sind z.B. Mitteilungen vorgesehen, wenn diese für den Widerruf, die Rücknahme o.ä. erforderlich sind, falls der Betroffene Inhaber einer atom-, waffen- oder sprengstoffrechtlichen Berechtigung ist (vgl. § 14 Abs. 1 Nr. 7 lit. b EGGVG). Nach allem weist Art. 11 Satz 1 lit. b einen weiten Anwendungsbereich auf. So kann beispielsweise die Datenübermittlung zur Feststellung der gesetzlichen Voraussetzungen für den Erlass eines Verwaltungsaktes durch eine andere für Aufgaben der Gefahrenabwehr zuständige öffentliche Stelle unter Art. 11 Satz 1 lit. b subsumiert werden (vgl. § 20 Abs. 1 Satz 1 Nr. 4, § 20 Abs. 2 HmbPolDVG sowie Art. 40 Abs. 3, 4 BY PAG, § 41 Nds. SOG, §§ 192 Abs. 1, 193 Abs. 1 LVwG, §§ 42 Abs. 2, 43 Abs. 1 PolG BW).
Die Projektgruppe hat sich auch die Frage gestellt, in welchen Anwendungsbereich der in Art. 11 Satz 1 genannten Buchstaben die Verwendung übermittelter oder bereitgestellter Daten für die Verfolgung von Ordnungswidrigkeiten fällt. Eine Subsumtion unter Art. 11 Satz 1 lit. a würde voraussetzen, dass der Begriff der Ordnungswidrigkeit unter den Straftatenbegriff des Art. 11 subsumiert werden könnte. Dies wurde verneint.[3] Die Verwendung zur Verfolgung von Ordnungswidrigkeiten lässt sich aber bei Berücksichtigung der vorstehend genannten Beispiele unter Art. 11 Satz 1 lit. b subsumieren.

Die genannten Regelungen beschränken die Zweckänderung bzw. Übermittlung von Daten nicht auf Verfahren, die mit dem der Übermittlung zugrunde liegenden Verfahren in Zusammenhang stehen. Auch insoweit muss daher zur Umsetzung des RB DS eine Begrenzung erfolgen.

---

[2] Die in Art. 11 S. 1 lit. b verwendete Formulierung findet sich beispielsweise auch im Rahmenbeschluss 2008/978/JI des Rates vom 18. Dezember 2008 über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafsachen. Eine Umsetzung dieses Rahmenbeschluss durch den Bund steht aber noch aus, insofern können aus einem möglichen Gesetzgebungsverfahren keine Hinweise zu dieser Formulierung entnommen werden, vgl. BT-Drs. 17/1543.

[3] Vgl. zum Begriff der Straftat im Rahmenbeschluss 2008/977/JI siehe bereits oben unter C. I. 1. a) dd)
(4).

**dd) Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit**

Übermittelte oder bereitgestellte Daten dürfen gemäß Art. 11 Satz 1 lit. c ferner zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit verwendet werden. Diese Begrifflichkeit ist den deutschen Gesetzen fremd, wird aber im Rahmen von EU-Handlungsformen offenbar durchgehend verwendet. Der Begriff findet sich z.B. auch in Art. 8 Abs. 3 Satz 2 des Rahmenschlusses 2006/960/JI (Schwedische Initiative) sowie in Art. 23 Abs. 1 lit. c EU-RhÜbk. Zu letztem findet sich in dem Erläuternden Bericht zum EU-RhÜbk der Hinweis, dass der Ausdruck der unmittelbaren und ernsthaften Gefahr nicht zu restriktiv ausgelegt werden dürfe; er gelte beispielsweise für Maßnahmen im Zusammenhang mit Straftaten, bei denen Menschenleben gefährdet würden, Drogendelikten oder anderen ähnlichen schwerwiegenden Fällen. In diesem Zusammenhang erinnert der Erläuternde Bericht auch an die Erklärung der Bundesrepublik Deutschland zu der Frage, inwieweit Daten, die von der Justiz in einem Mitgliedstaat erhoben worden sind, von den Polizeidiensten in einem anderen Mitgliedstaat zur Abwehr erheblicher Gefahren und für die künftige Bekämpfung erheblicher Straftaten verwendet werden können (vgl. Erläuternder Bericht zu dem Übereinkommen vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (2000/C 379/02), S. 26, 27f). Die vorstehenden Anmerkungen sprechen dafür, auch hier einen Gefahrenmaßstab anzuwenden, der im Verhältnis zur konkreten Gefahr qualifiziert ist. Der Bund verwendet bei der Umsetzung der Schwedischen Initiative, respektive des oben erwähnten Art. 8 Abs. 3 Rahmenbeschluss 2006/960/JI, denn auch die Formulierung „gegenwärtige und erhebliche Gefahr“ (vgl. § 92b des Gesetzes über die internationale Rechtshilfe in Strafsachen (IRG)-E im Entwurf eines Gesetzes über die Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, BR-Drs. 853/10) und knüpft damit sowohl an eine besondere zeitliche Nähe der Gefahrenverwirklichung und ein gesteigertes Maß der Wahrscheinlichkeit des Schadenseintritts als auch an die Schwere der Rechtsgutsverletzung an (vgl. zu den Begrifflichkeiten Schenke, Polizei- und Ordnungsrecht, 6. Auflage 2009, Rn. 78; Pieroth/Schlink/Kniesel, Polizei- und Ordnungsrecht, 6. Auflage 2009, Rn. 19). Weitgehend synonym dürfte auch der Begriff der unmittelbar bevorstehenden oder unmittelbar drohenden Gefahr verwendet werden können. Die Erheblichkeit kann sich zum einen aus dem betroffenem Rechtsgut, der Tatbegehung oder dem möglichen Ausmaß des Schadens ergeben (vgl. zu dem Begriff der Straftat von erheblicher Bedeutung, BVerfG, Urt. v. 12.03.2003 – 1 BvR 330/96, Juris, Rn. 84).

Auch für diese Verwendungsbeschränkung ist festzustellen, dass die Ländergesetze insoweit weiter gefasst sind, denn sie erlauben eine Zweckänderung regelhaft, wenn die Polizei die Daten zu diesem Zweck erheben dürfte (vgl. § 14 Abs. 1 Satz 2 HmbPolDVG, Art. 37 Abs. 2 S. 2 BY PAG, § 188 Abs. 1 S. 2 LVwG, § 37 Abs. 2 Satz 2 PolG BW, § 39 Abs. 1 Nds. SOG). Insoweit ist ein Umsetzungsbedarf zu bejahen.

**ee) Jeden anderen Zweck mit vorheriger Zustimmung des übermittelnden Mitgliedstaats oder mit Einwilligung der betroffenen Person**

Schließlich können die personenbezogenen Daten gemäß Art. 11 S. 1 lit. d für jeden anderen Zweck verarbeitet werden, sofern der übermittelnde Mitgliedstaat zuvor zugestimmt hat oder die betroffene Person, im Einklang mit dem innerstaatlichen Recht, ihre Einwilli-

gung erteilt hat. Die Modalitäten einer solchen Zustimmung bleiben den Mitgliedstaaten überlassen (vgl. Erwägungsgrund Nr. 20).
In den Polizeigesetzen findet sich keine Regelung, die eine weitere Verwendung von Daten von der Zustimmung des übermittelnden Staates abhängig macht. Ob eine solche Zustimmung auch ohne entsprechende gesetzliche Regelung geeignet ist, Verarbeitungsbeschränkungen zu überwinden, ist zweifelhaft. Die Zustimmung des übermittelnden Mitgliedstaats zur Zweckänderung kann zwar grundsätzlich wie eine erstmalige Datenübermittlung betrachtet und dem übermittelnden Staat eine entsprechende Verfügungsbefugnis zugestanden werden. Andererseits dürfte jedoch die Schwelle für eine Zweckänderung deutlich niedriger sein als für eine erstmalige Datenübermittlung, da es sich hier um Daten handelt, die dem Empfänger bereits bekannt sind und die auf Initiative des Empfängers hin zu weiteren Zwecken verwendet werden sollen. Es besteht daher ein gesteigertes Schutzbedürfnis des Betroffenen, das für eine ausdrückliche gesetzliche Regelung spricht. Wenn daher eine Zweckänderung mit Zustimmung des übermittelnden Mitgliedstaates für die Fälle ermöglicht werden soll, die nicht unter Art. 11 Satz 1 lit a - c fallen, empfiehlt sich eine ausdrückliche Regelung. Insoweit besteht Umsetzungsbedarf.

**ff) Zwischenergebnis und Formulierungsvorschlag**
Die Prüfung hat mithin ergeben, dass die Landespolizeigesetze eine Datenverarbeitung erlauben, die in Teilen weitgehender ist als die in Art. 11 Satz. 1 lit. a-c genannten Zwecke. Um den Vorgaben des Rahmenbeschlusses zu entsprechen, ist somit ein Umsetzungsbedarf zu bejahen.

Eine mögliche Formulierung könnte lauten:

> „Personenbezogene Daten, die von einer Behörde eines Mitgliedstaates der Europäischen Union übermittelt oder bereitgestellt wurden, darf die Polizei vorbehaltlich entgegenstehender gesetzlicher Verwendungsbeschränkungen nur für folgende andere Zwecke als diejenigen, für die sie übermittelt oder bereitgestellt wurden, verarbeiten:
> a) Die Verhütung oder Verfolgung von Straftaten oder Vollstreckung von strafrechtlichen Sanktionen,
> b) andere mit den Zwecken nach Buchstabe a) unmittelbar zusammenhängende justizielle und verwaltungsbehördliche Verfahren oder
> c) die Abwehr einer unmittelbar bevorstehenden und erheblichen Gefahr für die öffentliche Sicherheit.
> Für einen anderen Zweck dürfen sie nur mit vorheriger Zustimmung des übermittelnden Mitgliedstaates oder mit Einwilligung der betroffenen Person verwendet werden."

Dabei ist unschädlich, dass der Landesgesetzgeber bestimmt, ob Daten auch für Strafverfolgungsbehörden nutzbar sein sollen.[4]

Der Formulierungsvorschlag erfasst nur Daten, die von einem Mitgliedstaat der EU übermittelt wurden, nicht hingegen Daten von Behörden, die aufgrund des Vertrages über die Europäische Union oder des Vertrages über die Arbeitsweise der Europäischen Union errichtet worden sind. Dies entspricht dem Wortlaut des Art. 11 Satz 1 („zuständige Behörde *eines anderen Mitgliedstaates*"). Eine Anwendung der Legaldefinition des Begriffs „zuständige Behörde" aus Art. 2 lit. h, die auch Agenturen und Einrichtungen erfasst, die aufgrund des Vertrages über die Europäische Union errichtet worden sind, erscheint an-

[4] Vgl. Schenke, Polizei- und Ordnungsrecht, 6. Auflage, Rn. 31. Die Ermächtigung zur Nutzung dieser Daten für die Strafverfolgung ergibt sich wiederum nur aus dem Strafverfahrensrecht.

gesichts der in Art. 11 Satz 1 vorgenommenen Einschränkung nicht angebracht. Eine Umsetzung, die auch Daten von EU-Institutionen den Verwendungsbeschränkungen unterwirft, wäre aber wohl ebenfalls mit dem RB DS zu vereinbaren und hätte den Vorteil, dass eine übermäßige Ausdifferenzierung der Verwendungsregeln vermieden würde[5].

**b) Verwendung für historische, statistische oder wissenschaftliche Zwecke**
**aa) Historische, statistische oder wissenschaftliche Zwecke (Satz 2)**
Über die in Art. 11 Satz 1 genannten Zwecke hinaus dürfen die übermittelten personenbezogenen Daten durch die zuständigen Behörden für historische, statistische oder wissenschaftliche Zwecke weiter verarbeitet werden, sofern die Mitgliedstaaten geeignete Garantien vorsehen, wie z.B. die Anonymisierung der Daten. Art. 11 Satz 2 ist fast wortgleich eine Wiederholung von Art. 3 Abs. 2 Satz 2. Hinsichtlich des Begriffs „anonymisieren" findet sich in Art. 2 lit. k eine Definition. Danach ist „Anonymisieren" das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Definition entspricht der des § 3 Abs. 6 Bundesdatenschutzgesetz (BDSG) und der Landesgesetze.[6]

Die Ländergesetze enthalten bereits Regelungen zur Datenverwendung entsprechend des Art. 11 Satz 2. So z.B. in § 17 HmbPolDVG (vgl. auch § 37 Abs. 3 und 4 PolG BW, Art. 38 Abs. 5 BY PAG, § 38 Abs. 4, § 39 Abs. 7 Nds. SOG, § 188 Abs. 4 LVwG). Gemäß § 17 Abs. 1 HmbPolDVG darf die Polizei personenbezogene Daten auch über die nach anderen Vorschriften zulässige Speicherungsdauer hinaus zur Aus- und Fortbildung nutzen. Dabei ist sicherzustellen, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden können (Anonymisierung). Die Anonymisierung kann unterbleiben, wenn diese nicht mit vertretbarem Aufwand möglich ist oder dem Aus- und Fortbildungszweck entgegensteht und jeweils die schutzwürdigen Belange des Betroffenen nicht offensichtlich überwiegen. Gemäß § 17 Abs. 2 PolDVG darf die Polizei gespeicherte personenbezogene Daten zu statistischen Zwecken nutzen; dabei sind die Daten zum frühestmöglichen Zeitpunkt zu anonymisieren. Eine Veröffentlichung ist nur zulässig, wenn kein Rückschluss auf die Verhältnisse einer natürlichen Person möglich ist.

Eine Verwendung für die Aus- und Fortbildung, wie sie in den oben stehend zitierten Polizeigesetzen vorgesehen ist, kann als Verarbeitung für wissenschaftliche Zwecke im Sinne des Art. 11 Satz 2 verstanden werden. Zwar unterscheidet das BDSG zwischen dem Zweck der Ausbildung und dem der wissenschaftlichen Forschung (vgl. z.B. § 14 Abs. 2 u. 3 BDSG). Die Aus- und Fortbildung kann aber im Kontext des Rahmenbeschlusses durchaus als ein Unterfall der wissenschaftlichen Verwendung verstanden werden. Dafür spricht, dass der Begriff der Wissenschaft gemeinhin auch als Oberbegriff verstanden

[5] Vgl. dazu bereits oben unter C. I. 1. a) cc).
[6] Im Wesentlichen gleichlautend sind: § 4 Abs. 9 HmbDSG, Art. 4 Abs. 8 BayDSG, § 2 Abs. 2 Nr. 6 LDSG Schleswig-Holstein, § 3 Abs. 6 Gesetz zum Schutz personenbezogener Daten Baden-Württemberg. Das niedersächsische Landesrecht verwendet den Begriff der Anonymisierung im Zusammenhang mit der Nutzung personenbezogener Daten in § 38 Abs. 4, § 39 Abs. 7 Nds. SOG, sieht jedoch weder in diesem noch im NDSG eine Begriffsbestimmung vor. Zur Auslegung dürfte aber ergänzend auf das BDSG verwiesen werden können.

wird, der aus Forschung und Lehre besteht (vgl. auch BVerfGE 35, 79, 113), wobei die Aus- und Fortbildung zu Letzterem gezählt werden kann.

