Deutscher Bundestag **Drucksache 18/6285**

18. Wahlperiode 08.10.2015

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden

A. Problem und Ziel

Mit dem Gesetz soll der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, umgesetzt werden.

B. Lösung

Der Rahmenbeschluss soll umgesetzt werden durch die Änderung des Bundeskriminalamtgesetzes, des Bundespolizeigesetzes, des Zollfahndungsdienstgesetzes, des Gesetzes über die internationale Rechtshilfe in Strafsachen und der Strafprozessordnung.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Keiner.

E.3 Erfüllungsaufwand der Verwaltung

Der Rahmenbeschluss sieht Verfahrenssicherungen bei der Inbetriebnahme von Dateien und beim Informationsaustausch zwischen zuständigen Stellen der EU-Mitgliedstaaten und Drittstaaten vor. Es lässt sich derzeit noch nicht abschätzen, ob diese Verfahrenssicherungen zu einem Mehraufwand für Personal und Sachmittel bei den Strafverfolgungsbehörden und den Beauftragten des Bundes und der Länder für den Datenschutz führen werden. Ein etwaiger Mehraufwand soll im Rahmen des jeweils betroffenen Einzelplans erwirtschaftet werden.

F. Weitere Kosten

Keine.

BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

Berlin, 8. Oktober 2015

An den
Präsidenten des
Deutschen Bundestages
Herrn Prof. Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich den von der Bundesregierung beschlossenen

> Entwurf eines Gesetzes zur Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium des Innern.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG ist als Anlage 2 beigefügt.

Der Bundesrat hat in seiner 936. Sitzung am 25. September 2015 gemäß Artikel 76 Absatz 2 des Grundgesetzes beschlossen, zu dem Gesetzentwurf wie aus Anlage 3 ersichtlich Stellung zu nehmen.

Die Auffassung der Bundesregierung zu der Stellungnahme des Bundesrates ist in der als Anlage 4 beigefügten Gegenäußerung dargelegt.

Mit freundlichen Grüßen

Dr. Angela Merkel

Anlage 1

Entwurf eines Gesetzes zur Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*)

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Artikel 3 i .V. m. Artikel 9 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 27a wie folgt gefasst:

   „§ 27a Verwendung von Daten, die aus Mitgliedstaaten der Europäischen Union oder aus Schengen-assoziierten Staaten übermittelt wurden“.

2. Nach § 10 Absatz 3 Satz 1 wird folgender Satz eingefügt:

   „Für personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates zum Zweck der Verhütung oder Verfolgung von Straftaten oder der Strafvollstreckung übermittelt oder bereitgestellt wurden, gilt Satz 1 mit der Maßgabe, dass die zuständige Behörde des anderen Staates der Übermittlung zugestimmt hat und dass eine Übermittlung nach Absatz 2 Nummer 3 nur zulässig ist, wenn sie für die Verhütung von Straftaten oder sonst für die Abwehr einer gegenwärtigen und erheblichen Gefahr unerlässlich ist.“

3. Dem § 14 werden die folgenden Absätze 8 bis 10 angefügt:

   „(8) Personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates zum Zweck der Verhütung oder Verfolgung von Straftaten oder der Strafvollstreckung übermittelt oder bereitgestellt wurden, dürfen an öffentliche Stellen sonstiger Staaten sowie an zwischen- oder überstaatliche Stellen nur übermittelt werden, soweit dies für die Verhütung oder Verfolgung einer Straftat oder für die Strafvollstreckung erforderlich ist und der Mitgliedstaat oder der Schengen-assoziierte Staat, der die Daten übermittelt oder bereitgestellt hat, der Übermittlung zugestimmt hat.

   (9) Ohne die nach Absatz 8 erforderliche Zustimmung des betroffenen Mitgliedstaates oder des betroffenen Schengen-assoziierten Staates dürfen personenbezogene Daten an öffentliche Stellen im Sinne des Absatzes 1 übermittelt werden, wenn die Übermittlung in den Fällen des Absatzes 1 Satz 1 Nummer 3 oder zur Wahrung wesentlicher Interessen eines Mitgliedstaates oder eines Schengen-assoziierten Staates unerlässlich ist und die vorherige Zustimmung nicht rechtzeitig eingeholt werden konnte. In diesem Fall unterrichtet das Bundeskriminalamt die für die Erteilung der Zustimmung zuständige Behörde unverzüglich.

   (10) Vor einer Übermittlung oder Bereitstellung soll das Bundeskriminalamt die Richtigkeit, Vollständigkeit und Aktualität der personenbezogenen Daten überprüfen. Bei jeder Übermittlung personenbezogener Daten werden nach Möglichkeit Informationen beigefügt, die es dem Empfänger gestatten, die Richtigkeit, Vollständigkeit, Aktualität und Zuverlässigkeit der personenbezogenen Daten zu beurteilen. Das Bundeskriminalamt kann bei der Übermittlung oder Bereitstellung der personenbezogenen Daten die nach nationalem Recht geltenden Fristen für die Aufbewahrung der Daten angeben, nach deren Ablauf auch der Empfänger

*) Dieses Gesetz dient der Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60).

die Daten zu löschen, zu sperren oder daraufhin zu überprüfen hat, ob ihre Speicherung noch erforderlich ist. Das Bundeskriminalamt weist den Empfänger auf besondere nach nationalem Recht geltende Verwendungsbeschränkungen für den Datenaustausch hin. Besteht keine gesetzliche Verpflichtung zur Benachrichtigung der betroffenen Person über die Erhebung oder Verarbeitung seiner personenbezogenen Daten oder kann im Einzelfall von der Benachrichtigung abgesehen werden, kann das Bundeskriminalamt den Empfänger darum ersuchen, den Betroffenen nicht ohne die vorherige Zustimmung des Bundeskriminalamts zu informieren."

4. Dem § 14a wird folgender Absatz 7 angefügt:

„(7) Das Bundeskriminalamt kann unter den Voraussetzungen des § 10 Absatz 3 Satz 2 personenbezogene Daten an nicht öffentliche Stellen in Mitgliedstaaten der Europäischen Union und in Schengen-assoziierten Staaten übermitteln."

5. § 27a wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

„§ 27a

Verwendung von Daten, die aus Mitgliedstaaten der Europäischen Union oder aus Schengen-assoziierten Staaten übermittelt wurden".

b) Dem bisherigen Absatz 1 wird folgender Absatz 1 vorangestellt:

„(1) In Dateien gespeicherte personenbezogene Daten, die von einer Behörde eines Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates übermittelt oder bereitgestellt wurden, dürfen unbeschadet des Absatzes 2 außer für Zwecke, für die sie übermittelt oder bereitgestellt wurden, nur für folgende Zwecke verwendet werden:

1. die Verhütung oder Verfolgung von Straftaten oder die Strafvollstreckung,
2. andere mit den Zwecken nach Nummer 1 unmittelbar zusammenhängende justizielle und verwaltungsbehördliche Verfahren oder
3. die Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit.

Für sonstige Zwecke dürfen sie nur mit vorheriger Zustimmung des übermittelnden Mitgliedstaates oder des übermittelnden Schengen-assoziierten Staates oder mit Einwilligung der betroffenen Person (§ 4a des Bundesdatenschutzgesetzes) verwendet werden. Das Bundeskriminalamt berücksichtigt die Verwendungsbeschränkungen nach dem nationalen Recht eines Mitgliedstaates oder Schengen-assoziierten Staates, auf die dessen übermittelnde Behörde hingewiesen hat. Die Sätze 1 bis 3 gelten auch, wenn Daten im Sinne des Satzes 1 an andere Mitgliedstaaten der Europäischen Union oder andere Schengen-assoziierte Staaten übermittelt oder für diese bereitgestellt werden sollen."

c) Der bisherige Absatz 1 wird Absatz 2.

d) Der bisherige Absatz 2 wird Absatz 3 und wie folgt gefasst:

„(3) Das Bundeskriminalamt erteilt der übermittelnden oder bereitstellenden Behörde auf deren Ersuchen Auskunft darüber, wie die übermittelten Daten verwendet wurden."

6. Dem § 32 wird folgender Absatz 10 angefügt:

„(10) Hat die übermittelnde Behörde eines Mitgliedstaates der Europäischen Union bei der Übermittlung oder Bereitstellung personenbezogener Daten Fristen zur Löschung, Sperrung oder Aussonderung mitgeteilt, nach deren Ablauf der Empfänger die Daten zu löschen, zu sperren oder daraufhin zu überprüfen hat, ob ihre Speicherung noch erforderlich ist, so hat das Bundeskriminalamt diese zu beachten. Diese Verpflichtung besteht nicht, solange die Speicherung der Daten für eine laufende Ermittlung, eine Verfolgung von Straftaten oder eine Vollstreckung strafrechtlicher Sanktionen erforderlich ist. Die Sätze 1 und 2 gelten auch für Übermittlungen durch Behörden Schengen-assoziierter Staaten oder durch Behörden und Informationssysteme nach dem Dritten Teil Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union."

Artikel 2

Änderung des Bundespolizeigesetzes

Das Bundespolizeigesetz vom 19. Oktober 1994 (BGBl. I S. 2978, 2979), das zuletzt durch Artikel 4 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 33a wie folgt gefasst:

   „§ 33a Verwendung von Daten, die aus Mitgliedstaaten der Europäischen Union oder aus Schengen-assoziierten Staaten übermittelt wurden“.

2. Dem § 32 Absatz 3 wird folgender Satz angefügt:

   „Personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates zum Zweck der Verhütung oder Verfolgung von Straftaten oder der Strafvollstreckung übermittelt oder bereitgestellt wurden, dürfen an Behörden sonstiger Staaten an sowie über- oder zwischenstaatliche Stellen nur übermittelt werden, soweit dies für die Verhütung oder Verfolgung einer Straftat oder für die Strafvollstreckung erforderlich ist.“

3. § 33 wird wie folgt geändert:

   a) Nach Absatz 2 wird folgender Absatz 2a eingefügt:

      „(2a) Personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates zum Zweck der Verhütung oder Verfolgung von Straftaten oder der Strafvollstreckung übermittelt oder bereitgestellt wurden, dürfen an Behörden sonstiger Staaten sowie an über- oder zwischenstaatliche Stellen gemäß § 32 Absatz 3 sowie an nicht-öffentliche Stellen gemäß § 32 Absatz 4 nur übermittelt werden, wenn der Mitgliedstaat oder der Schengen-assoziierte Staat, der die Daten übermittelt oder bereitgestellt hat, der Übermittlung zugestimmt hat. Eine Übermittlung an sonstige Staaten oder an über- oder zwischenstaatliche Stellen nach § 32 Absatz 3 ohne vorherige Zustimmung ist nur zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr für die öffentliche Sicherheit zulässig oder wenn die Übermittlung zur Wahrung wesentlicher Interessen eines Mitgliedstaates oder eines Schengen-assoziierten Staates unerlässlich ist und die vorherige Zustimmung nicht rechtzeitig eingeholt werden konnte. In diesem Fall unterrichtet die Bundespolizei die für die Erteilung der Zustimmung zuständige Behörde unverzüglich.“

   b) Dem Absatz 6 werden die folgenden Sätze angefügt:

      „Bei einer Übermittlung oder Bereitstellung von Daten an einen Mitgliedstaat der Europäischen Union kann die Bundespolizei den Empfänger darum ersuchen, den Betroffenen nicht ohne vorherige Zustimmung der Bundespolizei zu informieren, soweit keine gesetzliche Verpflichtung zur Benachrichtigung des Betroffenen über die Erhebung oder Verarbeitung seiner personenbezogenen Daten besteht oder im Einzelfall von der Benachrichtigung abgesehen werden kann. Satz 5 gilt auch für Übermittlungen an Schengen-assoziierte Staaten und an Behörden und Informationssysteme nach dem Dritten Teil Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union.“

   c) In Absatz 8 Satz 1 werden die Wörter „durchschnittlich jedem zehnten“ durch das Wort „jedem“ ersetzt.

   d) Folgender Absatz 9 wird angefügt:

      „(9) Vor einer Übermittlung oder Bereitstellung an öffentliche Stellen anderer Staaten sowie an über- oder zwischenstaatliche Stellen soll die Bundespolizei die Richtigkeit, Vollständigkeit und Aktualität der personenbezogenen Daten überprüfen. Ist der Empfänger der Daten eine öffentliche Stelle, werden nach Möglichkeit Informationen beigefügt, die es ihm gestatten, die Richtigkeit, Vollständigkeit, Aktualität und Zuverlässigkeit der Daten zu beurteilen.“

4. § 33a wird wie folgt geändert:
   a) Die Überschrift wird wie folgt gefasst:

„§ 33a
Verwendung von Daten, die aus Mitgliedstaaten der Europäischen Union oder aus Schengen-assoziierten Staaten übermittelt wurden“.

   b) Dem bisherigen Absatz 1 werden die folgenden Absätze 1 und 2 vorangestellt:

„(1) In Dateien gespeicherte personenbezogene Daten, die von einer Behörde eines Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates übermittelt oder bereitgestellt wurden, dürfen unbeschadet des Absatzes 3 außer für die Zwecke, für die sie übermittelt oder bereitgestellt wurden, nur für folgende Zwecke verwendet werden:

1. die Verhütung oder Verfolgung von Straftaten oder die Strafvollstreckung,
2. andere mit den Zwecken nach Nummer 1 unmittelbar zusammenhängende justizielle und verwaltungsbehördliche Verfahren oder
3. die Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit.