**bb) Geeignete Garantien**
Ferner sieht Art. 11 Satz 2 vor, dass eine Verwendung für historische, statistische oder wissenschaftliche Zwecke von geeigneten Garantien abhängig zu machen ist. Die Vorsehung geeigneter Garantien dürfte sich nach dem Sinn und Zweck der Regelung auf den Schutz personenbezogener Daten beziehen. D.h. die Verwendung für historische, statistische oder wissenschaftliche Zwecke wird unter die Bedingung gestellt, dass Verfahrensweisen existieren, die einen Schutz personenbezogener Daten gewährleisten. Zur Veranschaulichung nennt der Rahmenbeschluss in Art. 11 Satz 2 ein Beispiel für eine solche mögliche Verfahrensweise, nämlich die der Anonymisierung. Sie kann daher als eine mögliche Garantie zum Schutz personenbezogener Daten im Sinne des Art. 11 Satz 2 angesehen werden. Aus dieser nur exemplarischen Nennung folgt zugleich, dass andere Verfahrensweisen ebenso geeignet sein können. Soweit daher – wie in allen zitierten Landesgesetzen - eine Einschränkung vom Erfordernis der Anonymisierung vorgesehen ist, folgt daraus nicht zwangsläufig ein Widerspruch zu den Vorgaben des Art. 11 Satz 2. Denn indem bspw. der Nichtanonymisierung eine Abwägung mit den Belangen des Betroffenen vorangestellt wird, dürfte gleichwohl noch eine hinreichende Garantie im Sinne des Art. 11 Satz 2 angenommen werden können.

Soweit demnach die Landesgesetze eine Verwendung zu den in Art. 11 Satz 2 genannten Zwecken vorsehen und zugleich beispielsweise eine Anonymisierung - wenn auch unter bestimmten Voraussetzungen - vorsehen, dürfte dies mithin mit den Vorgaben des Art. 11 Satz 2 im Einklang stehen. Ein Umsetzungsbedarf besteht dann nicht.

**10. <u>Artikel 12 – Wahrung von innerstaatlichen Verarbeitungsbeschränkungen</u>**
Art. 12 enthält Regelungen zur Wahrung von Verarbeitungsbeschränkungen, die nach dem innerstaatlichen Recht des übermittelnden Mitgliedstaats gelten, durch den empfangenden Mitgliedstaat.

**a) Hinweis auf und Einhaltung von Verarbeitungsbeschränkungen (Abs. 1)**
Gelten nach dem innerstaatlichen Recht des übermittelnden Mitgliedsstaats unter besonderen Umständen besondere Verarbeitungsbeschränkungen für den Datenaustausch zwischen den zuständigen Behörden innerhalb dieses Mitgliedstaats, so weist die übermittelnde Behörde den Empfänger auf diese besonderen Beschränkungen hin (vgl. Art. 12 Abs. 1 Satz 1). Der Empfänger stellt sicher, dass diese Verarbeitungsbeschränkungen eingehalten werden (vgl. Art. 12 Abs. 1 Satz 2). Daraus folgt zum einen die Möglichkeit, Verarbeitungsbeschränkungen vorzugeben und zum anderen die Verpflichtung, solche einzuhalten, wenn sie von einem anderen Mitgliedstaat vorgeben werden.
Nicht recht deutlich wird, was unter „besonderen Umständen“ und „besonderen Verarbeitungsbeschränkungen“ zu verstehen ist. Zum einen dürfte dies als Abgrenzung zu Art. 9 zu verstehen sein, der vorsieht, dass die übermittelnde Behörde die Einhaltung von nach innerstaatlichem Recht bestehenden Lösch- und Prüffristen vorgeben kann. Danach sind unter „besonderen Verarbeitungsbeschränkungen“ über die Einhaltung von Löschungs- und Prüffristen hinausgehende Beschränkungen zu verstehen, denn andernfalls hätte Art.

12 Abs. 1 keinen eigenen Regelungsgehalt. Im Falle der Annahme eines Umsetzungsbedarfes erscheint es daher zweckmäßig, Art. 12 Abs. 1 und Art. 9 im Zusammenhang zu regeln. Zum anderen dürfte die Bezeichnung „besondere Verarbeitungsbeschränkungen“ in Art. 12 Abs. 1 auch als eine mögliche Einschränkung zu Art. 11 zu verstehen sein, wonach eine Verwendung personenbezogener Daten, die von der zuständigen Behörde eines anderen Mitgliedstaates übermittelt oder bereitgestellt wurden, (grundsätzlich) für die in Art. 11 Satz 1 lit. a - c bezeichneten anderen Zwecke verwendet werden dürfen. Art. 12 dient damit der Gewährleistung von innerstaatlichen Verarbeitungsbeschränkungen, die durch Art. 11 ggfs. ein Stück weit zurückgenommen werden könnten. Art. 11 ist damit die Regel und Art. 12 die Ausnahme. Dies wird auch bei Berücksichtigung von Erwägungsgrund Nr. 6 deutlich. Danach sollte der Rahmenbeschluss es den Mitgliedstaaten überlassen, auf nationaler Ebene näher zu bestimmen, welche anderen Zwecke als unvereinbar mit dem Zweck gelten, für die die personenbezogenen Daten ursprünglich erhoben wurden.
Besondere gesetzliche Verarbeitungsbeschränkungen gelten z.B. für Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (§ 18 Abs. 3 HmbPolDVG, § 41 Abs. 2 S. 3 PolG BW, Art. 39 Abs. 3 BY PAG, § 191 Abs. 2 LVwG, § 39 Abs. 1 Satz 3 Nds. SOG) oder mit besonderen Mitteln und Methoden erhoben worden sind (vgl. § 14 Abs. 2 HmbPolDVG, § 39 Abs. 2 S. 2 Nds. SOG, Art. 34 c Abs. 4 S. 2 BY PAG, § 23 Abs. 7 PolG BW, § 185 Abs. 6 LVwG).

**b) Maßstab innerstaatlicher Datenübermittlungen (Abs. 2)**

Bei der Anwendung von Art. 12 Abs. 1 wenden die Mitgliedstaaten gemäß Art. 12 Abs. 2 für Datenübermittlungen an andere Mitgliedstaaten oder an nach Titel VI des Vertrages über die Europäische Union errichtete Agenturen oder Einrichtungen nur solche Beschränkungen an, die auch für innerstaatliche Datenübermittlungen gelten. D.h., die Vorgabe von Bearbeitungsbeschränkungen im Sinne des Art. 12 Abs. 1 ist nur zulässig, wenn derartige Reglementierungen auch bei der innerstaatlichen Übermittlung gelten. Das hier zum Ausdruck kommende Diskriminierungsverbot oder Gleichstellungsgebot lag auch der Schwedischen Initiative zugrunde. Sofern sich dies nicht bereits aus der landesrechtlichen Umsetzung der Schwedischen Initiative ergibt, erscheint es angezeigt, bei einer Implementierung von Art. 12 Abs. 1 vorzusehen, dass nur auf die Einhaltung solcher Verwendungsbeschränkungen hingewiesen werden kann, die auch bei innerstaatlichen Datenübermittlungen gelten. Ein mögliches Umsetzungsbeispiel ergibt sich aus den Anwendungshinweisen vom 13.01.2011 des Bundesministeriums des Innern zum BKAG, Satz 3. Dort heißt es, dass

> das Bundeskriminalamt den Empfänger auf besondere bundesgesetzliche Verwendungsbeschränkungen für den Datenaustausch hinweist, sofern diese auch im innerstaatlichen Bereich Anwendung finden.

**c) Vergleichbare Regelungen**

Die Bindung an Verarbeitungsbeschränkungen ist nicht neu. Sie findet sich auch in Art. 8 Abs. 4 Rahmenbeschluss 2006/960/JI sowie in Art. 7 Abs. 2, 3 EU-RhÜbk. Gemäß Art. 7 Abs. 2 und 3 EU-RhÜbk kann die übermittelnde Behörde nach Maßgabe ihres innerstaatlichen Rechts Bedingungen für die Verwendung der Informationen durch die empfangende Behörde festlegen, an welche diese gebunden ist. Für Art. 7 Abs. 2 und 3 EU-RhÜbk

findet sich die bundesgesetzliche Umsetzung in § 61 a IRG sowie § 92 Abs. 2 IRG, der auf § 61 a IRG Bezug nimmt. § 61 a Abs. 2 IRG lautet:

> „Die Übermittlung ist mit der Bedingung zu verbinden, dass
> a) nach dem deutschen Recht geltende Löschungs- oder Löschungsprüffristen einzuhalten sind,
> b) die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt worden sind, und
> c) die übermittelten Daten im Falle einer Unterrichtung nach Absatz 4 unverzüglich zu löschen oder zu berichtigen sind."

Nach Art. 8 Abs. 4 Satz 1 Rahmenbeschluss 2006/960/JI kann die übermittelnde Strafverfolgungsbehörde Bedingungen für die Verwendung der Informationen und Erkenntnisse festlegen, die durch die empfangende Strafverfolgungsbehörde zu beachten sind. Die Umsetzung im Bundesrecht soll in § 92b S. 3 IRG-E, § 27 a Abs. 1 Satz 3 BKAG-E sowie in § 33a Abs. 1 Satz 3 BPolG-E Berücksichtigung finden (vgl. Entwurf eines Gesetzes über die Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, BR-Drs. 853/10). Diese Regelungen lauten gleichlautend:

> „Von dem übermittelnden Staat für die Verwendung der Daten gestellte Bedingungen sind zu beachten."

**d) Umsetzungsbedarf**

Soweit es um die Zweckbindung als besondere Verarbeitungsbeschränkung geht, findet Art. 12 Abs. 1 Satz 1 für den Fall der Übermittlung von personenbezogenen Daten an einen anderen Mitgliedstaat z.B. in § 18 Abs. 5 HmbPolDVG (vgl. auch § 43 Abs. 3 Satz 3 PolG BW, Art. 39 Abs. 2 Satz 2 BY PAG, § 193 Abs. 3 S. 2 LVwG) eine Entsprechung. Gemäß § 18 Abs. 5 HmbPolDVG darf der Empfänger die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck nutzen, zu dem sie ihm übermittelt worden sind. Ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie Personen und Stellen außerhalb des öffentlichen Bereichs sind bei der Datenübermittlung darauf hinzuweisen. Darüber hinaus ist in den Polizeigesetzen nicht ersichtlich, dass dem empfangenden Mitgliedstaat besondere Verarbeitungsbeschränkungen vorgegeben werden können bzw. von einem anderen Mitgliedstaat solche Beschränkungen erteilt werden, deren Einhaltung sicher zu stellen wäre.
Eine Anpassung der Polizeigesetze erscheint zweckmäßig, soweit es um die Beachtung von Vorgaben eines anderen übermittelnden Mitgliedstaates[7] sowie darum geht, als übermittelnde Behörde auf besondere Verarbeitungsbeschränkungen hinzuweisen. Letzteres auch im Interesse einer möglichst grundrechtsfreundlichen Umsetzung (vgl. BVerfG, Urt. v. 18.07.2005, NJW 2005, 2289). Dabei ist – für den Fall des Verweises auf Zweckbindungen – nicht ausgeschlossen, dass sich durch die Vorgabe von Verarbeitungsbeschränkungen eine gewisse Einschränkung von Art. 11 ergibt. Dies entspricht dem Art. 11 und 12 zugrundeliegende Regel-Ausnahmeverhältnis.[8]
Eine mögliche Formulierung könnte lauten:

---

[7] Die Projektgruppe Umsetzungsbedarf Ratsbeschluss Prüm und Schwedische Initiative kam in ihrem Bericht zum Umsetzungsbedarf des ähnlich lautenden Art. 8 Abs. 4 der Schwedischen Initiative zu dem Ergebnis, dass es zweckmäßig ist, die Beachtung von Vorgaben eines übermittelnden Mitgliedstaates, umzusetzen (vgl. Anlage 2: Umsetzungsbedarf Schwedische Initiative, S. 23).
[8] Siehe dazu bereits oben unter Nr. 10 lit. a.

„Sofern die Polizei personenbezogene Daten an einen Mitgliedstaat der Europäischen Union oder an Behörden, die aufgrund des Vertrages über die Europäische Union oder des Vertrages über die Arbeitsweise der Europäischen Union errichtet worden sind, übermittelt oder bereitstellt, hat sie auf besondere Verwendungsbeschränkungen hinzuweisen, sofern diese auch im innerstaatlichen Recht Anwendung finden. Von dem übermittelnden Staat für die Verwendung der Daten mitgeteilte Beschränkungen sind zu beachten."

## 11. Artikel 13 – Weiterleitung an die zuständige Behörde in Drittstaaten oder an internationale Einrichtungen

Artikel 13 hat die Weiterleitung von Daten an Drittstaaten oder an internationale Einrichtungen zum Gegenstand. Drittstaaten im Sinne des EU Rechtes sind Staaten, die nicht Vertragspartei/ Mitgliedstaat sind. Für die vom Anwendungsbereich des Rahmenbeschlusses erfassten Schengen-assoziierten Staaten gilt Art. 13 nicht.

### a) Weiterleitung mit Zustimmung des übermittelnden Staates (Abs. 1)

Abs. 1 enthält vier Zweck beschränkende Bedingungen (kumulativ) für die Weiterleitung von personenbezogenen Daten an Drittstaaten oder internationale Einrichtungen, die von einer zuständigen Behörde eines anderen Mitgliedstaates übermittelt oder bereitgestellt wurden.

#### aa) Erforderlich zur Verhütung oder Ermittlung, Feststellung, Verfolgung von Straftaten oder zur Strafvollstreckung

Die Weiterleitung der Daten muss zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Strafvollstreckung erforderlich sein. Die Polizeigesetze der Länder differenzieren bei einer Übermittlung von Daten an ausländische öffentliche Stellen zwischen der Übermittlung zur Erfüllung von Aufgaben des Übermittlers bzw. des Empfängers mit unterschiedlichen gesetzlichen Anforderungen; z.B. § 193 Abs. 2 LVwG SH, § 43 Abs. 2 Nr. 2 Nds. SOG, § 20 Abs. 3 PolDVG HH, Art. 40 Abs. 5 PAG BY, § 43 Abs. 3 Satz 1 PolG BW), wonach personenbezogene Daten an ausländische Stellen übermittelt werden können, sofern dies erforderlich ist

- zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr durch die übermittelnde Stelle,
- zur Abwehr einer im einzelnen Falle bevorstehenden erheblichen Gefahr durch den Empfänger.

Der RB DS enthält keine unterschiedlichen Anforderungen für „Übermittleraufgaben" bzw „Empfängeraufgaben" und ermöglicht eine Datenweiterleitung im Rahmen der Gesetzgebungskompetenz der Länder zur straftatenbezogenen Gefahrenabwehr.

Die ausgewerteten Polizeigesetze der Länder ermöglichen eine Datenübermittlung auch zu anderen Zwecken. Umsetzungsbedarf für die Weiterleitung von Daten i.S.d. Art. 13 besteht daher insoweit, als eine Zweckbeschränkung auf die straftatenbezogenen Gefahrenabwehrerfolgen muss.

**bb) Empfangende Stelle zuständig für Verhütung oder Verfolgung von Straftaten oder zur Strafvollstreckung**

Eine weitere Voraussetzung für eine Datenweiterleitung ist die Notwendigkeit, dass die empfangende Stelle für die Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen zuständig ist. Die Polizeigesetze der Länder erwähnen die Zuständigkeit der empfangenden Stelle nicht direkt, setzen diese jedoch voraus, weil die Übermittlung von personenbezogenen Daten zur Abwehr einer erheblichen Gefahr durch den Empfänger möglich ist. Umsetzungsbedarf besteht insoweit nicht (Nds. SOG § 43 Abs. 2 Nr. 2, PolDVG HH § 20 Abs. 3, PAG BY Art. 40 Abs. 5, PolG BW § 43 Abs. 3, LVwG SH § 193 Abs. 2).

**cc) Zustimmung des Herkunfts-Mitgliedstaates**

Personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übermittelt oder bereitgestellt wurden, dürfen grundsätzlich an Drittstaaten nur weitergeleitet werden, wenn der übermittelnde Mitgliedstaat einer Weiterleitung (entweder allgemein oder im Einzelfall) unter Beachtung seines innerstaatlichen Rechts zugestimmt hat. Jeder Mitgliedstaat sollte Modalitäten für diese Zustimmung (allgemeine Zustimmung für Kategorien von Informationen oder für bestimmte Drittstaaten) festlegen. Für ausgehende Daten muss dies nicht unbedingt durch Gesetz erfolgen, da durch den RB DS auch die Empfänger der Daten an die Beschränkungen des Art. 13 gebunden sind, so dass die Erteilung der Zustimmung eher von praktische Erwägungen abhängig sein wird als von rechtlichen.

Ein Zustimmungserfordernis des „Erstübermittlers“ zur Weiterleitung an Drittstaaten ist in keinem Landesrecht geregelt, insofern besteht in den Polizeigesetzen der Länder Umsetzungsbedarf.

**dd) Angemessenes Datenschutzniveau beim Empfänger**

Eine Datenweiterleitung setzt schließlich ein angemessenes Datenschutzniveau im Empfängerland voraus. Kriterien für eine Bewertung des Datenschutzniveaus enthält Abs. 4. Die Anforderungen sind in Abhängigkeit der Art der Daten, Zweckbestimmung, der Dauer der geplanten Verarbeitung, der Empfänger, die beim Empfänger geltenden Rechtsnormen sowie der dort geltenden Standesregeln und Sicherheitsmaßnahmen u. s. w. festzulegen.

Eine vergleichbare Regelung – wenn auch ohne Einzelheiten zu den maßgeblichen Kriterien – findet sich z.B. in § 43 Abs. 4 Nds. SOG. Teileweise enthalten die Polizeigesetze der Länder jedoch keine Bestimmungen über ein angemessenes Datenschutzniveau im Empfängerland. Die Anwendbarkeit von Regelungen aus den Landesdatenschutzgesetzen ist in den Ländern unterschiedlich ausgestaltet. Das BayPAG schließt z.B. bestimmte Regelungsbereiche des Bayerischen Datenschutzgesetzes in Artikel 49 aus. Demnach kann Art. 21 Abs. 2 BayDSG, der bei einer Datenübermittlung ein angemessenes Datenschutzniveau voraussetzt, nicht zur Anwendung kommen. Demgegenüber schließt das LVwG SH die Anwendbarkeit des LDSG nicht aus, sodass § 3 LDSH SH (Anwendbarkeit des LDSG bei fehlenden spezialgesetzlichen Regelungen) zur Anwendung kommt.

Sofern ein Rückgriff auf die Datenschutzgesetze der Länder nicht möglich ist und die Forderung nach einem angemessenen Datenschutzniveau nicht aus allgemeinen Übermittlungsvoraussetzungen abzuleiten ist, wäre eine Anwendbarkeitserklärung für den Regelungsbereich – Datenschutzniveau – aus den Landesdatenschutzgesetzen zu prüfen.

Bei der notwendigen Bewertung des Datenschutzniveaus (Abs. 4) ist zu beachten, dass der Übermittler nicht in jedem Fall alle notwendigen Faktoren (Standesregeln und Sicherheitsmaßnahmen im Drittstaat, allgemeine oder sektorielle Rechtsnormen im Drittstatt oder in einer internationalen Einrichtung) bewerten kann. Eine explizite Nennung der Bewertungskriterien erscheint jedoch entbehrlich; da sie sich aus allgemeinen Angemessenheitsüberlegungen ableiten lassen. Gesetzgeberischer Umsetzungsbedarf besteht insofern nicht. Es erscheint allerdings sinnvoll in Verwaltungsregelungen, die Zuständigkeit und das Verfahren für die Feststellung der Angemessenheit des im Drittstaat vorhandenen Datenschutzniveaus zu regeln.

**b) Weiterleitung ohne vorherige Zustimmung (Abs. 2)**

Abs. 2 enthält eine Sonderregelung, die eine Durchbrechung der kumulativen Bedingungen für den Regelungsgehalt des Abs. 1 lit. c (Zustimmungserfordernis) ermöglicht.
Eine Weiterleitung ohne vorherige Zustimmung ist möglich, wenn die Weiterleitung der Daten zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaates oder eines Drittstaates oder für die wesentlichen Interessen eines Mitgliedstaates unerlässlich ist und die Zustimmung nicht rechtzeitig eingeholt werden kann. Zum Gefahrengrad siehe die Erläuterungen zu Art 11 Satz 1 lit. c.
Nach einer Datenweiterleitung ohne Zustimmung besteht die Verpflichtung zur unverzüglichen Unterrichtung der für eine Zustimmungserteilung zuständigen Behörde.
Entsprechende Regelungen sind in den Landesgesetzen nicht vorhanden. Insoweit besteht daher Umsetzungsbedarf.

**c) Weiterleitung bei Fehlen eines angemessenen Datenschutzniveaus (Abs. 3)**

Abs. 3 enthält zwei Alternativen, die eine Weiterleitung von personenbezogenen Daten ermöglichen, obwohl das durch Abs. 1 lit. d geforderte angemessenes Schutzniveau für die Datenverarbeitung beim Empfänger nicht nachgewiesen ist. Danach ist eine Weiterleitung auch zulässig, wenn

- Regelungen im innerstaatlichen Recht des Übermittlers dies vorsehen
  - wegen überwiegender schutzwürdiger Interessen der betroffenen Person oder
  - überwiegender berechtigter Interessen, insbesondere wichtiger öffentlicher Interessen,

  oder
- der Empfänger Garantien bietet, die vom betreffenden Mitgliedstaat für angemessen befunden werden.

Eine mit den Voraussetzungen des ersten Spiegelstrichs vergleichbare Regelung findet sich z.B. in § 43 Abs. 4 Satz 2 Nds. SOG. Auch die Datenschutzgesetze der Länder enthalten zum Teil vergleichbare Vorschriften; in den Polizeigesetzen der Länder fehlen jedoch teilweise direkt korrespondierende Vorschriften. Ähnlich wie bereits zu Abs. 1 lit. d ausgeführt, besteht eine unterschiedlich ausgestaltete Möglichkeit des „Rückgriffs“ auf die Datenschutzgesetze der Länder. Sofern Landesdatenschutzgesetze nicht anwendbar sind und die in Abs. 3 genannten („Ersatz“) Kriterien für eine Datenweiterleitung ohne ein nachgewiesenes angemessenes Datenschutzniveau nicht aus allgemeinen Übermittlungsvoraussetzungen abgeleitet werden können, wäre eine Anwendbarkeitserklärung aus den Landesdatenschutzgesetzen zu prüfen.

**d) Formulierungsvorschlag**

Für die aufgezeigten fehlenden Regelungen in den Polizeigesetzen der Länder nachfolgender Formulierungsvorschlag, der aus Gründen der Übersichtlichkeit in Form einer separaten Regelung erfolgt; gegebenenfalls bietet sich auch die Aufnahme in bestehende Vorschriften an.

> **„Zustimmung zur Weiterleitung an Behörden in Drittstaaten oder an internationale Einrichtungen**
>
> (1) Personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates der EU übermittelt oder bereitgestellt wurden, darf die Polizei nur mit Zustimmung der zuständigen Behörde dieses Staates zur Verhütung von Straftaten an eine Behörde in einem Drittstaat oder eine internationale Einrichtung weiterleiten.
>
> (2) Die Weiterleitung ist nur zulässig, wenn der Drittstaat oder die internationale Einrichtung ein für die beabsichtige Datenverarbeitung angemessenes Schutzniveau gewährleistet. Sofern dieses Schutzniveau nicht nachgewiesen ist, dürfen personenbezogene Daten weitergeleitet werden, soweit dies aufgrund von überwiegenden schutzwürdigen Interessen der betroffenen Person oder überwiegender öffentlicher Interessen erforderlich ist oder der Drittstaat oder die empfangende internationale Stelle im Einzelfall angemessene Garantien bietet.
>
> (3) Ohne vorherige Zustimmung der übermittelnden Behörde ist eine Weiterleitung zulässig, wenn dies zur Abwehr einer unmittelbar bevorstehenden und erheblichen Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittstaats oder zur Wahrung wesentlicher Interessen eines Mitgliedstaats unerlässlich ist und die vorherige Zustimmung nicht rechtzeitig eingeholt werden kann. Die für die Erteilung der Zustimmung zuständige Behörde ist unverzüglich zu unterrichten.“

## 12. Artikel 14 – Übermittlung von Daten an nicht-öffentliche Stellen in Mitgliedstaaten

Art. 14 hat die Übermittlung von Daten, die von einer Behörde eines anderen Mitgliedstaates übermittelt bzw bereitgestellt wurden, an nicht-öffentliche Stellen in Mitgliedstaaten zum Gegenstand. Eine Weiterleitung ist nur an nicht-öffentliche Stellen in Mitgliedstaaten möglich, dabei ist es unerheblich, ob diese Stelle im eigenen Staat oder in einem anderen Mitgliedstaat angesiedelt ist. Eine Definition von nicht-öffentlichen Stellen ist § 2 BDSG zu entnehmen.
Die Regelung schließt eine Weiterleitung von personenbezogenen Daten an nicht-öffentliche Stellen in Drittstaaten aus.

Abs. 1 enthält in den Buchstaben a bis c kumulativ geltende Bedingungen für die Weiterleitung an nicht öffentliche Stellen. Es wird nicht unterschieden, ob die Übermittlung an eine nicht-öffentliche Stelle aufgrund einer Anfrage oder eigener Bewertung der Polizei geschieht.

### a) Zustimmungserfordernis

Nach Buchst. a muss die zuständige Behörde des Mitgliedstaates, übermittelt er die Daten erhalten hat, einer Weiterleitung zustimmen. Ausnahmen vom Zustimmungserfordernis sind nicht möglich. Die Erteilung der Zustimmung ist wie in Artikel 13 RB DS an keine formalen Regelungen gebunden, sodass sowohl einzelfallbezogene als auch generelle Weiterleitungsgenehmigungen erteilt werden können. Für ausgehende Daten ist festzule-

gen, nach welchen Kriterien durch wen eine Weiterleitungsgenehmigung erteilt werden kann; einer gesetzlichen Regelung bedarf es nicht[9].
Umsetzungsbedarf in den Polizeigesetzen der Länder besteht für die Bindung an die Zustimmung des Übermittlers bei aus dem Ausland empfangenen Daten.

**b) Kein Entgegenstehen überwiegender Interessen**
Überwiegende schutzwürdige Interessen des Betroffenen dürfen nach Buchst. b einer Datenweiterleitung nicht entgegenstehen. Die Ausgestaltung in den Polizeigesetzen der Länder ist heterogen: ausformulierte Verpflichtung die schützwürdigen Interessen Einzelner zu wahren (§ 44 PolG BW), möglicher Rückgriff auf Regelungen im Landesdatenschutzgesetz (§ 15 LDSG SH) oder die allgemeinen Verhältnismäßigkeitsgrundsätze bieten für die schutzwürdigen Interessen Einzelner ausreichende Garantien. Ein Umsetzungsbedarf besteht nicht.

**c) Übermittlungszwecke**
Die Zwecke, zu denen eine Übermittlung an nichtöffentliche Stellen erfolgen darf, sind in Buchst. c geregelt. Zulässig ist eine Übermittlung danach

- zur Erfüllung eigener Aufgaben der übermittelnden Stelle,
- zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung von strafrechtlichen Sanktionen. Der Anwendungsbereich beschränkt sich für die Polizeigesetze auf die straftatenbezogene Gefahrenabwehr (siehe Ausführungen zu Anwendungsbereich des RB DS)
- zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit (siehe Ausführungen zu Art. 11) oder
- zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner.