(2) Für sonstige Zwecke dürfen sie nur mit vorheriger Zustimmung des übermittelnden Mitgliedstaates oder mit der Einwilligung der betroffenen Person (§ 4a des Bundesdatenschutzgesetzes) verwendet werden. Die Bundespolizei berücksichtigt die Verwendungsbeschränkungen nach dem nationalen Recht eines Mitgliedstaates oder eines Schengen-assoziierten Staates, auf die dessen übermittelnde Behörde hingewiesen hat.“

   c) Der bisherige Absatz 1 wird Absatz 3.

   d) Der bisherige Absatz 2 wird Absatz 4 und wie folgt gefasst:

„(4) Die Bundespolizei erteilt der übermittelnden oder bereitstellenden Behörde auf deren Ersuchen Auskunft darüber, wie die übermittelten Daten verwendet wurden.“

5. Dem § 35 wird folgender Absatz 10 angefügt:

„(10) Hat die übermittelnde Behörde eines Mitgliedstaates der Europäischen Union bei der Übermittlung oder Bereitstellung personenbezogener Daten Fristen für die Aufbewahrung der Daten angegeben, nach deren Ablauf der Empfänger die Daten zu löschen, zu sperren oder daraufhin zu überprüfen hat, ob ihre Speicherung noch erforderlich ist, so hat die Bundespolizei diese zu beachten. Diese Verpflichtung besteht nicht, solange die Speicherung der Daten für eine laufende Ermittlung, eine Verfolgung von Straftaten oder eine Strafvollstreckung erforderlich ist. Die Sätze 1 und 2 gelten auch für Übermittlungen durch Behörden Schengen-assoziierter Staaten oder durch Behörden und Informationssysteme nach dem Dritten Teil Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union.“

Artikel 3

Änderung des Zollfahndungsdienstgesetzes

Das Zollfahndungsdienstgesetz vom 16. August 2002 (BGBl. I S. 3202), das zuletzt durch Artikel 5 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 35a wie folgt gefasst:

„§ 35a Verwendung von Daten, die aus Mitgliedstaaten der Europäischen Union oder aus Schengen-assoziierten Staaten übermittelt wurden“.

2. In § 11 Absatz 4 Satz 1 werden die Wörter „durchschnittlich jedem zehnten“ durch das Wort „jedem“ ersetzt.
3. § 33 wird wie folgt geändert:
   a) Dem Absatz 3 wird folgender Satz angefügt:

„Bei Übermittlungen an nicht öffentliche Stellen haben die Behörden des Zollfahndungsdienstes den Empfänger darauf hinzuweisen.“

b) In Absatz 5 wird nach Satz 1 folgender Satz eingefügt:

„Für personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates zum Zwecke der Verhütung oder Verfolgung von Straftaten oder der Strafvollstreckung übermittelt oder bereitgestellt wurden, gilt Satz 1 mit der Maßgabe, dass die zuständige Behörde des anderen Staates der Übermittlung zugestimmt hat, überwiegende schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden und eine Übermittlung nach Absatz 1 Satz 2 Nummer 3 nur zulässig ist, wenn sie zur Verhütung von Straftaten oder sonst zur Abwehr einer gegenwärtigen und erheblichen Gefahr unerlässlich ist.“

c) Nach Absatz 5 wird folgender Absatz 6 eingefügt:

„(6) Besteht Grund zu der Annahme, dass durch die Übermittlung von Daten nach Absatz 5 der der Erhebung der Daten zugrunde liegende Zweck gefährdet würde, so holen die Behörden des Zollfahndungsdienstes vor der Übermittlung die Zustimmung der Stelle ein, die die Daten übermittelt hat. Im Fall der Annahme einer Gefährdung nach Satz 1 kann die übermittelnde Stelle Daten so kennzeichnen oder mit einem Hinweis versehen, dass vor einer Übermittlung nach Absatz 5 ihre Zustimmung einzuholen ist.“

d) Der bisherige Absatz 6 wird Absatz 7.

4. Dem § 34 werden die folgenden Absätze 5 bis 7 angefügt:

„(5) Personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates zum Zweck der Verhütung oder Verfolgung von Straftaten oder der Strafvollstreckung übermittelt oder bereitgestellt wurden, dürfen an öffentliche Stellen sonstiger Staaten sowie an zwischen- oder überstaatliche Stellen nur übermittelt werden, soweit dies für die Verhütung oder Verfolgung einer Straftat oder für die Strafvollstreckung erforderlich ist und der Mitgliedstaat oder Schengen-assoziierte Staat, der die Daten übermittelt oder bereitgestellt hat, der Übermittlung zugestimmt hat.

(6) Ohne die nach Absatz 5 erforderliche Zustimmung des betroffenen Mitgliedstaates oder des betroffenen Schengen-assoziierten Staates, dürfen personenbezogene Daten an öffentliche Stellen im Sinne des Absatzes 1 übermittelt werden, wenn die Übermittlung in den Fällen des Absatzes 1 Satz 1 Nummer 3 oder für die Wahrung wesentlicher Interessen eines Mitgliedstaates oder Schengen-assoziierten Staates unerlässlich ist und die vorherige Zustimmung nicht rechtzeitig eingeholt werden konnte. In diesem Fall unterrichten die Behörden des Zollfahndungsdienstes die für die Erteilung der Zustimmung zuständige Behörde unverzüglich.

(7) Vor einer Übermittlung oder Bereitstellung sollen die Behörden des Zollfahndungsdienstes die Richtigkeit, Vollständigkeit und Aktualität der personenbezogenen Daten überprüfen. Bei jeder Übermittlung personenbezogener Daten werden nach Möglichkeit Informationen beigefügt, die es dem Empfänger gestatten, die Richtigkeit, Vollständigkeit, Aktualität und Zuverlässigkeit der personenbezogenen Daten zu beurteilen. Die Behörden des Zollfahndungsdienstes können bei der Übermittlung oder Bereitstellung der personenbezogenen Daten die nach nationalem Recht geltenden Fristen für die Aufbewahrung der Daten angeben, nach deren Ablauf auch der Empfänger die Daten zu löschen, zu sperren oder daraufhin zu überprüfen hat, ob ihre Speicherung noch erforderlich ist. Die Behörden des Zollfahndungsdienstes weisen den Empfänger auf besondere nach nationalem Recht geltende Verwendungsregelungen für den Datenaustausch hin. Besteht keine gesetzliche Verpflichtung zur Benachrichtigung des Betroffenen über die Erhebung oder Verarbeitung seiner personenbezogenen Daten oder kann im Einzelfall von der Benachrichtigung abgesehen werden, so können die Behörden des Zollfahndungsdienstes den Empfänger darum ersuchen, den Betroffenen nicht ohne die vorherige Zustimmung der Behörden des Zollfahndungsdienstes zu informieren.“

5. Dem § 34a wird folgender Absatz 7 angefügt:

„(7) Die Behörden des Zollfahndungsdienstes können unter den Voraussetzungen des § 33 Absatz 5 Satz 2 personenbezogene Daten an nicht öffentliche Stellen in Mitgliedstaaten der Europäischen Union oder in Schengen-assoziierten Staaten übermitteln.“

6. § 35a wird wie folgt geändert:
   a) Die Überschrift wird wie folgt gefasst:

„§ 35a
Verwendung von Daten, die aus Mitgliedstaaten der Europäischen Union oder aus Schengen-assoziierten Staaten übermittelt wurden“.

   b) Dem bisherigen Absatz 1 wird folgender Absatz 1 vorangestellt:

„(1) In Dateien gespeicherte personenbezogene Daten, die von einer Behörde eines Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates übermittelt oder bereitgestellt wurden, dürfen unbeschadet des Absatzes 2 außer für die Zwecke, für die sie übermittelt oder bereitgestellt wurden, nur für folgende Zwecke verwendet werden:

1. die Verhütung oder Verfolgung von Straftaten oder die Strafvollstreckung,
2. andere mit den Zwecken nach Nummer 1 unmittelbar zusammenhängende justizielle und verwaltungsbehördliche Verfahren oder
3. die Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit.

Für sonstige Zwecke dürfen sie nur mit vorheriger Zustimmung des übermittelnden Mitgliedstaates oder des übermittelnden Schengen-assoziierten Staates oder mit Einwilligung der betroffenen Person (§ 4a des Bundesdatenschutzgesetzes) verwendet werden. Die Behörden des Zollfahndungsdienstes berücksichtigen die Verwendungsbeschränkungen nach dem nationalen Recht eines Mitgliedsstaates oder Schengen-assoziierten Staates, auf die dessen übermittelnde Behörde hingewiesen hat. Die Sätze 1 bis 3 gelten auch, wenn Daten im Sinne des Satzes 1 an andere Mitgliedstaaten der Europäischen Union übermittelt oder für diese bereitgestellt werden sollen.“

   c) Der bisherige Absatz 1 wird Absatz 2.
   d) Der bisherige Absatz 2 wird Absatz 3 und wie folgt gefasst:

„(3) Die Behörden des Zollfahndungsdienstes erteilen der übermittelnden oder bereitstellenden Behörde auf deren Ersuchen Auskunft darüber, wie die übermittelten Daten verwendet wurden.“

7. Dem § 39 wird folgender Absatz 11 angefügt:

„(11) Hat die übermittelnde Behörde eines Mitgliedstaates der Europäischen Union bei der Übermittlung oder Bereitstellung personenbezogener Daten Fristen für die Aufbewahrung der Daten angegeben, nach deren Ablauf auch der Empfänger die Daten zu löschen, zu sperren oder daraufhin zu überprüfen hat, ob ihre Speicherung noch erforderlich ist, so haben die Behörden des Zollfahndungsdienstes diese zu beachten. Diese Verpflichtung besteht nicht, solange die Speicherung der Daten für eine laufende Ermittlung, eine Verfolgung von Straftaten oder eine Strafvollstreckung erforderlich ist. Die Sätze 1 und 2 gelten auch für Übermittlungen durch Behörden Schengen-assoziierter Staaten oder durch Behörden oder Informationssysteme nach dem Dritten Teil Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union.“

Artikel 4

Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen

Das Gesetz über die internationale Rechtshilfe in Strafsachen in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 1 des Gesetzes vom 16. Juli 2015 (BGBl. I S. 1197) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) Nach der Angabe zu § 97 werden die folgenden Angaben eingefügt:

„Elfter Teil

Schutz personenbezogener Daten im Zusammenhang mit dem Rechtshilfeverkehr innerhalb der Europäischen Union und mit den Schengen-assoziierten Staaten

b) Die Angabe zum bisherigen Elften Teil wird die Angabe zum Zwölften Teil.

2. Nach dem Zehnten Teil wird folgender Elfter Teil eingefügt:

„Elfter Teil
Schutz personenbezogener Daten im Zusammenhang mit dem Rechtshilfeverkehr innerhalb der Europäischen Union und mit den Schengen-assoziierten Staaten

§ 97a
Anwendungsbereich

(1) Die Vorschriften dieses Teils sind auf personenbezogene Daten anzuwenden, soweit

1. die Daten
   a) ganz oder teilweise automatisiert erhoben, verarbeitet oder genutzt werden oder
   b) im Fall einer nicht automatisierten Erhebung, Verarbeitung oder Nutzung in einer Datei gespeichert sind oder werden sollen und
2. die Daten nach Nummer 1 an Mitgliedstaaten der Europäischen Union oder an Behörden oder Informationssysteme nach dem Dritten Teil Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union übermittelt oder für diese bereitgestellt oder von diesen empfangen werden.

(2) Schengen-assoziierte Staaten stehen den Mitgliedstaaten der Europäischen Union bei der Anwendung dieses Teils gleich.

§ 97b
Verwendung von Daten

(1) Personenbezogene Daten, die von einem anderen Mitgliedstaat übermittelt oder bereitgestellt wurden, dürfen, soweit dies gesetzlich vorgesehen ist, außer für die Zwecke, für die sie übermittelt oder bereitgestellt wurden, nur für folgende andere Zwecke verwendet werden:

1. für die Verhütung oder Verfolgung von anderen Straftaten oder anderen Ordnungswidrigkeiten als denen, für die die Daten übermittelt oder bereitgestellt wurden,
2. für die Vollstreckung oder den Vollzug von anderen strafrechtlichen Sanktionen als denen, für die die Daten übermittelt oder bereitgestellt wurden,
3. für andere justizielle oder verwaltungsbehördliche Verfahren, die mit den Zwecken nach den Nummern 1 oder 2 unmittelbar zusammenhängen,
4. für die Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit oder

5. für jeden anderen Zweck, wenn der übermittelnde oder bereitstellende Mitgliedstaat oder die betroffene Person zuvor zugestimmt haben.

(2) Personenbezogene Daten, die von einem anderen Mitgliedstaat übermittelt oder bereitgestellt wurden, dürfen im Zusammenhang mit einem Strafverfahren oder einem Bußgeldverfahren an nicht öffentliche Stellen weitergeleitet werden, soweit dies gesetzlich vorgesehen ist. Im Übrigen dürfen diese Daten, soweit dies gesetzlich vorgesehen ist, außer für die Zwecke, für die sie übermittelt oder bereitgestellt wurden, nur an nicht öffentliche Stellen weitergeleitet werden, wenn folgende Voraussetzungen erfüllt sind:

1. die zuständige Behörde des Mitgliedstaates, von dem die Daten übermittelt oder bereitgestellt wurden, hat der Weiterleitung zugestimmt,
2. überwiegende schutzwürdige Interessen der betroffenen Person stehen nicht entgegen und
3. die Weiterleitung ist für die weiterleitende Stelle im Einzelfall unerlässlich
   a) für die Erfüllung einer ihr zugewiesenen Aufgabe,
   b) für die Verhütung oder Verfolgung von anderen Straftaten oder anderen Ordnungswidrigkeiten als denen, für die die Daten übermittelt oder bereitgestellt wurden,
   c) für die Vollstreckung oder den Vollzug von anderen strafrechtlichen Sanktionen als denen, für die die Daten übermittelt oder bereitgestellt wurden,
   d) für die Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit oder
   e) für die Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner.

Die weiterleitende Behörde weist die empfangende nicht öffentliche Stelle darauf hin, zu welchen Zwecken die personenbezogenen Daten ausschließlich verwendet werden dürfen.

(3) Personenbezogene Daten, die von einem anderen Mitgliedstaat oder von Behörden oder Informationssystemen nach dem Dritten Teil Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union übermittelt oder bereitgestellt wurden, dürfen die zuständigen Behörden unbeschadet der Verwendung nach den Absätzen 1 und 2 nach Maßgabe der geltenden Vorschriften auch für historische, statistische oder wissenschaftliche Zwecke verwenden.

(4) Werden personenbezogene Daten ohne Ersuchen von einem anderen Mitgliedstaat oder von Behörden oder Informationssystemen nach dem Dritten Teil Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union übermittelt, prüft die empfangende Stelle unverzüglich, ob die Daten für den Zweck, für den sie übermittelt wurden, benötigt werden.

§ 97c

Übermittlung oder Bereitstellung von Daten

(1) Die Verantwortung für die Zulässigkeit der Übermittlung oder Bereitstellung von personenbezogenen Daten im Rechtshilfeverkehr trägt die übermittelnde oder bereitstellende Stelle.

(2) Die übermittelnde oder bereitstellende Stelle

1. soll personenbezogene Daten vor ihrer Übermittlung oder Bereitstellung auf Richtigkeit, Vollständigkeit und Aktualität überprüfen,
2. fügt bei der Übermittlung von personenbezogenen Daten nach Möglichkeit Informationen bei, die es der empfangenden Stelle gestatten, die Richtigkeit, Vollständigkeit, Aktualität und Zuverlässigkeit der Daten zu beurteilen,
3. weist die empfangende Stelle auf nach deutschem Recht geltende besondere Verwendungsbeschränkungen hin, denen die personenbezogenen Daten unterliegen,
4. kann bei der Übermittlung oder Bereitstellung von personenbezogenen Daten die nach deutschem Recht geltenden Fristen für die Aufbewahrung der Daten angeben, nach deren Ablauf die empfangende Stelle die Daten zu löschen, zu sperren oder daraufhin zu überprüfen hat, ob ihre Speicherung noch erforderlich ist, und
5. unterrichtet die empfangende Stelle unverzüglich, wenn sich herausstellt, dass Daten nicht hätten übermittelt werden dürfen oder dass unrichtige Daten übermittelt wurden.

§ 97d

Weiterleitung von Daten an Drittstaaten sowie an zwischen- oder überstaatliche Einrichtungen

(1) Personenbezogene Daten, die von einem anderen Mitgliedstaat übermittelt oder bereitgestellt wurden, dürfen, soweit dies gesetzlich vorgesehen ist, an Drittstaaten oder an zwischen- oder überstaatliche Einrichtungen nur weitergeleitet werden, wenn

1. dies für die Verhütung oder Verfolgung von Straftaten oder von Ordnungswidrigkeiten oder für die Vollstreckung oder den Vollzug von strafrechtlichen Sanktionen erforderlich ist,
2. die empfangende Stelle für eine der in Nummer 1 genannten Aufgaben zuständig ist,
3. der Mitgliedstaat, der die Daten übermittelt oder bereitgestellt hat, der Weiterleitung der Daten zuvor zugestimmt hat und
4. der Drittstaat oder die zwischen- oder überstaatliche Einrichtung ein angemessenes Schutzniveau für die beabsichtigte Datenverarbeitung gewährleistet.

(2) Kann die nach Absatz 1 Nummer 3 erforderliche vorherige Zustimmung des betroffenen Mitgliedstaates nicht rechtzeitig eingeholt werden, ist die Weiterleitung von personenbezogenen Daten auch ohne eine Zustimmung zulässig, wenn die Weiterleitung unerlässlich ist zur Abwehr einer gegenwärtigen und erheblichen Gefahr

1. für die öffentliche Sicherheit eines Mitgliedstaates oder eines Drittstaates oder
2. für wesentliche Interessen eines Mitgliedstaates.

In diesem Fall unterrichtet die übermittelnde Stelle unverzüglich die für die Erteilung der Zustimmung zuständige Behörde des betroffenen Mitgliedstaates.

(3) Fehlt es an einem angemessenen Schutzniveau gemäß Absatz 1 Nummer 4, dürfen personenbezogene Daten nur weitergeleitet werden, wenn

1. überwiegende schutzwürdige Interessen der betroffenen Person zu wahren sind,
2. andere überwiegende Interessen, insbesondere wichtige öffentliche Interessen, zu wahren sind oder
3. der Drittstaat oder die zwischen- oder überstaatliche Einrichtung angemessene Garantien zum Datenschutz anbietet.“

3. Der bisherige Elfte Teil wird der Zwölfte Teil.

Artikel 5

Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 12. Juni 2015 (BGBl. I S. 926) geändert worden ist, wird wie folgt geändert:

1. § 488 wird wie folgt geändert:
   a) Absatz 3 wird wie folgt geändert:
      aa) In Satz 3 werden die Wörter „zumindest durch geeignete Stichprobenverfahren“ gestrichen.
      bb) In Satz 4 wird das Wort „soll“ durch das Wort „hat“ ersetzt, das Wort „zehnten“ gestrichen sowie vor dem Wort „protokollieren“ das Wort „zu“ eingefügt.
      cc) Satz 5 wird wie folgt gefasst:

      „Die Protokolldaten dürfen nur für Zwecke der Datenschutzkontrolle, insbesondere zur Kontrolle der Zulässigkeit der Abrufe und der Datensicherheit, verwendet werden und sind nach zwölf Monaten zu löschen.“

b) Folgender Absatz 4 wird angefügt:

„(4) Die Absätze 2 und 3 gelten für das automatisierte Anfrage- und Auskunftsverfahren entsprechend.“

2. Dem § 489 wird folgender Absatz 10 angefügt:

„(10) Nimmt die speichernde Stelle eine von einer betroffenen Person beantragte Berichtigung, Löschung oder Sperrung nicht vor, teilt sie ihr dies schriftlich mit und weist sie auf die bestehenden Rechtsbehelfe hin.“

3. § 490 wird wie folgt geändert:

a) Nach Satz 1 werden die folgenden Sätze eingefügt:

„Die speichernde Stelle gewährleistet, dass vor der Verarbeitung personenbezogener Daten in einer neu zu errichtenden automatisierten Datei die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständige Stelle angehört wird. Ist auf Grund der Dringlichkeit der Errichtung der Datei die Mitwirkung der in Satz 2 genannten Stelle nicht möglich, so kann die speichernde Stelle eine Sofortanordnung treffen. In diesem Fall ist die Anhörung unverzüglich nachzuholen.“

b) In dem neuen Satz 5 werden die Wörter „Dies gilt“ durch die Wörter „Die Sätze 1 bis 4 gelten“ ersetzt.

4. § 493 Absatz 3 wird wie folgt geändert:

a) In Satz 3 wird das Wort „zehnten“ gestrichen.

b) Satz 4 wird wie folgt gefasst:

„Die Protokolldaten dürfen nur für Zwecke der Datenschutzkontrolle, insbesondere zur Kontrolle der Zulässigkeit der Abrufe und der Datensicherheit, verwendet werden und sind nach sechs Monaten zu löschen.“

5. § 494 Absatz 3 wird wie folgt gefasst:

„(3) § 489 Absatz 7, 8 und 10 gilt entsprechend.“

Artikel 6

Änderung des Gesetzes über Ordnungswidrigkeiten

In § 110d Absatz 2 Satz 4 des Gesetzes über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), das zuletzt durch Artikel 4 des Gesetzes vom 13. Mai 2015 (BGBl. I S. 706) geändert worden ist, werden die Wörter „der Zeitpunkt, die abgerufenen Daten und die Kennung der abrufenden Stelle bei jedem Abruf zu protokollieren sind und“ gestrichen.

Artikel 7

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Entstehungsgeschichte

Der Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60 – im Folgenden: RbDatenschutz), wurde am 27. November 2008 vom Rat der Innen- und Justizminister der Europäischen Union angenommen.

Der auf einen Vorschlag der Kommission zurückgehende Rahmenbeschluss dient der Umsetzung der im „Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union“ (ABl. C 53, S. 1) niedergelegten Grundsätze. Nachdem mit dem Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89) der Grundsatz der Verfügbarkeit umgesetzt worden ist, soll der RbDatenschutz die in diesem Zusammenhang erforderliche strenge Einhaltung bestimmter Kernbedingungen für den Datenschutz sicherstellen. Dies ist zum einen zum Schutz der Grundrechte der betroffenen Personen erforderlich. Zum anderen wird bei den übermittelnden Mitgliedstaaten bzw. Behörden das erforderliche Vertrauen in den (trotz Weitergabe aus dem eigenen Verantwortungsbereich hinaus) unvermindert gleich gewährleisteten Schutz der Daten gestärkt.