Unklar ist dabei der Regelungsgehalt des ersten Spiegelstrichs, der die Übermittlung zur Erfüllung eigener Aufgaben der übermittelnden Stelle ermöglicht. Dem Wortlaut nach enthält dieser Spiegelstrich kaum eine Begrenzung der Übermittlungsbefugnis und würde die folgenden, wesentlich engeren Regelungen zum Übermittlungszweck überflüssig machen. Denkbar ist, dass der Spiegelstrich im Lichte der Bestimmungen über die Zweckbindung und -änderung des RB DS auszulegen ist und die Übermittlung nur zu Zwecken erlaubt, zu denen die Behörde die Daten selbst verarbeiten darf. Insbesondere wären dann die Beschränkungen des Art. 11 zu beachten. Auch bei dieser Auslegung wären die Übermittlungszwecke des Art. 14 nicht widerspruchsfrei, da sich dann auch bei den anderen Spiegelstrichen die Frage nach ihrem Verhältnis zu den Reglungen in Art. 11 stellen würde. Die Arbeitsgruppe rät daher von einer Umsetzung des ersten Spiegelstrichs ab.

Die Regelungen in den Polizeigesetzen der Länder sind unterschiedlich. Teilweise wird eine Datenübermittlung an nicht-öffentliche Stellen nur zur Abwehr einer Gefahr ermöglicht (§ 44 Nds. SOG, § 193 LVwG SH); nach anderen Gesetzen darf sie auch zur Aufgabenwahrnehmung der übermittelnden Behörde, im Interesse des Empfängers oder bei Bestehen berechtigter öffentlicher oder privater Interessen erfolgen (§ 44 PolG BW, Art. 41 BY PAG, § 21 HmbPolDVG).

[9] s.o. Ziff. 11 lit. a) cc) zu Art. 13.

Sofern Landesgesetzgeber, die eine Datenübermittlung an nicht-öffentliche Stellen nur zur Abwehr einer Gefahr zulassen, die geltenden engen Übermittlungsregelungen beibehalten wollen, besteht Umsetzungsbedarf dahingehend, dass die weitergehenden Beschränkungen des Art 14 RB DS übernommen werden müssen. Eine Datenweiterleitung an nicht-öffentliche Stellen wäre unter den in Buchst. a und b genannten Voraussetzungen zur
- Abwehr einer straftatenbezogenen Gefahr und
- Abwehr einer gegenwärtigen und erheblichen sonstigen Gefahr
möglich.

Die Länder, denen der Gesetzgeber eine weit gefasste Möglichkeit der Datenübermittlung an nicht öffentlichen Stellen eingeräumt hat, können entsprechend den Regelungen in Art. 14 Abs. 1 lit. c RB DS weitergehende Übermittlungszwecke aufnehmen und die Datenübermittlung je nach Rechtslage zusätzlich zur
- Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner oder
- zur Erfüllung eigener Aufgaben der übermittelnden Stelle
zulassen.

Der bestehende Umsetzungsbedarf kann systemisch unterschiedlich gelöst werden. Entweder schafft der Landesgesetzgeber eine eigene Regelung für die Datenweiterleitung von aus Mitgliedstaaten erhaltenen Daten (siehe nachfolgender Vorschlag) oder ergänzt bestehende Übermittlungsbefugnisse an Private um Ausnahmeregelungen.

**d) Verpflichtung, Daten mit Zweckbindung zu versehen**

In Abs. 2 ist geregelt, dass die zuständige Behörde, die die Daten an eine nicht-öffentliche Stelle weiterleitet, dies mit einer Zweckbindung des Empfängers an den Übermittlungszweck verbinden muss. Umsetzungsbedarf besteht insoweit nicht, da in den Gesetzen der Länder bereits entsprechende Regelungen bestehen (siehe Ausführungen zu Art. 12 Abs.1 RB DS).

**e) Formulierungsvorschlag**

> **„Übermittlung von Daten an nicht-öffentliche Stellen in Mitgliedstaaten**
> Personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaats der EU übermittelt oder bereitgestellt wurden, darf die Polizei mit Zustimmung der zuständigen Behörde dieses Staates an nicht-öffentliche Stellen in den Mitgliedstaaten nur übermittelt werden, wenn überwiegende schutzwürdige Interessen der betroffenen Person nicht entgegenstehen und die Übermittlung im Einzelfall unerlässlich ist
> 1. zur Verhütung von Straftaten,
> 2. zur Abwehr einer unmittelbar bevorstehenden und erheblichen Gefahr für die öffentliche Sicherheit oder
> 3. zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner.“

**13. <u>Artikel 15 – Unterrichtung auf Antrag der zuständigen Behörde</u>**

Artikel 15 enthält ein Informationsrecht (auf Ersuchen) des Übermittlers darüber, wie personenbezogene Daten beim Empfänger verarbeitet worden sind. Die Kennzeichnung von übermittelten oder abgerufenen personenbezogenen Daten ist Voraussetzung für die Gewährleistung des Informationsrechtes des Übermittlers. Dem Übermittler ist über die Ver-

arbeitung (definiert in Artikel 2 Nr. b RB DS) der Daten Auskunft zu geben. Anders als bei der Umsetzung des Art. 8 Abs. 4 S. 5 des RB 2006/960/JI des Rates vom 18. Dezember 2006 (RB Schwedische Initiative) erscheint eine Beschränkung der Auskunftsmöglichkeit des Übermittlers auf Zwecke der Datenschutzkontrolle nicht angezeigt, da der RB DS keinerlei Voraussetzungen für ein Ersuchen des Übermittlers regelt.
Die Polizeigesetze der Länder enthalten keine Auskunftsrechte des Übermittlers. Ein Umsetzungsbedarf dürfte bestehen, ob als selbständige Lösung (vgl. den Gesetzentwurf der Bundesregierung zur Umsetzung des RB SWI mit Blick z.B. auf § 33a PolG-E, BR-Drs. 853/10) oder als Ergänzung bestehender Auskunftspflichten ist durch Landesgesetzgeber zu entscheiden.

Ein Auskunftsrecht des Übermittlers könnte wie folgt formuliert werden:

> „Die Polizei unterrichtet die Stelle, die Daten übermittelt hat, auf Ersuchen über die Verarbeitung der Daten."

Durch die systematische Einordnung oder durch ausdrückliche Formulierung kann die Regelung auf den Anwendungsbereich des RB DS beschränkt werden.

## 14. Artikel 16 – Information der betroffenen Person

### a) Information des Betroffenen im Einklang mit dem innerstaatlichen Recht (Abs. 1)

Nach Art. 16 Abs. 1 haben die Mitgliedstaaten zu gewährleisten, dass der Betroffene „im Einklang mit dem innerstaatlichen Recht" über die Erhebung oder Verarbeitung personenbezogener Daten durch die zuständigen Behörden informiert wird.

Die Vorschrift enthält ein Gleichstellungsgebot, wonach bestehende Regelungen zur Benachrichtigung gegenüber Betroffenen in gleicher Weise wie bei der innerstaatlichen Datenerhebung oder -verarbeitung auch bei Datenerhebungen oder -verarbeitungen mit mitgliedstaatlichem Bezug zu gelten haben. Mit der Formulierung „im Einklang mit dem innerstaatlichen Recht" macht der Rahmenbeschluss deutlich, dass die Informationspflicht vom Bestehen innerstaatlichen Rechts abhängig ist. Daher sind insoweit keine speziellen Regelungen zur Umsetzung erforderlich. Vor diesem Hintergrund ist es auch unschädlich, dass die Bestimmung weithin auch Konstellationen erfasst, die keinen zwischenstaatlichen Bezug aufweisen und nach hier vertretener Auffassung (s.o.) gar nicht in den Regelungsbereich des Rahmenbeschlusses fallen (vgl. auch Erwägungsgrund 7 des Rahmenbeschlusses).
Ein Blick in die Polizeigesetze der Länder zeigt, dass es zum gesicherten Datenschutzstandard im Bereich der polizeilichen Datenerhebung gehört, dass eine Unterrichtungspflicht des Betroffenen (nur) bei heimlichen, eingriffsintensiven Maßnahmen gegeben ist. Selbst in diesem Bereich werden umfangreiche Ausnahmetatbestände normiert.

### b) Unterlassen der Information auf Ersuchen des übermittelnden Mitgliedstaats (Abs. 2)

Nach Abs. 2 Satz 1 kann der die Daten übermittelnde Mitgliedstaat den Empfangsmitgliedstaat „nach Maßgabe seines innerstaatlichen Rechts" darum ersuchen, dass dieser den Betroffenen von der Datenübermittlung nicht informiert.

Eine solche Regelung fehlt bislang in den Polizeigesetzen der Länder. Ein zwingender Umsetzungsbedarf besteht allerdings nicht, da die Vorschrift an Regelungen in den Mitgliedstaaten anknüpft, aber keine Verpflichtung statuiert, unabhängig hiervon entsprechende Regelungen erst zu schaffen.

Gleichwohl dürfte es sich zu Zwecken der Gefahrenabwehr und ggf. auch der Strafverfolgung empfehlen, insoweit eine (klarstellende) Befugnisnorm in das jeweilige Landespolizeigesetz einzufügen. Denn es liegt im Interesse der Polizei, sicherzustellen, dass gegenüber dem Betroffenen geheimhaltungsbedürftige Informationen aus ermittlungstaktischen Gründen (zunächst) auch geheim bleiben. Zu denken ist insbesondere an Fälle, in denen zwar im Inland keine Benachrichtigungspflicht besteht, in einem anderen Mitgliedstaat aber doch. Eine Regelung könnte etwa wie folgt aussehen:

> „Die Polizei kann den die Daten empfangenden Mitgliedstaat darum ersuchen, den Betroffenen ohne vorherige Zustimmung der Polizei von der Übermittlung der Daten nicht zu informieren, sofern nach diesem Gesetz oder anderen Rechtsvorschriften eine Verpflichtung zur Benachrichtigung des Betroffenen über die Erhebung oder Verarbeitung seiner personenbezogenen Daten nicht besteht."

In Abs. 2 Satz 2 ist bestimmt, dass bei Ersuchen nach Satz 1 der Empfangsmitgliedstaat den Betroffenen nicht ohne (vorherige) Zustimmung des Übermittlungsmitgliedstaats informiert.

In den Polizeigesetzen der Länder fehlt es an Bestimmungen, die die Beachtung entsprechender Vorgaben statuieren. Es ist allerdings zweifelhaft, ob insoweit Umsetzungsbedarf besteht, nachdem in den Landespolizeigesetzen Pflichten zur Mitteilung von Amts wegen an verdeckte Ermittlungsmaßnahmen anknüpfen, nicht aber an die Übermittlung von Daten aus anderen Mitgliedstaaten.

Sofern eine Umsetzung befürwortet wird, könnte eine Regelung etwa wie folgt aussehen:

> „Hat die übermittelnde Stelle eines Mitgliedstaats darum ersucht, die Benachrichtigung des Betroffenen von ihrer Zustimmung abhängig zu machen, ist dies zu beachten."

Durch die systematische Einbindung oder ausdrückliche Formulierung kann die Regelung auf den Anwendungsbereich des RB DS beschränkt werden.

Zu beachten ist, dass die in Art. 16 Abs. 2 Satz 1 angeordnete Bindung – wie aus der systematischen Stellung der Vorschrift abgeleitet werden kann – nur die Fälle betrifft, in denen gesetzlich festgelegte Informationspflichten von Amts wegen zu erfüllen ist. Einschränkungen für das in Art. 17 statuierte Recht auf Auskunft können daraus nicht resultieren. Insoweit enthält der Rahmenbeschluss in Art. 17 Absatz 2 vorrangige Regelungen.

## 15. Artikel 17 – Recht auf Auskunft

### a) Auskunftsrecht (Abs. 1)

In Abs. 1 ist zunächst vorgesehen, dass eine Auskunft an den Betroffenen zu in angemessenen Abständen gestellte Ersuchen frei und ungehindert und ohne unzumutbare Verzögerungen oder übermäßig hohe Kosten erfolgen muss.

Die Polizei- bzw. Datenschutzgesetze und das Verwaltungsverfahrensrecht der Länder entsprechen diesen Vorgaben bereits. Umsetzungsbedarf besteht insoweit nicht.

Zum Umfang der Auskunft enthält die Bestimmung zwei Alternativen, in der die Mindestanforderungen an die Auskunft beschrieben werden:
Entweder muss dem Betroffenen von dem für die Verarbeitung Verantwortlichen oder von der nationalen Kontrollstelle bestätigt werden, ob ihn betreffende Daten übermittelt worden sind, ggf. eine Information zum Empfänger der Daten sowie ferner eine Mitteilung über die Daten, die Gegenstand der Verarbeitung sind (lit. a), oder
dem Betroffenen muss von der nationalen Kontrollstelle bestätigt werden, dass alle erforderliche Überprüfungen durchgeführt worden sind (lit. b).

Sämtliche für die Polizei geltenden Datenschutzbestimmungen der Länder sehen ein Recht auf Auskunft vor. Der Umfang der Auskunftserteilung ist jedoch unterschiedlich. Während in einigen Landesbestimmungen (z.B. § 16 NDSG, § 45 PolG BW i.V.m. § 21 LDSG BW) weitgehende Auskunftspflichten statuiert sind, die den Vorgaben von Art. 17 Abs. 1 lit. a des Rahmenbeschlusses häufig bereits entsprechen, bleibt die Auskunftspflicht in anderen Ländern hinter diesen Vorgaben zurück. Dies betrifft in erster Linie die Auskunft dazu, ob und dass personenbezogene Daten des Empfängers übermittelt worden sind und zu der Frage des Empfängers. Bezogen auf Art. 17 Abs. 1 lit. a des Rahmenbeschlusses besteht insoweit abhängig von der jeweiligen Gesetzeslage Umsetzungsbedarf.
Mit Blick auf die Ausgestaltung des Auskunftsrechts in Deutschland (Geltendmachung der Auskunft gegenüber der speichernden Stelle) erscheint es nicht möglich, von der Alternative in Art. 17 Abs. 1 lit. b des Rahmenbeschlusses Gebrauch zu machen.
Zwar nimmt auch der Landesbeauftragte für den Datenschutz Überprüfungen im Sinne dieser Bestimmung vor. Dessen Anrufung setzt indes das Vorbringen voraus, dass die öffentliche Stelle Datenschutzbestimmungen verletzt hat. Ein solches Vorbringen ist dem Betroffenen mangels näherer Kenntnis des relevanten Sachverhalts regelmäßig nicht möglich. Im Übrigen hat der Landesbeauftragte für den Datenschutz auch nicht die Funktion einer allgemeinen Auskunftsstelle.