II. Neuerungen des RbDatenschutz

Der RbDatenschutz verfolgt das Ziel, die Weiterentwicklung der Union als Raum der Freiheit, der Sicherheit und des Rechts, verbunden mit einem gemeinsamen Vorgehen der Mitgliedstaaten bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, durch gemeinsame Normen für die Verwendung und den verbesserten Schutz personenbezogener Daten zu begleiten.

Die bisherigen Rechtsvorschriften auf europäischer Ebene reichten nicht aus, um auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit Daten so zu schützen, dass eine Diskriminierung der Zusammenarbeit zwischen den Mitgliedstaaten ausgeschlossen ist und gleichzeitig die Grundrechte des Betroffenen in vollem Umfang gewahrt bleiben. Denn die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31) findet keine Anwendung auf die Verarbeitung und Nutzung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgen, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, insbesondere nicht auf Verwendungen im Bereich der öffentlichen Sicherheit und der Strafverfolgung.

Der RbDatenschutz gibt nunmehr den Mitgliedstaaten einen einheitlichen Rahmen für ein angemessenes Datenschutzniveau bei der Zusammenarbeit innerhalb der EU vor. Sein Anwendungsbereich ist nach Artikel 1 Absatz 2 RbDatenschutz beschränkt auf Daten, die von zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen erhoben oder verarbeitet werden, soweit diese Daten zwischen Mitgliedstaaten weitergegeben oder bereitgestellt werden. Unterliegen die Daten danach einmal dem Anwendungsbereich des Rahmenbeschlusses, gilt dieser auch für die Weitergabe an Drittstaaten.

In Bezug auf die Datenverarbeitung im innerstaatlichen Bereich haben die Mitgliedstaaten im Erwägungsgrund 8 lediglich ihre Absicht bekundet, dass ein Datenschutzstandard gewährleistet wird, der dem im RbDatenschutz festgelegten wenigstens entspricht.

Ein grundlegendes Prinzip der weiteren Verwendung von aus Mitgliedstaaten übermittelten Daten für verfahrensübergreifende Zwecke ist die Zustimmung. Wichtigster Anwendungsfall ist hierbei die Übermittlung von Daten aus Mitgliedstaaten an Dritte (vgl. die Artikel 11, 13 und 14 RbDatenschutz). Der Rahmenbeschluss lässt es allerdings zu, dass der Herkunftsmitgliedstaat der Daten eine allgemeine Zustimmung für bestimmte Arten von

personenbezogenen Daten, bestimmte Drittstaaten oder bestimmte Formen der Weiterverwendung erteilt. Darüber hinaus enthält Artikel 13 RbDatenschutz eine Eilfallregelung zugunsten dringender Maßnahmen.

Der RbDatenschutz sieht in Artikel 16 sowie in Erwägungsgrund 26 die grundsätzliche Notwendigkeit, dass Betroffene bei besonders schwerwiegenden Eingriffen in ihre Rechte durch Maßnahmen der heimlichen Datenerhebung zu informieren sind, damit ihnen nachträglich die Möglichkeit effektiven Rechtsschutzes eröffnet ist. Allerdings verzichtet er hierbei auf einheitliche Regelungen und verweist vielmehr auf das innerstaatliche Recht. Im Erwägungsgrund 27 wird zudem allgemein die Empfehlung ausgesprochen, dass die Mitgliedstaaten von der Datenverarbeitung Betroffene darüber informieren, dass ihre personenbezogenen Daten auch an andere Mitgliedstaaten übermittelt werden könnten. Letztlich verweist der RbDatenschutz aber auch hier auf das einzelstaatliche Recht.

Das Auskunftsrecht des Betroffenen regelt der RbDatenschutz nur in wenigen Eckpunkten. Dies ist dem Umstand geschuldet, dass einige Mitgliedstaaten nach ihrem innerstaatlichen Recht dem Betroffenen nur ein indirektes Auskunftsrecht einräumen, das über die zuständige Datenschutzaufsichtsbehörde wahrzunehmen ist, während andere, so auch Deutschland, dem Betroffenen ein direktes Auskunftsrecht gewähren. An diesen systemischen Unterschieden ändert der RbDatenschutz nichts, da die Einzelheiten des Auskunftsanspruchs sich nach dem innerstaatlichen Recht richten.

Der RbDatenschutz geht in Artikel 23 davon aus, dass insbesondere von einer automatisierten Datenverarbeitung Risiken für die Grundrechte und Grundfreiheiten ausgehen und sieht vor der Verarbeitung personenbezogener Daten in neu zu errichtenden entsprechenden Dateien eine Vorabkonsultation der nationalen Datenschutzaufsichtsbehörden vor. Das Bundesrecht sieht eine Beteiligung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) dagegen vor allem für Zweifelsfälle vor; im Regelfall erfolgt die Vorabkontrolle behördenintern durch den behördlichen Datenschutzbeauftragten.

Unabhängige Kontrollstellen etabliert der RbDatenschutz als wesentliches Element des Schutzes personenbezogener Daten. An die Mitgliedstaaten ergeht in Erwägungsgrund 34 die Empfehlung, den nach der Richtlinie 95/46/EG errichteten Kontrollstellen auch diese Aufgabe zu übertragen.

Der RbDatenschutz lässt nach seinem Erwägungsgrund 38 bestehende Verpflichtungen der Mitgliedstaaten aufgrund von Übereinkünften mit Drittstaaten unberührt, verpflichtet die Mitgliedstaaten jedoch, bei zukünftigen Übereinkünften die Vorgaben des Rahmenbeschlusses zu beachten. Nach dem in den Erwägungsgründen 39 und 40 näher dargelegten Grundsatz der Spezifität gehen zudem insbesondere die Datenschutzvorschriften der Rechtsakte, die die Arbeitsweise von Europol, von Eurojust, des Schengener Informationssystems (SIS) und des Zollinformationssystems (ZIS) regeln, dem RbDatenschutz vor; gleiches gilt für die Datenschutzvorschriften, die die automatisierte Übermittlung von DNA-Profilen, daktyloskopischen Daten und Daten aus nationalen Fahrzeugregistern zwischen Mitgliedstaaten gemäß dem Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1), regeln.

III. Änderungsbedarf im deutschen Recht aufgrund des RbDatenschutz

Das geltende Bundesrecht enthält bereits zahlreiche bereichsspezifische Vorschriften zum Schutz personenbezogener Daten. Diese gewährleisten ein hohes Schutzniveau für in Deutschland bei Polizeibehörden, Staatsanwaltschaften und Strafgerichten verarbeitete personenbezogene Daten und verfolgen zumeist auch Regelungsansätze, die mit denen des RbDatenschutz identisch sind. In einigen Fällen wird der Grundrechtsschutz für die von der Datenverarbeitung Betroffenen jedoch auf andere Weise als im RbDatenschutz vorgesehen verwirklicht. In diesen Fällen besteht ein Änderungsbedarf im innerstaatlichen Recht.

Da der Anwendungsbereich des RbDatenschutz begrenzt ist auf bestimmte Fälle europäischer Zusammenarbeit, steht es dem nationalen Gesetzgeber frei, sein Datenschutzregime für den Bereich der Strafjustiz und Polizei insgesamt an das Regelungskonzept des RbDatenschutz anzupassen, oder zunächst an dem bewährten innerstaatlichen Regelungskonzept festzuhalten und die dem RbDatenschutz unterfallende Materie wo erforderlich gesondert zu regeln. Für eine einheitliche Regelung spricht ihre Anwenderfreundlichkeit durch den damit verbundenen Verzicht auf Sondertatbestände. Für eine differenzierende Umsetzung des RbDatenschutz spricht, dass das Regelungskonzept des Rahmenbeschlusses in der deutschen Rechtsordnung nicht erprobt ist, nach Artikel 27 RbDatenschutz selbst unter Evaluierungsvorbehalt steht und der Rahmenbeschluss zudem nach den derzeitigen Planun-

gen der Europäischen Union durch eine „Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“ abgelöst werden soll (vgl. Artikel 58 des entsprechenden von der Europäischen Kommission am 25. Januar 2012 vorgelegten Richtlinienentwurfs). Eine gesonderte innerstaatliche Regelung der dem RbDatenschutz unterfallenden Materie gestattet es, vor einer Entscheidung über die allgemeine Einführung einer neuartigen Regelung deren Auswirkungen zunächst in einem begrenzten Anwendungsbereich innerstaatlich zu beobachten.

Artikel 1 RbDatenschutz beschreibt den Zweck und den Anwendungsbereich des Rahmenbeschlusses. Nach Artikel 1 Absatz 1 ist es Zweck des RbDatenschutz, bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen gemäß Titel VI des Vertrags über die Europäische Union (EUV) zum einen hohen Schutz der Grundrechte und Grundfreiheiten natürlicher Personen (insbesondere ihres Rechts auf Privatsphäre) sowie zum anderen gleichzeitig ein hohes Maß an öffentlicher Sicherheit zu gewährleisten. Der in Bezug genommene Titel VI wurde mit Inkrafttreten des Vertrags von Lissabon aufgehoben und in den Dritten Teil Titel V des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) integriert.

Der RbDatenschutz erfasst nach seinem Artikel 1 Absatz 3 sowohl die automatisierte Verarbeitung personenbezogener Daten als auch die nicht-automatisierte Verarbeitung solcher personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Datei ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind. Hierzu gehören zum Beispiel die DNA-Datei, aber auch Registraturprogramme und das Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV), wobei die Datenverarbeitung in entsprechenden Dateien in heutiger Zeit in aller Regel automatisiert erfolgt. Auch sofern Akten bereits elektronisch geführt oder eingescannt werden, findet eine automatisierte Datenverarbeitung statt. Spezielle Dateiregelungen finden sich im nationalen Strafprozessrecht dabei in den §§ 483 ff. StPO.

Keine Dateien sind hingegen die bisher in Papierform geführten Ermittlungs- und Strafakten der Polizei, des Zollfahndungsdienstes und der Justizbehörden. Selbst bei einer gewissen Strukturierung einer umfangreichen Akte sind einzelne personenbezogene Daten (z. B. Name, Größe, Augenfarbe) nicht nach bestimmten Kriterien strukturiert und ohne besondere Kenntnis der Akte nicht ohne weiteres auffindbar und zugänglich. Daher fallen in Papierakten enthaltene Daten nicht unter den RbDatenschutz. Das gilt auch für Daten, die im Ausland elektronisch verarbeitet wurden und in Deutschland lediglich in eine Papierakte gelangen. Es erscheint weder sachgerecht noch erforderlich, auf diese Daten andere datenschutzrechtliche Vorschriften anzuwenden als für den restlichen Akteninhalt. Auch wenn Daten aus einer Akte ins Ausland (elektronisch) übermittelt werden und dort ggf. automatisiert verarbeitet werden, unterfällt die Akte sodann nicht dem Anwendungsbereich des RbDatenschutz. Der Rahmenbeschluss bezieht sich in diesen Fällen nur auf das isolierte, übermittelte Datum, nicht aber auf die Akte, aus der das Datum stammt oder die Akte, in die ein übermitteltes Datum aufgenommen wird.

Nach seinem Artikel 1 Absatz 4 gilt der RbDatenschutz für nachrichtendienstliche Tätigkeiten nicht; er lässt zudem die wesentlichen nationalen Sicherheitsinteressen unberührt.

Artikel 1 Absatz 5 RbDatenschutz stellt zudem klar, dass der Rahmenbeschluss lediglich den Mindeststandard der Datenschutzbestimmungen vorgibt, d. h. nur den zumindest zu gewährleistenden Schutzumfang festlegt. Er hindert die Mitgliedstaaten nicht daran, auf nationaler Ebene erhobene oder verarbeitete personenbezogene Daten durch strengere Bestimmungen zu schützen.

Artikel 2 RbDatenschutz enthält Begriffsbestimmungen. Der Begriff „personenbezogene Daten“ (Buchstabe a) wird im Wesentlichen deckungsgleich mit dem deutschen innerstaatlichen Recht verwandt.

Unter „Verarbeitung personenbezogener Daten“ und „Verarbeitung“ (Buchstabe b) wird jeder Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten bezeichnet. Der Begriff der Verarbeitung entspricht also dem der Datenschutzrichtlinie 95/46/EG und ist mithin weiter als der deutsche Verarbeitungsbegriff, der nur das Speichern, Verändern, Übermitteln, Sperren und Löschen umfasst (vgl. § 3 Absatz 4 des Bundesdatenschutzgesetzes (BDSG)), nicht aber das Erheben und das sonstige Nutzen von Daten. Aus dieser Divergenz ergibt sich kein besonderer Umsetzungsbedarf; der Gesetzentwurf hat allerdings die innerstaatlich verwandte Diktion zu berücksichtigen.

Die Definitionen der Begriffe „Sperrung“ (Buchstabe c), „Datei“ (Buchstabe d), „Auftraggeber“ (Buchstabe e), „Empfänger“ (Buchstabe f), „Einwilligung der betroffenen Person“ (Buchstabe g) und „Anonymisieren“ (Buchstabe k) entsprechen im Wesentlichen ihrem Gebrauch im innerstaatlichen Recht.

In Artikel 2 Buchstabe i RbDatenschutz wird der „für die Verarbeitung Verantwortliche“ definiert. Hierbei handelt es sich um die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Diese Begriffsbestimmung entspricht derjenigen des Artikels 2 Buchstabe d der Richtlinie 95/46/EG, die leicht abweichend in § 3 Absatz 7 BDSG mit der Definition „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“ umgesetzt wurde. Änderungsbedarf ergibt sich aus dieser Definition nicht; sie ist insbesondere vereinbar mit den besonderen Festlegungen in § 12 BKAG zur verantwortlichen Stelle im polizeilichen Informationssystem und der entsprechenden Regelung in § 12 ZFdG zur verantwortlichen Stelle im Zollfahndungsinformationssystem.

Eine „Kennzeichnung“ (Buchstabe j) ist nach dem RbDatenschutz die Markierung gespeicherter personenbezogener Daten, ohne dass damit das Ziel verfolgt wird, ihre künftige Verarbeitung einzuschränken. Eine Kennzeichnungsvorschrift enthält der RbDatenschutz in Artikel 18 Absatz 2 für den Fall des Bestreitens der Richtigkeit eines Datums. Damit werden dem Begriff der Kennzeichnung im RbDatenschutz Fälle zugeordnet, die im innerstaatlichen Datenschutzrecht der Sperrung unterfallen (vgl. § 35 Absatz 4 BDSG). „Sperrung“ im Sinne des § 3 Absatz 4 Satz 2 Nummer 4 BDSG ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken. Der Begriff der „Kennzeichnung“ wird im Bundesdatenschutzgesetz nicht definiert, sondern vorausgesetzt. Verwandt wird er als Oberbegriff, unter den auch „Sperrung“ fällt. Damit hat er denselben Bedeutungsgehalt wie „Markierung“ im RbDatenschutz. Regelungstechnische Konsequenzen ergeben sich aus diesen Abweichungen nicht.

Die „zuständige Behörde“ (Buchstabe h) wird schließlich definiert als durch Rechtsakt errichtete Agentur oder Einrichtung sowie Polizei-, Zoll-, Justiz- oder sonstige Behörde der Mitgliedstaaten, die nach innerstaatlichem Recht ermächtigt sind, personenbezogene Daten im Anwendungsbereich dieses Rahmenbeschlusses zu verarbeiten.

Artikel 3 RbDatenschutz enthält die wesentlichen Grundsätze der Rechtmäßigkeit, der Verhältnismäßigkeit und der Zweckbindung für die Datenverarbeitung und -nutzung nach dem Rahmenbeschluss. Die in Artikel 3 normierten Grundsätze bedürfen keiner Umsetzung. Sie sind im Bundesrecht entweder expressis verbis als solche verankert oder werden seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 aus dem Grundrecht auf informationelle Selbstbestimmung abgeleitet (BVerfGE 65, 1, 46) und haben ihren Niederschlag in den einschlägigen Vorschriften über die Datenerhebung, -verarbeitung und -nutzung gefunden.

Artikel 4 RbDatenschutz enthält Regelungen zur Berichtigung, Löschung und Sperrung von Daten. Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind, zu löschen oder zu anonymisieren, wenn sie nicht mehr erforderlich sind, bzw. zu sperren, wenn schutzwürdige Interessen der betroffenen Person einer Löschung entgegenstehen. Diese Regelungen entsprechen denen der § 32 BKAG, § 35 BPolG und § 39 ZFdG, die unter gleichen Voraussetzungen eine Pflicht zur Berichtigung, Löschung, Anonymisierung oder Sperrung vorsehen. § 32 Absatz 2 Satz 2 Nummer 2 BKAG, § 35 Absatz 6 Nummer 2 BPolG und § 39 Absatz 2 Satz 2 Nummer 2 ZFdG, die anstelle einer Löschung die Sperrung von Daten erlauben, sofern sie noch für laufende Forschungsarbeiten benötigt werden, sind ebenfalls mit Artikel 4 Absatz 2 RbDatenschutz vereinbar. Die Nutzung zu Forschungszwecken ist gemäß Artikel 3 Absatz 2 Satz 2 RbDatenschutz eine rechtmäßige Weiterverarbeitung im Sinne des Artikels 4 Absatz 2 RbDatenschutz.

Entsprechendes gilt in Anbetracht der §§ 489 und 494 StPO auch für das Strafverfahren, so dass hier die Vorgaben zur Berichtigung, Löschung und Sperrung in Dateien gespeicherter Daten ebenfalls bereits umgesetzt sind. Personenbezogene Daten in Verfahrensakten sind zu löschen bzw. die Akte ist zu vernichten, wenn die gesamte Akte für die Aufgabenerfüllung nicht mehr erforderlich ist. Unrichtige Daten in einer Verfahrensakte werden nach den geltenden Grundsätzen der Aktenwahrheit und -vollständigkeit durch einen entsprechenden Vermerk berichtigt. Die Berichtigung unrichtiger Daten in einem Gerichtsbeschluss oder einem Gerichtsprotokoll erfolgt gemäß Artikel 4 Absatz 4 RbDatenschutz nach Maßgabe der nationalen Prozessordnung. Die nach Artikel 4 Absatz 2 RbDatenschutz anstelle der Löschung mögliche Anonymisierung nicht mehr erforderlicher Daten ist für den Bereich der Forschung durch § 476 Absatz 6 StPO (ggf. i. V. m. § 487 Absatz 4 Satz 2 StPO) geregelt.

§ 32 Absatz 2 Satz 2 Nummer 3 BKAG, § 25 Absatz 6 Nummer 3 BPolG, § 39 Absatz 2 Satz 2 Nummer 3 ZFdG und § 35 Absatz 6 Nummer 3 BPolG und § 489 Absatz 7 Nummer 3 StPO sowie der für das ZStV auf diese zuletzt

genannte Vorschrift verweisende § 494 Absatz 3 StPO sind ebenfalls mit Artikel 4 RbDatenschutz vereinbar. Diese Normen erlauben anstelle einer Löschung auch dann eine Sperrung, wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Diese Regelungen entsprechen § 35 Absatz 3 Nummer 3 BDSG und tragen dem Umstand Rechnung, dass eine Löschung nach dem innerstaatlichen Recht die Unkenntlichmachung der gespeicherten Informationen bewirken muss. Dabei muss es sich um einen irreversiblen Prozess handeln, der die Entfernung der Signale eines Datensatzes, die Zerstörung des Datenträgers oder die irreversible Löschung der Verknüpfung zweier Datenteilmengen beinhaltet (vgl. Dammann in Simitis [Hrsg.], Bundesdatenschutzgesetz, 6. Auflage, § 3, Rn. 177 ff.). Das Löschungsgebot wird hingegen nicht durch eine bloße Änderung der Datenorganisation erfüllt, die einen gezielten Zugriff zwar ausschließt oder erschwert, aber die Information selbst nicht zum Verschwinden bringt. Da einfache Löschfunktionen von Computersoftware lediglich die Verknüpfung mit der Information, aber nicht die Information selbst beseitigen, ist in deren Nutzung regelmäßig keine Löschung zu sehen. Diese Anforderungen an die Löschung bedingen es, dass eine Löschung bestimmter Datensätze etwa aus einer Sicherungskopie unter Umständen technisch nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. In diesen Fällen ist dem Löschungsgebot im Sinne des RbDatenschutz jedoch mit einer Sperrung im Sinne der bezeichneten Normen ausreichend genüge getan, da diese dazu führt, dass die Daten nicht mehr verarbeitet werden dürfen.

Gesperrte Daten dürfen über die Zweckbindung des Artikels 4 Absatz 3 Satz 2 RbDatenschutz hinaus gemäß § 489 Absatz 7 Satz 4 StPO auch zur Behebung einer bestehenden Beweisnot verwendet werden. Damit wird einer notstandsähnlichen Situation Rechnung getragen, in der ausschließlich durch die in der Datei enthaltenen Informationen der erforderliche Beweis erlangt werden kann, gleichwohl hierdurch aber ein abweichender als der den Anlass der Sperrung bildende Zweck verfolgt wird. In europarechtsfreundlicher Auslegung ist diese Ausnahme für Daten, die aus einem anderen Mitgliedstaat übermittelt wurden, auf eine Beweisnot zu Lasten des Betroffenen zu beschränken. Sollten die Daten des Betroffenen nicht zum Schutz seiner Interessen, sondern zum Beispiel zu Zwecken der Datensicherung gesperrt und noch nicht gelöscht worden sein, entspricht es dem Rechtsgedanken des Artikels 4 Absatz 3 RbDatenschutz, dass der Betroffene seine Daten für eigene Zwecke verwenden kann und ihm seine Daten nicht aus formalen Gründen vorenthalten werden.

Der vorgenannten Regelung der Strafprozessordnung entsprechende Regelungen zur Behebung einer Beweisnot finden sich in den § 32 Absatz 2 Satz 3, § 33 Absatz 4 BKAG, § 35 Absatz 7 BPolG und § 39 Absatz 2 Satz 3 ZFdG. Die Abwendung einer notstandsähnlichen Situation wird auch beabsichtigt, wenn darüber hinaus die zweckändernde Nutzung der gesperrten personenbezogenen Daten zur Abwehr einer erheblichen Gefahr für zulässig erklärt wird (§ 33 Absatz 4 BKAG, § 35 Absatz 7 BPolG). Auch in diesen Fällen sind daher in europarechtsfreundlicher Auslegung die Verwendungsbefugnisse für Daten, die aus einem anderen Mitgliedstaat übermittelt wurden, auf eine Beweisnot zu Lasten des Betroffenen zu beschränken.

Artikel 5 RbDatenschutz bestimmt, dass Löschungs- und Prüffristen festzulegen sind. Durch verfahrensrechtliche Vorkehrungen ist sicherzustellen, dass diese Fristen eingehalten werden. Diese Vorgaben werden durch das Bundesrecht erfüllt (im Strafprozessrecht insbesondere durch § 489 Absatz 2 bis 5, § 490 Satz 1 Nummer 7, § 494 Absatz 2 StPO).