### b) Beschränkungen des Auskunftsrechts (Abs. 2)

Abs. 2 enthält die – auch am Verhältnismäßigkeitsgrundsatz zu messende – Möglichkeit gesetzlicher Beschränkungen des Auskunftsrechts nach Absatz 1 lit. a. Im Einzelnen werden fünf Fallgruppen aufgezählt, die sich inhaltlich teilweise überschneiden.

Die Ausgestaltung der Verweigerungsgründe ist in den Ländern im Einzelnen unterschiedlich. Zumeist dürften die landesrechtlichen Bestimmungen bereits rahmenbeschlusskonform sein. Dies gilt insbesondere für die Länder, in denen als Ausschlussgründe die Gefährdung der Aufgabenerfüllung, die Gefährdung der öffentlichen Sicherheit oder Ord-

nung, Nachteile für das Wohl des Bundes oder eines Landes sowie Geheimhaltungsbedürftigkeit angeführt sind (vgl. z.B. § 16 Abs. 3 NDSG, Art. 48 Abs. 2 PAG BY, § 21 Abs. 5 LDSG BW).

**c) Formvorschriften bei Versagung der Auskunft (Abs. 3)**

In Abs. 3 ist geregelt, dass eine - auch teilweise - Versagung der Auskunft schriftlich mitzuteilen und hierfür die Gründe anzugeben sind, es sei denn, es liegt ein Versagungsgrund nach Absatz 2 vor. In allen Fällen der – auch teilweisen – Versagung der Auskunft muss der Betroffene darauf hingewiesen werden, dass er bei der zuständigen nationalen Kontrollstelle, bei einer Justizbehörde oder vor Gericht Beschwerde einlegen kann.

Vorschriften in den Landesgesetzen, nach denen die Ablehnung der Auskunftserteilung, die ja nur auf der Basis rahmenbeschlusskonformer Versagungsgründe möglich ist, keiner Begründung bedarf (vgl. z.B. Art. 48 Abs. 3 Satz 1 PAG BY), stehen ebenso mit dem Rahmenbeschluss in Einklang wie enger gefasste landesrechtliche Vorschriften, die von einer Begründungspflicht nur dann dispensieren, wenn durch die Begründung der Zweck der Ablehnung gefährdet würde (vgl. z.B. § 16 Abs. 5 Satz 1 NDSG, § 18 Abs. 4 Satz 1 HmbDSG, § 21 Abs. 6 Satz 1 LDSG BW).
Nicht ganz unproblematisch ist allerdings, dass bei – auch teilweiser – Versagung der Auskunft Mitteilungen der Polizei schriftlich zu erfolgen haben, während die Landesgesetze jedenfalls überwiegend ein solches Erfordernis nicht ausdrücklich aufführen. Teilweise ist die Schriftform durch untergesetzliche Regelungen, etwa in polizeilichen Richtlinien, festgeschrieben. In diesen Fällen dürfte den Vorgaben des Rahmbeschlusses ausreichend Rechnung getragen sein. Fehlt es auch hieran, kann ggf. darauf hingewiesen werden, dass die Versagung der Auskunft durchweg, d.h. in ständiger Praxis, schriftlich erfolgt und vor diesem Hintergrund eine Regelung entbehrlich ist.

In den Landesgesetzen ist vorgesehen, dass bei Versagung der Auskunft der Betroffene darauf hinzuweisen ist, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann (vgl. § 16 Abs. 6 NDSG, § 18 Abs. 6 HmbDSG, § 21 Abs. 6 Satz 2 LDSG BW). Da es sich bei dem Landesbeauftragten für den Datenschutz um eine nationale Kontrollstelle im Sinne von Art. 17 Abs. 3 Satz 3 des Rahmenbeschlusses handelt und der Hinweis hinsichtlich einer Rechtsschutzmöglichkeit genügt, besteht insoweit kein Umsetzungsbedarf.

**16. <u>Artikel 18 – Recht auf Berichtigung, Löschung oder Sperrung</u>**

**a) Subjektives Recht**

In Art. 18 **Abs. 1 Satz 1** wird ein subjektives Recht des Betroffenen darauf statuiert, dass der für die Datenverarbeitung Verantwortliche den Pflichten des Rahmenbeschlusses zur Berichtigung, Löschung oder Sperrung nachkommt.

Die in den Landesgesetzen enthaltene Verpflichtung zur Berichtigung etc. (vgl. etwa Art. 45 Abs. 1 bis 3 PAG BY, § 46 PolG BW, § 24 HmbPolDVG) gibt dem Betroffenen zugleich einen entsprechenden Anspruch gegen die Polizei, so dass insoweit kein Umsetzungsbedarf besteht.

Nach **Satz 2** legen die Mitgliedstaaten fest, ob der Betroffene das Recht nach Satz 1 direkt gegenüber dem für die Verarbeitung Verantwortlichen oder über die zuständige nationale Kontrollstelle geltend machen kann.

Eine solche Festlegung wird in den landesrechtlichen Regelungen nicht ausdrücklich getroffen. Ansprüche auf Berichtigung, Löschung oder Sperrung kann der Betroffene direkt gegenüber der Polizei geltend machen. Daneben kann der Betroffene sich auch an den Landesbeauftragten für den Datenschutz mit dem Vorbringen wenden, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch die Polizei in seinen Rechten verletzt worden zu sein. Mit Blick hierauf erscheint es gut vertretbar, einen Umsetzungsbedarf zu verneinen.

Für die Fälle, in denen der für die Verarbeitung Verantwortliche den Antrag ablehnt, bestimmt **Satz 3**, dass dies der betroffenen Person schriftlich mitzuteilen und sie auf die nach innerstaatlichem Recht vorgesehenen Möglichkeiten einer Beschwerde oder eines Rechtsbehelfs hinzuweisen ist. Nach **Satz 4** muss der Betroffene über das Ergebnis einer durch Beschwerde oder Rechtsbehelf angestoßenen Überprüfung informiert werden. Dabei können die Mitgliedstaaten nach **Satz 5** auch vorsehen, dass dem Betroffenen durch die zuständige nationale Kontrollstelle mitgeteilt wird, dass eine Überprüfung stattgefunden hat.

Eine Verpflichtung zu einer schriftlichen Mitteilung entsprechend Satz 3 unter Hinweis auf eine Rechtsschutzmöglichkeit sehen die Landesgesetze bislang nicht vor. Sofern man die Ablehnung entsprechender Anträge als Verwaltungsakt auffasst[10], ergibt sich aus § 37 Abs. 2 Satz 2 VwVfG eine Verpflichtung zur Schriftform, die allerdings nur bei berechtigtem Interesse eingreift und von dem Betroffenen unverzüglich verlangt werden muss. Ob dies den Anforderungen des Rahmenbeschlusses genügt, ist fraglich. Ausreichend wäre aber möglicherweise eine ständige Verwaltungspraxis, die den Vorgaben des Art. 18 Satz 3 bereits entspricht. Hinsichtlich des erforderlichen Hinweises kommt dabei sowohl ein Hinweis auf die Rechtsschutzmöglichkeiten nach der Verwaltungsgerichtsordnung als auch – wie Satz 5 zeigt – ein Hinweis auf die Möglichkeit der Anrufung des Landesbeauftragten für den Datenschutz in Betracht.

Insbesondere aus Transparenzgründen liegt es nahe, zur Umsetzung eine ausdrückliche (neue) Regelung zu schaffen. Soweit die Berichtigung, Löschung und Sperrung von Daten in dem Polizeigesetz des Landes geregelt ist, könnte einer solchen Regelung z.B. folgender neuer Absatz angefügt werden (wobei zu überlegen ist, ob die Regelung nur für die Anwendungsfälle des Rahmenbeschlusses oder generell gelten soll):

> „Der Betroffene kann sein Recht auf Einhaltung der Pflichten nach Absatz x bis y der Polizei gegenüber geltend machen. Die Ablehnung eines solchen Antrags hat schriftlich zu erfolgen und ist mit einer Rechtsbehelfsbelehrung zu versehen."

Oder:

> „(...) und ist mit dem Hinweis zu versehen, dass der Betroffene sich an den Landesbeauftragten für den Datenschutz wenden kann."

[10] Gola/Schomerus, BDSG, § 20 Rn. 40. Vgl. zum ähnlich gelagerten Fall der Verweigerung der Auskunft nach § 19 BDSG auch Gola/Schomerus, BDSG, § 19, Rn. 31; Mallmann in: Simitis, BDSG, § 19, Rn. 55; a.A. BayVGH, NVwZ 1990, 775.

**b) Kennzeichnung bei Bestreiten**

Nach **Abs. 2** „kann“ die Kennzeichnung (zum Begriff s. Art. 2 lit. j) eines personenbezogenen Datums erfolgen, wenn dessen Richtigkeit von dem Betroffenen bestritten wird und die Richtigkeit nicht festgestellt werden kann.

Manche Landesgesetze enthalten insoweit zumindest ähnliche Regelungen, indem sie einen so genannten Sperrvermerk bei einem Bestreiten der Richtigkeit durch den Betroffenen vorsehen (z.B. § 17 Abs. 3 Satz 1 Nr. 1 NDSG, § 24 Abs. 1 S. 3 HmbPolDVG). In anderen Ländern fehlen derartige Bestimmungen. Da es sich bei Art. 18 Abs. 2 um eine „kann“-Regelung handelt, besteht kein zwingender Umsetzungsbedarf.

## 17. Artikel 19 – Recht auf Schadenersatz

Art. 19 enthält Regelungen zum Schadensersatz und Regress wegen rechtswidriger Datenverarbeitung. Für die ähnliche Vorschrift des Art. 31 RatsB Prüm hatte der Bericht „Umsetzungsbedarf Ratsbeschluss Prüm und Schwedische Initiative“ auf § 8 des Ausführungsgesetzes zum Prümer Vertrag (PrümVtrAG) verwiesen, der eine Schadensersatzpflicht des Bundes und einen Regressanspruch gegen das verantwortliche Bundesland regelt. Auf Grundlage der konkurrierenden Gesetzgebungskompetenz des Bundes für das Staatshaftungsrecht (Art. 74 Nr. 25 GG) wäre auch im Anwendungsbereich des RB DS eine Regelung durch den Bund denkbar. Entsprechende Pläne sind jedoch nicht bekannt; die Haftung für eine rechtswidrige Datenverarbeitung ist vielmehr in den Datenschutzgesetzen der Länder geregelt. Im Folgenden werden daher die Regelungserfordernisse bei einer Umsetzung durch Landesrecht dargestellt.

**a) Schadenersatz ohne Exkulpationsmöglichkeit**

Nach Abs. 19 **Abs. 1** muss bei Verletzung von Datenschutzvorschriften des Rahmenbeschlusses dem Betroffenen ein Anspruch auf Schadenersatz eingeräumt werden.

Nachdem die Landesgesetze (vgl. z.B. § 18 NDSG, Art. 14 DSG BY, § 25 LDSG BW, § 20 HmbPolDVG) Regelungen zum Schadenersatz bei Verletzung von Datenschutzvorschriften enthalten, die auch für das Handeln der Polizei gelten, und im Übrigen auch die Vorschriften der Staatshaftung nach Art. 34 GG i.V.m. § 839 BGB zur Anwendung kommen, ist ein Umsetzungsbedarf nicht gegeben.

In **Abs. 2 Satz 1** ist bestimmt, dass im Falle der Datenübermittlung durch einen anderen Mitgliedstaat der Empfänger sich im Rahmen seiner Haftung „nach Maßgabe des innerstaatlichen Rechts“ nicht darauf berufen kann, dass die übermittelten Daten unrichtig gewesen sind.

Die Norm regelt also den Ausschluss der Exkulpationsmöglichkeit in Fällen der Datenübermittlung durch andere Mitgliedstaaten. Die datenverarbeitende Stelle soll sich zu ihrer Entlastung nicht darauf berufen können, dass die verwendeten Daten bereits unrichtig durch einen Mitgliedstaat übermittelt worden sind. Eine Haftungshöchstgrenze fehlt. In den Landesgesetzen ist demgegenüber eine verschuldensunabhängige Haftung nur in Fällen der automatisierten Datenübermittlung realisiert (vgl. etwa Art. 14 Abs. 2 Satz 1

DSG BY, § 18 Abs. 1 Satz 1 NDSG) und hier auch höhenmäßig begrenzt (vgl. etwa Art. 14 Abs. 2 Satz 3 und 4 DSG BY, § 18 Abs. 1 Satz 3 NDSG).

Ob hier Umsetzungsbedarf besteht, könnte mit Blick darauf fraglich sein, dass nach dem Wortlaut der Bestimmung an die Maßgaben des innerstaatlichen Rechts angeknüpft wird und dieses eben keine vollumfängliche (verschuldensunabhängige und unbegrenzte) Haftung vorsieht. Verweise auf das nationale Recht sollen den Mitgliedstaaten entsprechend dem Subsidiaritätsgrundsatz regelmäßig soweit wie möglich Raum zur Anwendung des innerstaatlichen Rechts lassen. Für eine solche Sichtweise könnte auch sprechen, dass die Statuierung einer Gefährdungshaftung ohne gleichzeitige Bestimmung einer Haftungshöchstgrenze dem Recht grundsätzlich fremd ist (vgl. für Deutschland etwa Art. 14 Abs. 2 Satz 3 DSG BY, § 12 StVG, §§ 9, 10 HPflG, § 10 ProdHG, § 15 UmweltHG). Auch hatte die Projektgruppe, die den Umsetzungsbedarf des Ratsbeschlusses und der Schwedischen Initiative untersucht hatte, für die nahezu identische Regelung in Art. 31 Abs. 2 Satz 1 des Ratbeschlusses Prüm (2008/615/JI) ebenfalls keinen Umsetzungsbedarf gesehen.

Bezieht man die Worte „nach Maßgabe des innerstaatlichen Rechts“ dagegen nur auf die Regelung der näheren Modalitäten einer verschuldensunabhängigen und unbegrenzten Haftung für sämtliche Fälle der Übermittlung unrichtiger Daten, besteht Umsetzungsbedarf. Für eine solche Sichtweise könnte ins Feld geführt werden, dass die Regelung, die für den Betroffenen vor allem eine Verfahrenserleichterung bedeutet, nur einer Abmilderung von Risiken dient, die aus der transnationalen Übermittlung von Daten resultieren, und diesbezüglich keine sachgerechten Gründe für eine Differenzierung zwischen automatisierter und nicht-automatisierter Datenübermittlung bestehen.