Artikel 6 RbDatenschutz enthält an die Richtlinie 95/46/EG angelehnte Bestimmungen zur Verarbeitung besonderer Kategorien personenbezogener Daten löst jedoch weder für das Polizei- noch das Strafprozessrecht Umsetzungsbedarf aus. Nach Artikel 6 RbDatenschutz ist 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 nur zulässig, wenn dies unbedingt notwendig ist und das innerstaatliche Recht einen angemessenen Schutz gewährleistet. Das geltende Polizei- und Strafprozessrecht entspricht im Ergebnis diesen Anforderungen:

Die von Artikel 6 RbDatenschutz in Bezug genommenen besonderen Kategorien personenbezogener Daten sind in der polizeilichen und staatsanwaltschaftlichen Arbeit nicht selten relevant, etwa bei der Verfolgung von Sexual- oder extremistischen Straftaten. Die Erhebung und Verarbeitung solcher Daten ist im deutschen Recht schon nach dem Grundsatz der Verhältnismäßigkeit generell nur zulässig, wenn dies zur Aufgabenwahrnehmung unbedingt erforderlich ist. Im Rahmen der Verhältnismäßigkeitsprüfung ist zudem eine Verarbeitung besonderer Kategorien personenbezogener Daten stärker zu gewichten, wenn diese Daten einem speziellen Grundrechtsschutz unterfallen, etwa dem Intimbereich zuzuordnen sind, woraus sich gegebenenfalls Einschränkungen bei der Datenverarbeitung ergeben können.

Auch die Dateiregelungen des Polizeirechts und der Strafprozessordnung gewährleisten einen angemessenen Schutz. Bei der Errichtung von Dateien sind gemäß § 34 Absatz 1 BKAG, § 36 Absatz 1 BPolG, § 41 Absatz 1 ZFdG sowie § 490 Satz 1 StPO die Art der zu speichernden Daten sowie die Voraussetzungen festzulegen, unter denen die in der Datei verarbeiteten Daten an bestimmte Empfänger in bestimmten Verfahren übermittelt werden dürfen. Ergänzt wird der Schutz durch die bestehenden Rechte des Betroffenen auf Auskunft und Löschung, einschließlich der Möglichkeit, um gerichtlichen Rechtsschutz nachzusuchen.

Artikel 7 RbDatenschutz zu automatisierten Einzelentscheidungen geht ebenfalls über die Beschränkungen, die nach Bundesrecht gelten, nicht hinaus und löst deshalb keinen Umsetzungsbedarf aus. Im Strafverfahren gibt es keine Verfahren, bei denen die nachteilige Entscheidung unmittelbar aus der automatisierten Datenauswertung resultiert. Eine Entscheidung mit nachteiliger Rechtsfolge geht immer auf das Tätigwerden einer natürlichen Person zurück, die die Daten bewertet und eine Entscheidung trifft.

Artikel 8 RbDatenschutz enthält Regelungen zur Sicherung der Datenqualität. Nach seinem Absatz 1 trägt die übermittelnde Behörde dafür Sorge, dass die Daten richtig, vollständig und aktuell sind. Zu diesem Zwecke hat sie die Daten vor einer Übermittlung zu überprüfen sowie nach Absatz 1 Satz 3 bei jeder Übermittlung von Daten nach Möglichkeit Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, Vollständigkeit, Aktualität und Zuverlässigkeit der Daten zu beurteilen.

Die Richtigkeit der verwendeten Daten gehört zu den international anerkannten Grundsätzen der Datenverarbeitung und wird – wie auch die Mitteilungspflicht bei Übermittlung unrichtiger Daten – für Datenübermittlungen nach dem Bundeskriminalamtgesetz durch § 32 Absatz 1 und § 33 Absatz 1 BKAG bzw. § 32 Absatz 6 und § 33 Absatz 6 BKAG, für Datenübermittlungen nach dem Bundespolizeigesetz durch § 35 Absatz 1 und 8 BPolG und für Übermittlungen nach dem Zollfahndungsdienstgesetz durch § 39 Absatz 1 und § 40 Absatz 1 ZFdG bzw. § 39 Absatz 7 und § 40 Absatz 5 ZFdG gewährleistet. Umsetzungsbedarf besteht aber hinsichtlich der Pflicht aus Artikel 8 Absatz 1 Satz 3 RbDatenschutz, Informationen beizufügen, die auch dem Empfänger eine angemessene Überprüfung der Daten ermöglichen sollen.

Im IRG werden die Vorgaben aus Artikel 8 Absatz 1 Satz 1 bis 3 RbDatenschutz in § 97c Absatz 2 Nummer 1 und 2 IRG-E, aus Artikel 8 Absatz 1 Satz 4 RbDatenschutz in § 97b Absatz 4 IRG-E sowie aus Artikel 8 Absatz 2 Satz 1 RbDatenschutz in § 97c Absatz 2 Nummer 5 IRG-E umgesetzt.

Im Strafprozessrecht ist die aus Artikel 8 Absatz 1 Satz 4 RbDatenschutz folgende Verpflichtung, nach der die empfangende Behörde bei einer Datenübermittlung ohne vorheriges Ersuchen unverzüglich zu prüfen hat, ob sie die empfangenen Daten für den Zweck, für den sie übermittelt wurden, benötigt, eine Selbstverständlichkeit, die aus den §§ 160 und 163 StPO folgt. Für die Speicherung personenbezogener Daten in Dateien setzen die §§ 483 bis 485 StPO voraus, dass sie für Zwecke des Strafverfahrens, für Zwecke künftiger Strafverfahren oder für Zwecke der Vorgangsverwaltung erforderlich ist. Ein Umsetzungsbedarf ergibt sich daher aus Artikel 8 Absatz 1 Satz 4 RbDatenschutz für den Bereich des Strafverfahrens nicht.

Auch aus Artikel 8 Absatz 2 Satz 1 RbDatenschutz ergibt sich kein weiterer Umsetzungsbedarf in der Strafprozessordnung: „Empfänger“ im Sinne der Vorschrift ist die Stelle, der die Berichtigung von einem anderen Mitgliedstaat übermittelt wurde. Die Weiterleitung der Berichtigung innerhalb Deutschlands richtet sich dann nach dem nationalen Recht. Dieses sieht für Dateien in § 489 Absatz 8 StPO und § 494 Absatz 3 StPO vor, dass die speichernde Stelle dann, wenn sie die Unrichtigkeit von Daten erkennt, dies den Empfängern der Daten mitzuteilen hat, soweit dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist. Entsprechende ungeschriebene Grundsätze gelten auch für die Strafakte.

Die sich durch Artikel 8 Absatz 2 Satz 2 RbDatenschutz ergebende Verpflichtung, unrichtige oder unrechtmäßig übersandte Daten zu berichtigen, zu löschen oder zu sperren ist für das Strafverfahren, soweit es die Löschung unrichtiger Daten in Dateien betrifft, durch § 489 Absatz 1 StPO umgesetzt.

Artikel 8 Absatz 2 Satz 2 RbDatenschutz lässt offen, welche Alternative des Artikels 4 RbDatenschutz (Berichtigung, Löschung oder Sperrung) einschlägig sein soll, wenn ein Datum unrechtmäßig übersandt wurde. Aus der sich u. a. aus Artikel 3 Absatz 1 Satz 2 RbDatenschutz ergebenden Intention, die Verarbeitung personenbezogener Daten nur im Rahmen rechtmäßig erfolgender Datenverarbeitung zuzulassen, wird gefolgert werden können, dass eine Weiterverarbeitung unrechtmäßig übersandter Daten grundsätzlich unzulässig sein soll. Dies begründet nach § 489 Absatz 2 Satz 1 Alternative 1 StPO die Pflicht, solche Daten zu löschen, wobei unter den in § 489 Absatz 7 StPO genannten Voraussetzungen an die Stelle der Löschung eine Sperrung treten kann (vgl. dazu die obigen Erläuterungen zu Artikel 4 RbDatenschutz).

Sollten unrichtige oder unrechtmäßig übersandte Daten Eingang in eine Verfahrensakte gefunden haben, ist dies nach den geltenden Grundsätzen der Aktenwahrheit und -vollständigkeit in dieser zu vermerken, um so der vorstehend aufgezeigten, vom RbDatenschutz intendierten Weiterverarbeitungsbeschränkung Rechnung zu tragen.

Artikel 9 RbDatenschutz enthält weitere Regelungen zu Aufbewahrungsfristen und statuiert die Möglichkeit der übermittelnden Stelle, die Beachtung der nach innerstaatlichem Recht geltenden Fristen auch dem Empfängermitgliedstaat rechtsverbindlich aufzuerlegen. Eine derartige Verpflichtung zur Löschung, Sperrung oder Prüfung ist hinsichtlich Daten, die von anderen Mitgliedstaaten übermittelt worden sind, bislang im Bundeskriminalamtgesetz, Bundespolizeigesetz und Zollfahndungsdienstgesetz nicht vorgesehen, es besteht daher Umsetzungsbedarf.

Artikel 10 RbDatenschutz normiert Protokollierungs- und Dokumentationspflichten, die über das nach dem Bundeskriminalamtgesetz, auch in Verbindung mit dem Bundesdatenschutzgesetz, Geforderte nicht hinausgehen. § 33 Absatz 8 BPolG sowie § 11 Absatz 4 ZFdG sehen bislang jedoch statt einer Vollprotokollierung, welche durch Artikel 10 Absatz 1 RbDatenschutz gefordert wird, nur eine Protokollierung jedes zehnten Abrufs vor. Hier besteht daher Umsetzungsbedarf, dem durch die jeweils geänderte Formulierung in § 33 Absatz 8 Satz 1 BPolG-E und § 11 Absatz 4 Satz 1 ZFdG-E Rechnung getragen wird.

Für das Strafverfahren ist beim automatisierten Abrufverfahren nach § 488 Absatz 3 Satz 3 und § 493 Absatz 3 Satz 3 StPO ebenfalls nicht – wie durch Artikel 10 Absatz 1 RbDatenschutz gefordert – jede Übermittlung zu protokollieren, sondern es reicht die Protokollierung jedes zehnten Abrufes aus. Die protokollierten Daten dürfen zudem gemäß § 488 Absatz 3 Satz 5 und § 493 Absatz 3 Satz 4 StPO nur zur Kontrolle der Zulässigkeit der Abrufe verwendet werden, während Artikel 10 Absatz 1 i. V. m. Absatz 2 RbDatenschutz zusätzlich die Verwendung zur „Eigenüberwachung“ und zur „Sicherstellung der Integrität und Sicherheit der Daten“ vorsieht. Insoweit besteht daher Umsetzungsbedarf, dem durch die Änderungen in § 488 Absatz 3 Satz 3 bis 5 sowie § 493 Absatz 3 Satz 3 und 4 StPO-E Rechnung getragen wird.

Hinsichtlich der Übermittlung von personenbezogenen Daten, die nicht im automatisierten Verfahren erfolgt und für die die §§ 488 und 493 StPO deshalb keine Anwendung finden, ist eine gesonderte gesetzliche Vorgabe der Protokollierung nicht erforderlich. Entsprechende Übermittlungen nach § 487 Absatz 1 StPO oder Auskunftserteilungen nach § 487 Absatz 2 StPO werden bereits durch die Anfragen auf Übermittlung oder Auskunftserteilung und die daraufhin gegebenen Antworten zumindest in Form entsprechender Vermerke darüber in der Verfahrensakte dokumentiert. Denn für die Strafverfolgungsbehörden und Strafgerichte besteht eine Pflicht zur Aktenführung, auch wenn dies nicht ausdrücklich bestimmt ist. Diese Pflicht wird durch die Gebote der Aktenvollständigkeit und der wahrheitsgetreuen Aktenführung ausgefüllt. Die Akte ist die maßgebliche Erkenntnisquelle für das Handeln der Strafverfolgungsbehörden und Strafgerichte. Eine wahrheitsgemäße und vollständige Dokumentation aller Ermittlungsschritte ist eine unabdingbare Voraussetzung für die Nachvollziehbarkeit der durchgeführten Ermittlungen. Sie ist insbesondere auch Grundlage für die Nachprüfung der getroffenen Entscheidungen durch übergeordnete Behörden und/oder Gerichte.