Zu einem Umsetzungsvorschlag siehe unten.

**Abs. 2 Satz 2** regelt den Regress in den Fällen, in denen ein Mitgliedstaat unrichtige Daten übermittelt hat und der Empfänger dem Betroffenen wegen der Verwendung dieser unrichtigen Daten Schadenersatz leisten musste. Hier hat die übermittelnde zuständige Behörde dem Empfänger den Betrag des geleisteten Schadenersatzes abzüglich eines etwaigen Mitverschuldensanteils zu erstatten.

Ein Umsetzungsbedarf dürfte insoweit nicht bestehen. Der nationalen Regelung eines in europäischen Rechtsakten vorgesehenen Regressanspruchs gegenüber einem anderen Mitgliedstaat kann allenfalls deklaratorische Bedeutung zugemessen werden. Gleichwohl kann eine Regelung zumindest aus Transparenzgründen sinnvoll sein.

**b) Umsetzungsvorschlag**

Eine Regelung zur Umsetzung des Art. 19 Abs. 2 könnte (bei Bejahung des Umsetzungsbedarfs) unter Anknüpfung an eine im jeweiligen Landesdatenschutzgesetz geregelte Schadenersatzpflicht z.B. wie folgt lauten:

> „§ ... des (Landes-)Datenschutzgesetzes findet in den Fällen, in denen die zu verarbeitenden personenbezogenen Daten zuvor von einer Behörde eines Mitgliedstaats der Europäischen Union im Anwendungsbereich des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 übermittelt wurden, mit der Maßgabe Anwendung, dass sich die Poli-

> zei gegenüber dem Betroffenen zu ihrer Entlastung nicht darauf berufen kann, dass die übermittelten Daten unrichtig gewesen sind. Leistet die Polizei nach § ... des Landesdatenschutzgesetzes Ersatz wegen eines Schadens, der durch die Verarbeitung unrichtiger Daten verursacht wurde, so macht sie diesen unter Berücksichtigung etwaigen Mitverschuldens gegenüber der zuständigen Stelle des Mitgliedstaates zum Ausgleich geltend. Auf Aufforderung eines Mitgliedstaates erstattet die Polizei nach den Grundsätzen der Sätze 1 und 2 Schadenersatz, den ein Mitgliedstaat infolge der Verarbeitung durch die Polizei unrichtig übermittelter Daten erbringen musste."

### 18. Artikel 20 – Rechtsbehelfe

Hiernach muss der von der Datenverarbeitung betroffenen Person das Recht eingeräumt sein, bei Verletzung ihrer innerstaatlich garantierten Rechte bei Gericht Rechtsbehelfe einzulegen.

Ein Umsetzungsbedarf ruft diese Bestimmung nicht hervor. Art. 19 Abs. 4 GG gewährleistet ausreichenden Rechtsschutz in Deutschland. So können Datenschutzverstöße bei der polizeilichen Datenverarbeitung im Wege verwaltungsrechtsrechtlicher Rechtsbehelfe, insbesondere in Gestalt einer Feststellungs- oder Verpflichtungsklage, geltend gemacht werden (vgl. auch § 40 VwGO).

### 19. Artikel 21 – Vertraulichkeit der Verarbeitung

Diese Bestimmung will die Vertraulichkeit der Verarbeitung sichern, indem bestimmt wird, dass die Verarbeitung personenbezogener Daten grundsätzlich nur durch Angehörige oder auf Weisung der zuständigen Behörde handelnde Personen erfolgen darf. Für letztere gelten dann sämtliche Datenschutzbestimmungen der jeweils zuständigen Behörde.

Das nationale Recht sieht zahlreiche Bestimmungen vor, die die Vertraulichkeit der Verarbeitung, insbesondere den Schutz vor Kenntniserlangung durch Unbefugte, und die Verantwortlichkeit als speichernde Stelle (z.B. bei Datenverarbeitung im Auftrag, vgl. Art. 6 DSG BY, § 7 Abs. 1 LDSG BW) sichern und damit den Anforderungen von Art. 21 Genüge tun. Zu nennen sind etwa die Vorschriften über die dienstliche Verschwiegenheitspflicht (z.B. § 37 BeamtStG), die entsprechende strafrechtliche Absicherung (z.B. § 203 Abs. 2, § 353b StGB, Art. 37 DSG BY §§ 41, 6 LDSG BW) sowie untergesetzliche Dienstvorschriften, wie etwa Regelungen zum Schutz der Vertraulichkeit und zur Begrenzung der Datenzugriffsbefugnisse in den Richtlinien für die Führung polizeilicher personenbezogener Sammlungen.

### 20. Artikel 22 – Sicherheit der Verarbeitung

#### a) Technische und organisatorische Maßnahmen

In **Abs. 1 und 2** ist bestimmt, dass die Mitgliedstaaten dafür Sorge zu tragen haben, dass die zuständigen Behörden zur Sicherheit der Verarbeitung geeignete technische und organisatorische Maßnahmen ergreifen. Für die automatisierte Datenverarbeitung werden diese Anforderungen in Absatz 2 in zehn Punkten näher konkretisiert.

Die Gesetzeslage in den Ländern dürfte diesen Vorgaben wohl zumeist entsprechen. Da die bisherige landesrechtliche Ausgestaltung der Bestimmungen zu den technischen und

organisatorischen Maßnahmen im Einzelnen jedoch unterschiedlich ist, lassen sich pauschale Aussagen ohne Blick auf die individuelle Rechtslage nicht treffen. Nicht stets, wo es an ausdrücklichen Regelungen fehlt, besteht jedoch ein Normierungsbedarf. Dies gilt etwa für die Verpflichtung nach Art. 22 Abs. 2 lit. i des Rahmenbeschlusses, wonach die Wiederherstellung eingesetzter Systeme im Störungsfall gewährleistet werden muss. Hier wird man im Falle fehlender gesetzlicher Regelungen (vgl. z.B. § 7 Abs. 2 NDSG, Art. 7 Abs. 2 DSG BY, § 9 LDSG BW) argumentieren können, dass es sich um einen allgemeinen technischen Standard handelt. Gleiches dürfte hinsichtlich der Gewährleistung der Zuverlässigkeit und Datenintegrität nach Art. 22 Abs. 2 lit. j des Rahmenbeschlusses zu gelten haben. Die Vorgaben in Art. 22 Abs. 2 lit. i und lit. j leiten sich insbesondere aus dem Bereich des IT-Grundschutzes (Sicherheit) ab und liegen im ureigensten Interesse der jeweils verantwortlichen Stellen.

**b) Auftragsdatenverarbeitung**

**Abs. 3 und 4** betreffen die Auftragsdatenverarbeitung. Hiernach dürfen nur solche Stellen mit der Auftragsdatenverarbeitung betraut werden, die die erforderlichen technischen und organisatorischen Maßnahmen nach Absatz 1 treffen und Weisungen beachten, was von der zuständigen Stelle zu überwachen ist. Die Auftragsdatenverarbeitung muss dabei auf der Grundlage eines Rechtsakts oder eines schriftlichen Vertrages erfolgen.

Ein Umsetzungsbedarf dürfte jedenfalls regelmäßig nicht bestehen. Die Auftragsdatenverarbeitung ist in den Ländern im Einzelnen allerdings nicht ganz einheitlich geregelt, so dass die Übereinstimmung der landesrechtlichen Regeln mit den Vorgaben des Rahmenbeschlusses jeweils individuell zu prüfen ist. In den Ländern wird die beauftragte Stelle auf die Einhaltung der Datenschutzbestimmungen verpflichtet (vgl. z.B. § 3 Abs. 1 Satz 1 HmbDSG, § 6 Abs. 1 Satz 1 NDSG, Art. 6 Abs. 1 Satz 1 DSG BY, § 7 Abs. 2 Satz 4 LDSG BW). Aus dem Auftragsverhältnis folgt auch ein Weisungsrecht, was in den Ländern zumeist näher gesetzlich ausgeführt wird (vgl. z.B. § 3 Abs. 2 HmbDSG, § 6 Abs. 2 NDSG, Art. 6 Abs. 3 DSG BY, § 7 Abs. 3 Satz 2, 3 LDSG BW). In teilweise unterschiedlichen Formulierungen ist bestimmt, dass Auftragnehmer die Gewähr für die Einhaltung der technischen und organisatorischen Maßnahmen bieten müssen bzw. mit Blick hierauf sorgfältig auszuwählen sind (vgl. z.B. § 3 Abs. 1 Satz 2 und 3 HmbDSG, § 6 Abs. 3 Satz 1 NDSG, Art. 6 Abs. 2 Satz 1 PAG BY, § 7 Abs. 2 Satz 1, 2 LDSG BW). Teilweise wird auch ausdrücklich aufgeführt, dass sich der Auftragnehmer hiervon zu überzeugen hat (vgl. z.B. Art. 6 Abs. 3 Satz 2 DSG BY, § 7 Abs. 2 Satz 6 LDSG BW) und der Auftrag schriftlich zu erteilen ist (vgl. z.B. Art. 6 Abs. 2 Satz 2 DSG BY, § 7 Abs. 2 Satz 3 LDSG BW).

## 21. Artikel 23 – Vorabkonsultation

Nach Art. 23 haben die Mitgliedstaaten zu gewährleisten, dass die nationalen Kontrollstellen vor der Verarbeitung personenbezogener Daten in neu zu errichtenden Dateien konsultiert werden, wenn besondere Kategorien von Daten nach Artikel 6 verarbeitet werden (lit. a) oder die Art der Verarbeitung, etwa mit Blick auf neue Technologien, spezifische Risiken für die Grundrechte und Grundfreiheiten des Betroffenen birgt (lit. b).

Ziel der Vorschrift ist es, die nationalen Kontrollstellen bei besonders grundrechtsrelevanter Datenverarbeitung frühzeitig im Wege einer Konsultation zu beteiligen. Dabei bezieht

sich die Konsultation auf die Verarbeitung einer unbestimmten Vielzahl personenbezogener Daten in neu einzurichtenden Dateien, sie ist also nicht bezogen auf Einzelfälle. Die Vorschrift geht dem Wortlaut nach weit über den eigentlichen Anwendungsbereich des Rahmenbeschlusses hinaus.

Ob Umsetzungsbedarf besteht, hängt von den einzelnen landesrechtlichen Vorschriften ab, die auch in diesem Bereich nicht einheitlich sind. Die Unterrichtung des Landesbeauftragten für den Datenschutz erstreckt sich weithin auf automatisierte Verfahren. Beispielsweise ist in Art. 47 PAG BY geregelt, dass der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, einer Errichtungsanordnung bedarf, die auch dem Landesbeauftragten für den Datenschutz mitzuteilen ist. Hierdurch wird ihm die Möglichkeit der Einflussnahme noch vor der endgültigen Verwirklichung des Vorhabens gegeben und ihm die nötigen Informationen für seine Kontrolltätigkeit verschafft (vgl. Berner/Köhler/Käß, Polizeiaufgabengesetz [Bayern], 20. Aufl. 2010, Art. 47 Rn. 3). Darüber hinaus haben in Bayern Staatskanzlei und Staatsministerien den Landesbeauftragten für den Datenschutz über „Planungen bedeutsamer Automatisationsvorhaben“ zu unterrichten, sofern diese die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betreffen (vgl. Art. 32 Abs. 3 DSG BY).

In anderen Bundesländern ist keine allgemeine Konsultationspflicht des Landesbeauftragten für den Datenschutz statuiert oder es ist zumindest nicht geregelt, dass eine Beteiligung des Landesbeauftragten vor Inbetriebnahme des jeweiligen Verfahrens zu erfolgen hat (§ 22 Abs. 5 NDSG). Vielmehr wird vorgesehen, dass die Vorabkontrolle vorrangig dem behördlichen Datenschutzbeauftragten zur Prüfung zugeleitet wird, während der Landesbeauftragte für den Datenschutz „nur“ zur Unterstützung in Zweifelsfällen hinzugezogen wird oder subsidiär, wenn kein behördlicher Datenschutzbeauftragter bestellt ist, das Ergebnis der Vorabkontrolle erhält (vgl. § 12 S. 2, 3 LDSG BW).
Gegenüber dem 2005 in den Bundesrat eingebrachten Rahmenbeschluss-Vorschlag (Art. 26) enthält die jetzige Fassung keine Beteiligung des behördlichen Datenschutzbeauftragten mehr, der im Zweifel den Landesbeauftragten für den Datenschutz beteiligt. Damals hatte die - hier wegen Übersetzungsfehlern wiedergegebene englischsprachige Fassung - noch folgenden Wortlaut gehabt: „Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller by the data protection official, who, in case of doubt, must consult the supervisory authority.”
Für die Länder, die bislang eine Konsultation des Landesbeauftragte für den Datenschutz nicht in allen Fällen oder nicht zwingend vor Beginn der Datenverarbeitung vorsehen, ist daher ein Umsetzungsbedarf zu bejahen. Eine Umsetzungsregelung im Polizei- bzw. Sicherheits- und Ordnungsgesetz könnte unter Verweis auf die jeweilige landesdatenschutzrechtliche Vorabkontroll-Regelung z.B. wie folgt lauten:

> „§ ... des (Landes-)Datenschutzgesetzes ist mit der Maßgabe anzuwenden, dass der Landesbeauftragte für den Datenschutz stets vor Beginn der Datenverarbeitung angehört wird.“

Fraglich ist, was hinsichtlich nicht-automatisierter Verarbeitungen gilt, soweit in den Gesetzen der Länder nicht auch hierfür ausdrückliche Regelungen vorhanden sind (vgl. z.B. § 46 Nds. SOG i.V.m. §§ 8, 22 Abs. 5 Nr. 2 NDSG). Auch mit Blick auf den Regelungsumfang des Rahmenbeschlusses, der sich - auch bezogen auf Art. 23 - nur auf die Fälle

erstrecken kann, in denen die zu verarbeitenden personenbezogenen Daten zuvor von einer Behörde eines Mitgliedstaats im Anwendungsbereich des Rahmenbeschlusses übermittelt worden sind, könnte ggf. argumentiert werden, dass es in der Praxis bei der Verarbeitung dieser Daten „in neu zu errichtenden Dateien“ heutzutage keine Fälle mehr gibt, in denen eine solche Verarbeitung nicht automatisiert erfolgt. Hält man dagegen eine Regelung für erforderlich, so könnte z.B. eine Umsetzungsregelung im Polizeirecht unter Verweis auf die für automatisierte Verarbeitungen (Vorabkontrolle) geltende landesdatenschutzrechtliche Regelung (vgl. auf Bundesebene § 4d Abs. 5 BDSG), etwa nach folgendem Beispiel, erfolgen:

> „Bei neu zu errichtenden Dateien ist § ... des (Landes-)Datenschutzgesetzes in Fällen, in denen die zu verarbeitenden personenbezogenen Daten zuvor von einer Behörde eines Mitgliedstaats der Europäischen Union im Anwendungsbereich des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 übermittelt wurden, entsprechend auf nicht-automatisierte Verarbeitungen anzuwenden.“

### 22. Artikel 24 – Sanktionen

Hiernach haben die Mitgliedstaaten für die ordnungsgemäße Anwendung der Vorschriften des Rahmenbeschlusses Sorge zu tragen. Dazu müssen sie insbesondere wirksame, angemessene und abschreckende Sanktionen festlegen, die bei Verstößen gegen die Vorschriften zur Umsetzung des Rahmenbeschlusses zu verhängen sind.

Es ist davon auszugehen, dass in sämtlichen Datenschutzgesetzen der Länder, die für den Polizeibereich subsidiär gelten (vgl. etwa für Bayern Art. 49 PAG), Regelungen zu Straftaten und Ordnungswidrigkeiten vorhanden sind, die Verstöße auch bei der polizeilichen Datenverarbeitung ausreichend sanktionieren (vgl. etwa §§ 28, 29 NDSG, §§ 32, 33 HmbDSG, Art. 37 DSG BY, §§ 40, 41 LDSG BW). Ein Umsetzungsbedarf besteht daher nicht.

### 23. Artikel 25 – Nationale Kontrollstellen

Hier ist vorgesehen, dass die Mitgliedstaaten öffentliche Stellen vorhalten müssen, die hinsichtlich der Anwendung und Einhaltung der der Umsetzung des Rahmenbeschlusses dienenden innerstaatlichen Vorschriften beratend und überwachend tätig sind (**Abs. 1**), die ferner über Untersuchungs- und wirksame Einwirkungsbefugnisse sowie ein Klage- oder Anzeigerecht bei festgestellten Verstößen verfügen müssen (**Abs. 2**). Dem Betroffenen muss ein Anrufungsrecht gegenüber einer solchen Stelle eingeräumt sein (**Abs. 3**). Die Bediensteten dieser Stelle müssen den behördlichen Datenschutzregeln unterliegen und auch nach ihrem Ausscheiden der Verschwiegenheitspflicht unterliegen (**Abs. 4**).

In den geltenden gesetzlichen Bestimmungen wird entsprechenden Vorgaben bereits Rechnung getragen. Die Datenschutzgesetze der Länder haben als eine solche unabhängige nationale Kontrollstelle den Landesbeauftragten für den Datenschutz vorgesehen. Dieser überwacht bei öffentlichen Stellen die Einhaltung der Vorschriften über den Datenschutz und kann auch beratend tätig werden (vgl. z.B. Art. 30 DSG BY, § 31 LDSG BW). Er besitzt Untersuchungsbefugnisse i.S.d. Art. 25 Abs. 2 lit. a in Gestalt von Auskunft-, Vorlegungs- und Zutrittsrechten (vgl. z.B. Art. 32 DSG BY, § 29 LDSG BW) sowie

wirksame Einwirkungsbefugnisse i.S.d. Art. 25 Abs. 2 lit. b, indem er Verstöße beanstanden und ihre Behebung verlangen (vgl. z.B. Art. 31 DSG BY, § 30 LDSG BW). Das Erfordernis einer Anzeigebefugnis nach Art. 25 Abs. 2 lit. c wird durch die bestehenden Regelungen des allgemeinen Datenschutzrechts, z.B. Art. 37 Abs. 3 Satz 3 DSG BY, § 28 Abs. 4 LDSG BW (Antragsbefugnis des Landesbeauftragten für den Datenschutz bei datenschutzrechtlichen Straftaten; daneben Anzeigebefugnis bei datenschutzrechtlichen Ordnungswidrigkeiten), erfüllt.
Darüber hinaus gewähren die Datenschutzgesetze jedermann das Recht, den Landesbeauftragten für den Datenschutz anzurufen (vgl. z.B. Art. 9 DSG BY, § 27 LDSG BW). Der Datenschutzbeauftragte und seine Bediensteten unterliegen auch Verschwiegenheits- und sonstigen behördlichen Datenschutzregeln.

**24. Artikel 26 – Beziehung zu Übereinkünften mit Drittstaaten**

Art. 26 bestimmt in Satz 1, dass bestehende bi- und/oder multilaterale Übereinkünfte mit Drittstaaten (zu EU-Rechtsakten siehe Art. 28) durch den Rahmenbeschluss unberührt bleiben. Ein Umsetzungsbedarf besteht insoweit nicht.

In Satz 2 ist einschränkend festgelegt, dass auch bei Anwendung dieser Übereinkünfte die Weiterleitung personenbezogener Daten, die von einem anderen Mitgliedstaat erhalten worden sind, an einen Drittstaat nur unter den Voraussetzungen von Art. 13 Abs. 1 lit. c oder ggf. Art. 13 Abs. 2 des Rahmenbeschlusses erfolgen darf. Hintergrund dieser Vorschrift ist das Anliegen einiger Mitgliedstaaten, dass keine der Straftatenverhütung oder Strafverfolgung dienenden Daten, die an einen anderen Mitgliedstaat übermittelt werden, ohne Zustimmung oder (ausnahmsweise) jedenfalls Kenntnis des Ursprungsmitgliedstaats an einen Drittstaat weitergeleitet werden sollen.
Ein zwingender Umsetzungsbedarf dürfte insoweit nicht bestehen, nachdem die Vorschrift des Art. 13 ohnehin umgesetzt werden muss (s.o.) und die entsprechende nationale Bestimmung dann für die spezifische Konstellation, dass personenbezogene Daten, die aus anderen Mitgliedstaaten erlangt sind, an Drittstaaten übermittelt werden sollen, eine Spezialregelung auch für Übereinkünfte mit Drittstaaten darstellt, soweit diese eine entsprechende Weiterleitung überhaupt zulassen. In der Gesetzesbegründung zur landesrechtlichen Umsetzung des Art. 13 kann dies unter Verweis auf Art. 26 Satz 1 ggf. auch noch mal klargestellt werden.

**25. Artikel 27 – Evaluierung**

Die Regelungen zur Evaluierung in Art. 27 sind nicht umsetzungsbedürftig.

**26. Artikel 28 – Beziehung zu bereits früher angenommenen EU-Rechtsakten**

Hier ist bestimmt, dass bereits bestehende EU-Rechtsakte, die den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen betreffen und den mitgliedstaatlichen Datenaustausch, auch hinsichtlich der Datenverwendung, regeln, Vorrang vor den in dem Rahmenbeschluss enthaltenen Verwendungsregelungen haben.

Diese Vorschrift ruft keinen Umsetzungsbedarf hervor. Der Vorrang spezifischer Datenverarbeitungsregelungen in bereits früher angenommenen Rechtsakten der EU ergibt sich bereits aus dem allgemeinen Grundsatz des „lex specialis“. Zu dem Verhältnis des Rahmenbeschlusses Datenschutz zu den Regelungen des Rahmenbeschlusses 2006/960/JI (Schwedische Initiative) und des Ratsbeschlusses Prüm (2008/615/JI) siehe im Einzelnen unten im Teil C.

## D. Verhältnis des RB Datenschutz zu den Regelungen des RB Schwedische Initiative und des Ratsbeschlusses Prüm

Neben dem Rahmenbeschluss Datenschutz betreffen auch der Beschluss 2008/615/JI des Rates vom 23.06.2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (Ratsbeschluss Prüm) und der Rahmenbeschluss 2006/960/JI des Rates vom 18.12.2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (Rahmenbeschluss Schwedische Initiative) den Regelungsbereich der Polizeigesetze der Länder. Der sich aus diesen Rechtsakten ergebende Umsetzungsbedarf wurde in dem Bericht „Umsetzungsbedarf Ratsbeschluss Prüm und Schwedische Initiative“, Stand: 05.01.2011, dargelegt. Während der Rahmenbeschluss Datenschutz die Verarbeitung von Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen ausgetauscht worden sind, beschränkt, enthalten der Ratsbeschluss Prüm und der Rahmenbeschluss Schwedische Initiative spezifische Rechtsgrundlagen für die Übermittlung von Daten in andere Mitgliedstaaten der EU. Für die in ihrem Anwendungsbereich zu übermittelnden Daten enthalten sie jedoch auch Vorschriften zum Datenschutz, die nicht in jeder Hinsicht mit den Regelungen des RB DS übereinstimmen. Das Verhältnis dieser Vorschriften zueinander ist daher zu klären.
Die im Ratsbeschluss Prüm und im Rahmenbeschluss Schwedische Initiative geregelten Übermittlungsbefugnisse bleiben unberührt und sind nicht Gegenstand der folgenden Betrachtung.

### I. Artikel 28 RB Datenschutz

Maßgeblich ist Art. 28 RB DS, nach dem „spezifische Bestimmungen über die Verwendung von Daten durch den Empfängermitgliedstaat“ in früher angenommenen Rechtsakten Vorrang vor den Regelungen des RB DS haben. Sowohl der RB Schwedische Initiative als auch der Ratsbeschluss Prüm sind vor dem RB DS angenommen worden. Der Begriff der Verwendung ist im Rahmenbeschluss nicht definiert. In Erwägungsgrund 40 ist von „Verwendung und Weiterleiten“ die Rede. Auch wenn in Art. 28 gerade nicht der in Art. 2 Buchst. b definierte umfassende Begriff der Datenverarbeitung benutzt wird, dürfte „Verwendung“ neben Vorschriften zur Zweckbestimmung und zur Übermittlung von Daten auch Löschfristen und die Bindung an Bedingungen der übermittelnden Stelle umfassen, da solche Bestimmungen auch die Möglichkeiten der Datennutzung unmittelbar regeln.

Nach Erwägungsgrund 39 sollen früher erlassene Rechtakte unberührt bleiben, wenn sie ein umfassendes Datenschutzregime regeln („ein vollständiges, in sich geschlossenes Regelwerk, das alle relevanten Datenschutzaspekte … erfasst“) oder einen direkten Zugriff auf bestimmte Datensysteme ermöglichen. Der in Erwägungsgrund 39 geforderte Vorrang für früher erlassene umfassende Datenschutzvorschriften ist im RB DS nicht ausdrücklich geregelt worden; Art. 28 RB DS erfasst lediglich die Regelungen über die Verwendung von aus dem Ausland empfangenen Daten. Der Vorrang ergibt sich jedoch aus dem Spezialitätsgrundsatz. Bei den in Erwägungsgrund 39 beschriebenen umfassenden Datenschutzvorschriften handelt es sich um im Verhältnis zum RB DS speziellere Regelungen.

Erwägungsgrund 40 befasst sich mit den Datenschutzvorschriften in Rechtsakten, die kein umfassendes Datenschutzregime statuieren, und fordert einen Vorrang dieser Vorschriften insoweit, als sie strengere Regelungen über die Verwendung oder Weiterleitung von aus einem anderen Mitgliedstaat empfangenen Daten enthalten. Eine einschränkende Auslegung des Art. 28 RB DS dahingehend, dass der dort angeordnete Vorrang früher erlassener Rechtsakte nur gelten soll, wenn sie strengere Regelungen enthalten, ist jedoch auch im Lichte dieses Erwägungsgrundes nicht geboten. Der Erwägungsgrund betont lediglich den Vorrang von früher erlassenen strengeren Einzelvorschriften, fordert aber keinen generellen Vorrang des jeweils strengeren Rechts. Die in Art. 28 RB DS getroffene Regelung steht dazu nicht in Widerspruch.

## II. Ratsbeschluss Prüm

### 1. Verhältnis zum RB Datenschutz

Der Ratsbeschluss Prüm (RatsB Prüm) enthält neben einigen datenschutzrechtlichen Einzelregelungen in Kapitel 6 allgemeine Bestimmungen zum Datenschutz, die ein vollständiges, in sich abgeschlossenes Regelwerk bilden. In Erwägungsgrund 39 des RB DS werden zwar nur die Vorschriften des Ratsbeschlusses Prüm über die automatisierte Übermittlung von DNA-Profilen, daktyloskopischen Daten und Daten aus nationalen Fahrzeugregistern als dem RB DS vorgehende umfassende Regelungen genannt. Die umfassenden Regelungen in Kapitel 6 beziehen sich jedoch auf den gesamten Ratsbeschluss und können daher insgesamt als Spezialregelungen betrachtet werden, die durch den RB DS unberührt bleiben.

Die Umsetzung des RatsB Prüm – der nach dem Bericht „Umsetzungsbedarf Ratsbeschluss Prüm und Schwedische Initiative“ allerdings ohnehin keinen zwingenden Regelungsbedarf in den Ländergesetzen auslöst – kann daher weiterhin auch durch einen allgemeinen Anwendungsbefehl erfolgen (vgl. Bericht Anlage 1, S. 37), ohne dass Einschränkungen oder Sonderregelungen im Hinblick auf den RB DS erforderlich werden. Die Umsetzung des RatsB Prüm wird allerdings insoweit entbehrlich, als der RB DS die gleichen Anforderungen an den Datenschutz stellt, da mit Umsetzung dieser Vorschriften des RB DS auch die Anforderungen des Ratsbeschlusses Prüm erfüllt werden. Das Gleiche gilt, soweit der RB DS strengere Regelungen enthält als der RatsB Prüm. Der RatsB Prüm steht insoweit, als es um die weitere Verarbeitung von nach seinen Vorschriften übermittelten Daten geht, der Schaffung strengerer Regelungen nicht entgegen. Aus

Gründen der Verständlichkeit und Übersichtlichkeit der Gesetze dürfte es in diesen Fällen vorzuziehen sein, insgesamt das strengere Regime anzuwenden. Spezielle Vorschriften bleiben allerdings erforderlich, soweit der Ratsbeschlusses Prüm strengere Regelungen enthält als der RB DS.

## 2. Vergleich der einzelnen Vorschriften

Im Folgenden werden diejenigen Datenschutzvorschriften des RatsB Prüm mit den Regelungen des RB DS verglichen, für die der Bericht „Umsetzungsbedarf Ratsbeschluss Prüm und Schwedische Initiative“ eine Umsetzung in Landesrecht empfiehlt.