Artikel 11 RbDatenschutz enthält Verwendungsbeschränkungen für personenbezogene Daten, die von einem anderen Mitgliedstaat übermittelt oder bereitgestellt worden sind. Danach ist die Verwendung zu anderen Zwecken als denjenigen, für die sie übermittelt oder bereitgestellt wurden, nur zulässig zur Verhütung, Ermittlung, Feststellung oder Verfolgung anderer Straftaten oder zur Vollstreckung von strafrechtlichen Sanktionen, für andere damit zusammenhängende justizielle und verwaltungsbehördliche Verfahren, die Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit oder jeden anderen Zweck, sofern der übermittelnde Staat oder die betroffene Person zugestimmt hat. Eine ausdrückliche Zweckbindung dieser Art ist dem Bundeskriminalamtgesetz in der geltenden Fassung fremd. Die Aufgabennormen der §§ 2 bis 6 BKAG und der §§ 3 bis 6 sowie 24 und 25 ZFdG dürften zwar regelmäßig mit diesen Voraussetzungen korrespondieren, doch sind Ausnahmen denkbar, die der Gesetzgeber beispielsweise in den Übermittlungsnormen des § 10 Absatz 2 Nummer 1 und des § 14 Absatz 1 Satz 1 Nummer 1 BKAG bzw. des § 33 Absatz 1 Nummer 1 und des § 34 Absatz 1 Satz 1 Nummer 1 ZFdG als Auffangtatbestände neben Strafverfolgung und Gefahrenabwehr berücksichtigt hat. Diesbezüglich besteht daher Änderungsbedarf im Hinblick auf die vom Rahmenbeschluss erfassten Daten. Außerdem differenzieren das Bundeskriminalamtgesetz und das Zollfahndungsdienstgesetz bislang nicht zwischen der Abwehr von Gefahren für strafrechtlich geschützte Rechtsgüter und solchen für sonstige Rechtsgüter der öffentlichen Sicherheit. Der Rahmenbeschluss indes privilegiert in Artikel 11 die Verhütung von Straftaten gegenüber der sonstigen

Gefahrenabwehr und zieht auch insoweit Änderungsbedarf im Bundeskriminalamtgesetz und dem Zollfahndungsdienstgesetz nach sich. Dem Bundespolizeigesetz in der geltenden Fassung ist eine entsprechende Zweckbindung fremd. Demnach besteht Änderungsbedarf im Hinblick auf die vom Rahmenbeschluss erfassten Daten.

Im IRG erfolgt die Umsetzung von Artikel 11 Satz 1 RbDatenschutz durch § 97b Absatz 1 IRG-E und diejenige von Artikel 11 Satz 2 RbDatenschutz durch § 97b Absatz 3 IRG-E.

Artikel 12 Absatz 1 RbDatenschutz bestimmt, dass die übermittelnde Behörde den Empfänger auf für sie geltende innerstaatliche Verwendungsbeschränkungen hinweist und der Empfänger die Einhaltung dieser Beschränkungen sicherstellt. Hierbei werden gemäß Artikel 12 Absatz 2 nur solche Verwendungsbeschränkungen angewendet, die auch für entsprechende innerstaatliche Datenübermittlungen gelten.

Dem Bundeskriminalamtgesetz, dem Bundespolizeigesetz und dem Zollfahndungsdienstgesetz sind vergleichbare Regelungen für nach den §§ 10 und 14 BKAG, § 32 BPolG sowie §§ 33, 34 und 34a ZFdG übermittelte Daten fremd. Erfolgt die Übermittlung allerdings im Rahmen völkerrechtlicher Verpflichtungen, so sehen viele der von der Bundesrepublik Deutschland mit Drittstaaten geschlossenen bereichsspezifischen Abkommen als geltendes Recht vor, dass die übermittelnde Stelle Bedingungen vorsehen kann, zu denen die Verwendung der Daten durch den Empfänger zu erfolgen hat. Der RbDatenschutz überträgt dieses Regelungsregime auf die europäische Ebene. Da der Rahmenbeschluss kein unmittelbar geltendes Recht darstellt, müssen seine Vorgaben im Recht der Mitgliedstaaten, so auch im Bundeskriminalamtgesetz, im Bundespolizeigesetz und im Zollfahndungsdienstgesetz umgesetzt werden.

Auch im IRG besteht in Bezug auf Artikel 12 Absatz 1 Satz 1 RbDatenschutz Umsetzungsbedarf, dem mit § 97c Absatz 2 Nummer 4 IRG-E nachgekommen wird.

Artikel 13 RbDatenschutz enthält Bestimmungen zur Weiterleitung an die zuständigen Behörden in Drittstaaten oder an internationale Einrichtungen. Wie schon für die Verwendung im Allgemeinen gelten auch bei der Übermittlung von Daten, die von der zuständigen Behörde eines anderen Mitgliedstaates im Anwendungsbereich des RbDatenschutz übermittelt wurden, Zweckbeschränkungen. Eine Weiterleitung an Drittstaaten kommt allerdings zum Zwecke der Gefahrenabwehr nur noch in Betracht, wenn es sich dabei um die Verhütung von Straftaten handelt. Andere Übermittlungszwecke als die Verhütung oder Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen erkennt der RbDatenschutz in diesem Zusammenhang nicht an, während § 14 Absatz 1 Nummer 3 BKAG bzw. § 34 Absatz 1 Nummer 3 ZFdG eine Übermittlung in das Ausland zur Abwehr einer jeden im Einzelfall bestehenden erheblichen Gefahr für die öffentliche Sicherheit ermöglicht, sofern die übrigen Voraussetzungen, darunter ein angemessenes Datenschutzniveau im Empfängerstaat, das auch Artikel 13 Absatz 1 Buchstabe d RbDatenschutz voraussetzt, vorliegen. Eine vergleichbare Regelung trifft § 32 Absatz 3 BPolG. Insoweit besteht daher Umsetzungsbedarf für Artikel 13 RbDatenschutz in § 14 BKAG, § 32 BPolG und § 34 ZFdG.

Artikel 13 Absatz 1 Buchstabe c RbDatenschutz statuiert ein Zustimmungserfordernis zugunsten des Mitgliedstaates, der die Daten ursprünglich übermittelte. Ausnahmen hierzu sieht Artikel 13 Absatz 2 RbDatenschutz vor. Danach ist eine Weiterleitung ohne Zustimmung nur zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit zulässig. Dem Zustimmungserfordernis kann freilich im Einklang mit den Erwägungsgründen auch generalisiert entsprochen werden, indem die übermittelnde Behörde ihre Zustimmung für bestimmte Übermittlungszwecke oder Drittländer allgemein erteilt. Dennoch muss bei einer Übermittlung (von den Ausnahmen abgesehen) die – allgemein oder im Einzelfall erteilte – Zustimmung vorliegen. Das Bundeskriminalamtgesetz bzw. Zollfahndungsdienstgesetz sieht bislang nur vor, dass das Bundeskriminalamt bzw. Zollkriminalamt auf Basis einer Einzelfallbeurteilung prüft, ob die Annahme begründet ist, dass durch die Übermittlung von Daten der der Erhebung dieser Daten zugrundeliegende Zweck gefährdet würde, und holt nur bejahendenfalls die Zustimmung der Stelle ein, von der die Daten übermittelt wurden. Für den Anwendungsbereich des Rahmenbeschlusses ist daher sicherzustellen, dass diese Rechtsfolge generell zur Anwendung kommt. In das Bundespolizeigesetz ist eine entsprechende Regelung neu einzufügen.

Die Vorgaben aus Artikel 13 RbDatenschutz werden im IRG in § 97d IRG-E umgesetzt.

In Artikel 14 RbDatenschutz werden Regelungen zur Übermittlung an nicht-öffentliche Stellen in den Mitgliedstaaten festgelegt. Auch hier besteht nach Artikel 14 Absatz 1 RbDatenschutz ein Zustimmungserfordernis, das nur die zu Artikel 13 dargelegte teilweise Entsprechung im Bundeskriminalamtgesetz und im Zollfahndungsdienstgesetz und keine im Bundespolizeigesetz findet. Darüber hinaus dürfen überwiegende schutzwürdige Interessen der betroffenen Person nicht entgegenstehen und die Weiterleitung im Einzelfall muss für die zuständige Behörde, die die Daten an eine nicht-öffentliche Stelle weiterleitet, aus den in Artikel 14 Absatz 1 Buchstabe c

RbDatenschutz genannten Gründen unerlässlich sein. Dadurch werden strenge Anforderungen an die Weitergabe der Daten aufgestellt. Die Umsetzung dieser Vorgaben erfolgt durch § 10 Absatz 3 BKAG-E, § 33 Absatz 2a BPolG-E sowie § 34a Absatz 7 ZFdG-E.

Die Hinweispflicht des Artikels 14 Absatz 2 RbDatenschutz ist bereits in § 10 Absatz 6 Satz 3 BKAG verwirklicht. Eine entsprechende Regelung fehlt bisher im Zollfahndungsdienstgesetz und ist im § 33 Absatz 3 neu anzufügen.

Im IRG werden die Vorgaben aus dem Erwägungsgrund 18 sowie aus Artikel 14 RbDatenschutz in § 97b Absatz 2 IRG-E umgesetzt.

In der Strafprozessordnung besteht nach der Neuregelung in § 97b Absatz 2 IRG-E im Ergebnis kein weiterer aus Artikel 14 RbDatenschutz folgender Umsetzungsbedarf. Zunächst erfasst Artikel 14 RbDatenschutz ausweislich des Erwägungsgrunds 18 die Fälle nicht, in denen die Strafverfolgungsbehörden und Strafgerichte ihnen von Behörden der Mitgliedstaaten übermittelte personenbezogene Daten zur Sachverhaltsaufklärung einsetzen, indem sie von sonstigen Stellen Auskünfte verlangen und ihnen dazu notwendigerweise personenbezogene Daten mitteilen müssen (z. B. Sachverhaltsschilderungen oder Namen von Beschuldigten). Dies ist auch insofern konsequent, als nach Satz 2 des Erwägungsgrunds 11 die mit dem Rahmenbeschluss verfolgten Ziele und die dazu aufgestellten Vorgaben die rechtmäßigen Tätigkeiten der Polizei-, Zoll-, Justiz- und sonstigen zuständigen Behörden in keiner Weise behindern sollen.

Erwägungsgrund 18 hebt des Weiteren hervor, dass Artikel 14 RbDatenschutz auf die Auskunftsrechte von „Privaten“ als auch sonstigen Stellen (siehe die englische Textfassung „private parties“) im Strafverfahren nicht anwendbar ist, wobei als „private party“ beispielhaft Opfer und Verteidiger genannt werden. Nicht unter Artikel 14 RbDatenschutz fallen damit die Akteneinsichts- und Auskunftsrechte nach den §§ 147 und 406e StPO oder auch nach der – über § 487 Absatz 2 StPO auch bei Dateien Anwendung findenden – Regelung des § 475 StPO zur Übermittlung personenbezogener Daten an Privatpersonen und sonstige Stellen, sofern das von § 475 StPO vorausgesetzte berechtigte Interesse der Privatperson oder sonstigen Stelle an der Auskunftserteilung im Zusammenhang mit dem Strafverfahren steht. Das berechtigte Interesse der Privatperson oder sonstigen Stelle wird durch das Recht auf informationelle Selbstbestimmung des von einer Auskunft Betroffenen von vornherein begrenzt (vgl. § 475 Absatz 1 Satz 2 StPO). Ein allgemeines Informationsbedürfnis begründet noch kein berechtigtes Interesse an der Auskunftserteilung im Sinne des § 475 Absatz 1 Satz 1 StPO. Schließlich zeigt Erwägungsgrund 17, dass vom Anwendungsbereich des Artikels 14 RbDatenschutz offenbar insbesondere Mitteilungen von Amts wegen erfasst werden sollen. Als Beispiele hierfür sind Warnmeldungen zu gefälschten Wertpapieren an Banken und Kreditinstitute oder im Bereich der Kfz-Kriminalität an Versicherungsunternehmen, um unter anderem einen ungesetzlichen Handel mit gestohlenen Kraftfahrzeugen zu verhindern, genannt. Eine entsprechende Befugnis zur Übermittlung personenbezogener Daten an nicht-öffentliche Stelle von Amts wegen enthalten die Strafprozessordnung und das Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) hingegen nicht.