### a) Artikel 14 RatsB Prüm – Übermittlung personenbezogener Daten

Nach Art. 14 Abs. 2 RatsB Prüm dürfen Daten, die bei Großveranstaltungen ausgetauscht werden, nur im Zusammenhang mit der Veranstaltung verwendet werden, für die sie übermittelt wurden, und sind unverzüglich, spätestens nach einem Jahr zu löschen. Damit werden zu Zweckbindung und Löschung strengere Regelungen getroffen als in Art. 11 und 4 RB DS. Für nach Art. 14 RatsB Prüm übermittelte Daten sind daher spezielle Regelungen zur Zweckbindung und Löschung zu schaffen.

### b) Artikel 26 RatsB Prüm – Zweckbindung

In Bezug auf die zum Datenabgleich übermittelten DNA-, Fingerabdruck- und Fahrzeugdaten enthält Art. 26 Abs. 2 und 3 RatsB Prüm strikte Zweckbindungen und die Pflicht zur unverzüglichen Löschung der Daten, die über die Regelungen des RB DS hinausgehen. Auch zur Umsetzung des Art. 26 RatsB Prüm bedarf es daher spezieller Regelungen.

### c) Artikel 27 RatsB Prüm – Zuständige Behörden

Eine Weiterleitung von Daten ist nach Art. 27 Ratsbeschluss Prüm nur mit Zustimmung des Herkunftsstaats zulässig. Nach Art. 11 und 13 Abs. 2 RB DS ist eine Weiterleitung hingegen zu bestimmten Zwecken auch ohne Zustimmung des Herkunftsstaats zulässig. Für den Anwendungsbereich des RatsB Prüm sind insoweit Sonderregelungen zur schaffen.

### d) Artikel 28 RatsB Prüm – Richtigkeit, Aktualität und Speicherungsdauer von Daten

Art. 28 RatsB Prüm legt allgemeine Grundsätze zur Richtigkeit, Aktualität und Speicherungsdauer fest. Möglicher Umsetzungsbedarf besteht nach dem Bericht „Umsetzungsbedarf Ratsbeschluss Prüm und Schwedische Initiative“, Stand: 05.01.2011, nur für Art. 28 Abs. 2 und Abs. 3 Sätze 3 und 4.

Nach Art. 28 Abs. 2 RatsB Prüm sind Daten, deren Richtigkeit bestritten wird und nicht nachvollzogen werden kann, nach Maßgabe des nationalen Rechts zu kennzeichnen. Eine ähnliche Regelung trifft Art. 18 Abs. 2 RB DS, nach dem in diesen Fällen eine Kennzeichnung der Daten erfolgen *kann*. Soweit die Ländergesetze Regelungen zur Sperrung von Daten enthalten, werden sie beiden Vorschriften gerecht. Zwingenden Umsetzungsbedarf lösen allerdings beide Vorschriften ohnehin nicht aus.

Nach Art. 28 Abs. 3 RatsB Prüm sind Daten zu löschen, wenn sie rechtswidrig übermittelt wurden, wenn sie nicht mehr zum Übermittlungszweck erforderlich sind oder wenn die Löschfrist des übermittelnden Staates abgelaufen ist und der Empfänger auf die Frist hin-

gewiesen wurde. Bei berechtigtem Interesse des Betroffenen hat nur eine Sperrung zu erfolgen. Entsprechende Regelungen enthält der RB DS in Art. 4 Abs. 2 und 3 (Löschen von Daten, die nicht mehr benötigt werden), Art. 8 Abs. 2 (Löschen von Daten, die rechtswidrig übermittelt wurden) und Art. 9 (Löschen von Daten, wenn der übermittelnde Staat verlangt, dass eine bei ihm geltende Löschfrist eingehalten wird).
Im Regelungsbereich des Art. 28 RatsB Prüm müssen daher neben den Vorschriften zur Umsetzung der Art. 4, 8 und 9 RB DS keine Sonderregelungen getroffen werden.

**e) Artikel 30 Abs. 1 RatsB Prüm – Dokumentation und Protokollierung, besondere Vorschriften zur automatisierten und nichtautomatisierten Übermittlung**

Art. 30 Abs. 1 RatsB Prüm enthält Regelungen zur Dokumentation und Protokollierung der nichtautomatisierten Übermittlung und des nicht automatisierten Empfangs von in Dateien gespeicherten Daten. Art. 10 Abs. 1 RB DS regelt die Protokollierung und Dokumentation zwar weniger detailliert, aber letztlich inhaltsgleich, denn um ihren Zweck zu erfüllen, muss auch eine Dokumentation nach Art. 10 RB DS die in Art. 30 Abs. 1 RatsB Prüm genannten Inhalte enthalten. Die Protokollierungs- und Dokumentationspflichten aus Art. 10 RB DS beziehen sich allerdings nur auf die Datenübermittlung, nicht auf den Empfang von Daten. Insoweit enthält Art. 30 Abs. 1 RatsB Prüm daher weitergehende Pflichten als der RB DS. Zur Dokumentation und Protokollierung des nicht automatisierten Empfangs von Daten müssen daher im Anwendungsbereich des RatsB Prüm Sonderregelungen geschaffen werden.

## III. Rahmenbeschluss Schwedische Initiative

### 1. Verhältnis zum RB Datenschutz

Der Rahmenbeschluss Schwedische Initiative (RB SWI) enthält keine umfassenden Datenschutzvorschriften, sondern verweist auf das nationale Datenschutzrecht und auf das Übereinkommen des Europarats vom 28.01.1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Er geht dem RB DS daher nicht insgesamt als speziellere Norm vor. Unberührt bleiben jedoch gem. Art. 28 RB DS die Vorschriften des RB SWI über die Verwendung von empfangenen Daten. Dies sind Art. 1 Abs. 4 Satz 2 und Art.8 Abs. 3 und 4 RB SWI. Auch die nach Art. 28 RB DS vorrangigen Vorschriften des RB SWI bedürfen allerdings insoweit keiner Umsetzung mehr, als der RB DS gleiche oder strengere Anforderungen stellt und zu seiner Umsetzung entsprechende Regelungen geschaffen werden. Auch hier sprechen Übersichtlichkeit und Verständlichkeit des Rechts dafür, die Datenverarbeitung nach dem RB SWI den nach dem RB DS zu schaffenden Regelungen auch insoweit zu unterwerfen, als der RB DS ein strengeres Regime vorschreibt. Sonderregelungen zur Umsetzung des RB SWI sind allerdings dort erforderlich, wo der RB SWI die strengeren Regelungen enthält.

### 2. Vergleich der einzelnen Vorschriften

**a) Artikel 1 RB SWI – Zurverfügungstellung von Informationen und Erkenntnissen**

Nach Art. 1 Abs. 4 Satz 2 dürfen nach dem RB SWI übermittelte Daten als Beweismittel im Strafverfahren nur mit Zustimmung des übermittelnden Mitgliedstaats verwendet werden. Nach Art. 11 RB DS ist die Zweckänderung zur Strafverfolgung hingegen nicht an die

Zustimmung des übermittelnden Mitgliedstaats geknüpft. Für Daten, die nach dem RB SWI übermittelt werden, ist daher über die nach Art. 11 RB DS zu normierenden Beschränkungen der Zweckänderung hinaus die Verwendung als Beweismittel im Strafverfahren von der Zustimmung des übermittelnden Mitgliedstaats abhängig zu machen.

**b) Artikel 8 RB SWI – Datenschutz**

Art. 8 RB SWI enthält allgemeine Vorschriften zum Datenschutz. Vorschriften über die Verwendung von Daten werden in den Absätzen 3 und 4 getroffen.

Nach Art. 8 Abs. 3 RB SWI dürfen nach dem RB SWI übermittelte Daten für die Zwecke, für die sie übermittelt wurden und zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit verwendet werden; die Verwendung zu anderen Zwecken bedarf der Zustimmung des übermittelnden Mitgliedstaats.
Art.11 RB DS gestattet die Verwendung von Daten ohne Zustimmung des übermittelnden Mitgliedstaats auch für historische, statistische und wissenschaftliche Zwecke und zur Verhütung von Straftaten. Die Verwendung zu historischen, statistischen oder wissenschaftlichen Zwecken ist trotz des Fehlens einer ausdrücklichen Regelung auch nach dem RB SWI nicht ausgeschlossen, denn Art. 8 Abs. 3 RB SWI regelt nur die Verwendung der Daten zur Aufgabenerfüllung der Strafverfolgungsbehörden im engeren Sinne. Eine Verwendung zu historischen, statistischen und wissenschaftlichen Zwecken, die nach dem in Art. 2 RB SWI in Bezug genommenen allgemeinen Datenschutzrecht zulässig ist, läuft dem Schutzzweck der in Art. 8 Abs. 3 getroffenen Regelungen nicht zuwider. Es kann daher davon ausgegangen werden, dass eine solche Datenverwendung durch Art. 8 Abs. 3 nicht ausgeschlossen werden sollte. Für nach dem RB SWI übermittelte Daten muss daher die Zweckänderung für historische, statistische und wissenschaftliche Zweck nicht ausgeschlossen werden.
Ausgeschlossen ist für die nach dem RB SWI übermittelten Daten jedoch die nach dem RB DS ohne Zustimmung des übermittelnden Mitgliedstaates zulässige Verwendung von Daten zur Verhütung von Straftaten. Insoweit sind Sonderregelungen zu schaffen.

Nach Art. 8 Abs. 4 RB SWI sind Bedingungen zu beachten, die die übermittelnde Stelle nach Maßgabe ihres nationalen Rechts an die Verwendung von Informationen und Erkenntnissen stellt. Art. 12 RB DS sieht dagegen eine Bindung nur unter besonderen Umständen vor, wenn nach dem innerstaatlichen Recht des übermittelnden Mitgliedstaats besondere Verarbeitungsbeschränkungen für den Datenaustausch zwischen den innerstaatlichen Behörden gelten. Trotz des unterschiedlichen Wortlauts der Regelungen bestehen nach dem RB SWI und dem RB DS die gleichen Möglichkeiten, die Datenübermittlung mit verbindlichen Bedingungen zu verbinden. Im Hinblick auf das Gleichstellungsgebot als wesentlichen Inhalt des RB SWI muss auch Art. 8 Abs. 4 RB SWI einschränkend so ausgelegt werden, dass auch mit Datenübermittlungen nach dem RB SWI nur solche Bedingungen verbunden werden dürfen, die beim innerstaatlichen Datenaustausch zulässig wären.
Nach Art. 8 Abs. 4 Sätze 2 und 5 RB SWI sind auf Verlangen Ermittlungsergebnisse mitzuteilen und in besonderen Fällen Auskünfte über die Verwendung und weitere Verarbeitung der übermittelten Daten zu erteilen. Die Auskunftserteilung soll hier nach dem Bericht „Umsetzungsbedarf des Ratsbeschluss Prüm und Schwedische Initiative“ nur zur Datenschutzkontrolle erfolgen (Anlage 2, S. 24). Für Art. 15 RB DS kann eine solche Zweckbe-

schränkung hingegen nicht ohne weiteres angenommen werden. Sofern daher die Auskunftserteilung zur Umsetzung des Art. 15 RB DS auch zu anderen als zu Zwecken der Datenschutzkontrolle ermöglicht wird, ist zur Umsetzung des Art. 8 Abs. 4 Satz 5 RB SWI eine gesonderte, engere Regelung erforderlich.

## E. Ausblick

Hingewiesen sei noch auf die laufenden Überlegungen der Europäischen Kommission für ein Gesamtkonzept für den Datenschutz in der EU. Die Kommission hat ein solches Konzept am 4. November 2010 vorgestellt (KOM (2010) 609 endg.). Die darin vorgestellte Strategie soll aufzeigen wie sich der EU-Rahmen für den Datenschutz modernisieren und vereinheitlichen lässt. Art. 16 AEUV soll die Grundlage für die Schaffung einer umfassenden, kohärenten Regelung der EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bilden. Gestützt auf diese neue Rechtsgrundlage will die Kommission den Datenschutz einheitlich regeln und zwar auch in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen und sogar bei rein innerstaatlicher Verarbeitung. Unter Ziffer 2.3, Seite 17, der o.g. Mitteilung der Kommission vom 4. November 2010 ist Folgendes festgehalten:

„Die Kommission wird

- die Einbeziehung der Bereiche der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in den Anwendungsbereich der allgemeinen Datenschutzbestimmungen prüfen, und zwar auch bei einer rein innerstaatlichen Verarbeitung, gegebenenfalls bei gleichzeitiger Einführung harmonisierter Einschränkungen bestimmter Datenschutzrechte von Personen, z.B. hinsichtlich des Zugriffsrechts oder des Transparenzprinzips
- prüfen, ob die neue allgemeine Datenschutzregelung besondere, harmonisierte Vorschriften enthalten sollte, beispielsweise für den Datenschutz bei der Verarbeitung von Gendaten zu strafrechtlichen Zwecken, oder unterschiedliche Vorschriften für verschiedene Gruppen von Betroffenen (Zeugen, Verdächtige usw.) im Bereich der Zusammenarbeit zwischen den Polizeibehörden und der justiziellen Zusammenarbeit in Strafsachen;
- 2011 eine Konsultation aller interessierten Kreise durchführen, um ihre Meinung zu den bestehenden Verfahren zur Änderung des derzeitigen Kontrollsystems im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen einzuholen und so eine wirksame, kohärente Datenschutzkontrolle in den Einrichtungen, Ämtern und Agenturen der EU sicherzustellen;
- prüfen, ob die in einzelnen Rechtsakten enthaltenen sektorspezifischen EU-Vorschriften für die polizeiliche und justizielle Zusammenarbeit in Strafsachen langfristig an die neue allgemeine Datenschutzregelung angepasst werden sollten.“

Zwar ändern diese Überlegungen, denen sowohl Bundesregierung als auch Bundesrat weitgehend kritisch gegenüberstehen (vgl. BR-Drs. 707/10 [Beschluss]), nichts an dem Umstand, dass bis zu einem etwaigen Inkrafttreten neuer Regelungen die bisher beschlossenen Maßnahmen, also auch der RB DS, wirksam und von den Mitgliedstaaten umzusetzen sind. Die Überlegungen der Kommission zum Gesamtkonzept für den Daten-

schutz können aber gegebenenfalls für die Umsetzung des RB DS von Bedeutung sein (z.B. im Hinblick auf in diesem Bericht offen gebliebene Fragen oder hinsichtlich der Art der Umsetzung).