Artikel 15 RbDatenschutz normiert, dass der Empfänger auf Antrag die zuständige Behörde über die weitere Verarbeitung der Daten unterrichtet. Eine entsprechende Regelung ist bereits in dem bisherigen § 27a Absatz 2 BKAG enthalten, der durch das Gesetz zur Umsetzung des Rahmenbeschlusses 2006/960/JI über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (BGBl. I, S. 1566) eingefügt wurde. Der Anwendungsbereich dieser Vorschrift ist anzupassen. Da das Bundespolizeigesetz und das Zollfahndungsdienstgesetz eine solche Regelung nicht enthalten, besteht auch dort Umsetzungsbedarf.

Artikel 16 RbDatenschutz betrifft die Information des Betroffenen über die Erhebung oder Verarbeitung personenbezogener Daten. Mit der Formulierung „im Einklang mit dem innerstaatlichen Recht“ macht der RbDatenschutz deutlich, dass sich der Umfang der Informationspflicht nach innerstaatlichem Recht bemisst. Wie sich auch aus Erwägungsgrund 26 ergibt, ist Artikel 16 Absatz 1 RbDatenschutz nicht so zu verstehen, als setze er die Benachrichtigung des Betroffenen auch bei Maßnahmen geringerer Eingriffsintensität voraus. Die Voraussetzungen einer Benachrichtigungspflicht zu normieren überlässt er vielmehr dem nationalen Gesetzgeber.

Das Bundeskriminalamtgesetz verfügt über eine Anzahl von Benachrichtigungspflichten (vgl. § 16 Absatz 5, §§ 20w, 31 BKAG). Das Zollfahndungsdienstgesetz enthält ebenso bereits an mehreren Stellen eine Anzahl Benachrichtigungspflichten (vgl. § 18 Absatz 5, § 20 Absatz 5, § 21 Absatz 5, § 22 Absatz 4, § 22a Absatz 4, § 23c Absatz 4 ZFdG und die §§ 28 bis 32a ZFdG, die entsprechende Verweise auf § 18 ZFdG enthalten). Für den Bereich des Bundespolizeigesetzes ergeben sich die Benachrichtigungspflichten aus dem Bundesdatenschutzgesetz. Die Strafprozessordnung enthält ebenfalls Informationspflichten, so z. B. in § 101 Absatz 4 StPO die Pflicht

zur Benachrichtigung von Personen, die von den in § 101 Absatz 1 StPO genannten heimlichen Ermittlungsmaßnahmen betroffen waren. Wird ein DNA-Identifizierungsmuster eines Beschuldigten, das gemäß § 81e Absatz 1 StPO zum Abgleich mit Spurenmaterial erhoben wurde, gemäß § 81g Absatz 5 Satz 2 Nummer 1 StPO in die DNA-Analyse-Datei eingestellt, ist der Beschuldigte hierüber gemäß § 81g Absatz 5 Satz 4 StPO zu benachrichtigen. Soweit Betroffene nach Erwägungsgrund 27 Kenntnis davon erlangen sollen, in welchen Fällen Daten aus einem Strafverfahren ins Ausland übermittelt werden dürfen, ergibt sich dies in Deutschland (wie von Satz 3 des Erwägungsgrunds für zulässig erklärt) unmittelbar aus den entsprechenden Vorschriften des Gesetzes über die internationale Rechtshilfe in Strafsachen. Im Ergebnis kann es daher bei der bestehenden nationalen Rechtslage verbleiben, nach der einzelfallbezogen im Wesentlichen nur über verdeckt erfolgte Datenerhebungen und -verwendungen informiert wird. Ein Änderungsbedarf besteht daher nicht.

Umsetzungsbedarf besteht aber hinsichtlich Artikel 16 Absatz 2 RbDatenschutz. Dieser ermächtigt einen Mitgliedstaat in Fällen der Übermittlung personenbezogener Daten zwischen Mitgliedstaaten, einen anderen Mitgliedstaat zu ersuchen, den Betroffenen nicht zu informieren. Das Ersuchen bindet den ersuchten Mitgliedstaat.

Die Benachrichtigungspflichten nach den Vorschriften des Bundeskriminalamtgesetzes und des Zollfahndungsdienstgesetzes treten grundsätzlich erst bei Nichtvorliegen bestimmter Negativvoraussetzungen ein (zum Beispiel keine Gefährdung des Untersuchungszwecks, des Zwecks der Maßnahme, der öffentlichen Sicherheit oder der Aufgabenerfüllung), binden dann allerdings das Bundeskriminalamt bzw. das Zollkriminalamt und eröffnen kein Ermessen. Ausnahmen, nach denen die Benachrichtigung auch unterbleibt, wenn der übermittelnde Mitgliedstaat darum ersucht hat, kennen das Bundeskriminalamtgesetz und das Zollfahndungsdienstgesetz nicht. Hier liegt allerdings keine Unvereinbarkeit mit dem RbDatenschutz vor, denn die nach dem Bundeskriminalamtgesetz bzw. dem Zollfahndungsdienstgesetz die Benachrichtigungspflichten auslösenden Tatbestände – zumeist heimliche Datenerhebungen – werden nur in einem Fall – der Benachrichtigung über die Speicherung von Daten Strafunmündiger gemäß § 31 BKAG – mögliche Überschneidungen mit dem Anwendungsbereich des RbDatenschutz aufweisen. § 31 BKAG enthält allerdings eine weite Negativvoraussetzung, die die Fälle der europäischen Zusammenarbeit mit umfasst. Umsetzungsbedarf besteht nicht.

Praktisch bedeutsamer dürften die Fälle sein, in denen im Inland keine Benachrichtigungspflicht besteht, in einem anderen Mitgliedstaat aber doch. Hier ist eine klarstellende Befugnisnorm für Ersuchen nach Artikel 16 Absatz 2 RbDatenschutz erforderlich.

Artikel 17 RbDatenschutz normiert ein antragsbedingtes Auskunftsrecht des Betroffenen und entspricht damit in weiten Teilen § 19 BDSG, der auch im Rahmen der Datenverarbeitung nach dem Bundeskriminalamtgesetz und dem Zollfahndungsdienstgesetz anwendbar ist. § 19 Absatz 4 BDSG enthält eine nach Artikel 17 Absatz 2 RbDatenschutz zulässige Beschränkung der Auskunftserteilung. Auch im Hinblick auf Begründungserfordernis und Rechtsbehelfsbelehrung besteht kein Umsetzungsbedarf.

Im Strafprozessrecht sind Auskunftsrechte des Betroffenen in § 491 StPO für in Dateien und in § 495 StPO für die im ZStV gespeicherten personenbezogenen Daten vorgesehen, ebenfalls unter jeweiliger Bezugnahme auf § 19 BDSG. Das in Artikel 17 Absatz 1 Buchstabe a RbDatenschutz vorgesehene Recht betroffener Personen auf Auskunft (Bestätigung, dass sie betreffende Daten übermittelt oder bereitgestellt wurden oder nicht, sowie Informationen über die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben wurden, und eine Mitteilung über die Daten, die Gegenstand der Verarbeitung sind) wird somit über § 19 Absatz 1 Satz 1 BDSG sicher gestellt, der über § 491 Absatz 1 Satz 1 bzw. § 495 Satz 1 StPO entsprechende Anwendung findet.

Eine Umsetzung der in Artikel 17 Absatz 1 Buchstabe b RbDatenschutz vorgesehenen Alternative, eine Bestätigung von der nationalen Kontrollstelle zu erhalten, dass alle erforderlichen Überprüfungen durchgeführt wurden, bedarf es daher nicht. Die in § 491 Absatz 1 Satz 2 bis 4 StPO vorgesehenen Ausnahmen von der Pflicht zur Auskunftserteilung, auf die auch § 495 StPO verweist, entsprechen – ebenso wie die in § 19 Absatz 4 BDSG vorgesehenen Versagungsgründe – den in Artikel 17 Absatz 2 RbDatenschutz vorgesehenen Beschränkungsmöglichkeiten, insbesondere um behördliche oder gerichtliche Ermittlungen, Untersuchungen oder Verfahren nicht zu behindern bzw. die Verfolgung von Straftaten nicht zu beeinträchtigen (Artikel 17 Absatz 2 Buchstaben a und b RbDatenschutz).

Da die Versagung nur in den in Artikel 17 Absatz 2 RbDatenschutz genannten Fallgruppen möglich ist, kann die nach Artikel 17 Absatz 3 Satz 2 RbDatenschutz vorgesehene Mitteilung der tatsächlichen oder rechtlichen Gründe, auf die eine Verweigerung oder Einschränkung einer Auskunft gestützt wird, gemäß Artikel 17 Absatz 3 Satz 3 RbDatenschutz unterbleiben. Ein Umsetzungsbedarf ergibt sich daher auch in diesem Punkt nicht.

Der über § 491 Absatz 1 Satz 1 und § 495 Satz 1 StPO entsprechend anzuwendende § 19 Absatz 5 Satz 2 BDSG sieht vor, dass der Betroffene dann, wenn die Auskunftserteilung begründungslos abgelehnt wird, darauf hinzuweisen ist, dass er sich an den BfDI wenden kann. Da es sich bei dem BfDI um eine nationale Kontrollstelle im Sinne des RbDatenschutz handelt, ist dadurch auch die Vorgabe des Artikels 17 Absatz 3 Satz 4 RbDatenschutz erfüllt, die den Hinweis an die betroffene Person verlangt, u. a. bei der zuständigen nationalen Kontrollstelle Beschwerde einlegen zu können.

Ferner kann der Betroffene nach § 475 Absatz 1 StPO Auskunft darüber verlangen, ob und ggf. welche personenbezogenen Daten zu ihm in einer Verfahrensakte enthalten sind und ob und ggf. wohin diese übermittelt wurden. Die Vorschrift gewährleistet im Strafprozessrecht das Grundrecht auf informationelle Selbstbestimmung, das ein berechtigtes Interesse im Sinne des § 475 Absatz 1 Satz 1 StPO bzw. rechtliches Interesse im Sinne des § 477 Absatz 3 StPO darstellt. Da es sich um die eigenen Daten des Betroffenen handelt, werden dem Auskunftsbegehren schutzwürdige Interessen eines anderen Betroffenen (§ 475 Absatz 1 Satz 2 bzw. § 477 Absatz 3 StPO) regelmäßig nicht entgegenstehen; soweit dies ausnahmsweise der Fall sein sollte, ist diese Beschränkung des Auskunftsrechts nach Artikel 17 Absatz 2 Buchstabe e RbDatenschutz zulässig.

Artikel 18 RbDatenschutz betrifft das Recht des Betroffenen auf Berichtigung, Löschung oder Sperrung. Ein Umsetzungsbedarf besteht für den Bereich des Bundeskriminalamtgesetzes, des Bundespolizeigesetzes und des Zollfahndungsdienstgesetzes nicht. Soweit in Artikel 18 Absatz 2 RbDatenschutz die Kennzeichnung eines Datums als Rechtsfolge vorgesehen ist, wenn der Betroffene die Richtigkeit eines personenbezogenen Datums bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, entspricht dies den Regelungen in § 33 Absatz 1 BKAG, § 35 Absatz 1 BPolG und § 40 Absatz 1 ZFdG, die den besonderen polizeilichen Belangen Rechnung tragen. Die weitergehende Regelung des § 20 Absatz 4 BDSG (Sperrung) findet nach § 37 BKAG, § 37 BPolG und § 43 ZFdG keine Anwendung.

Artikel 18 RbDatenschutz löst für den Bereich des Bundeskriminalamtgesetzes, des Bundespolizeigesetzes und des Zollfahndungsdienstgesetzes auch im Übrigen keinen Umsetzungsbedarf aus. Im Ergebnis verlangt Artikel 18 Absatz 1 Satz 3 RbDatenschutz für den Fall, dass die speichernde Behörde den Antrag des Betroffenen auf Berichtigung, Löschung oder Speicherung ablehnt, einen schriftlichen Ablehnungsbescheid mit Rechtsbehelfsbelehrung. Dies wird von den Behörden beachtet.

Für den Bereich der Strafprozessordnung besteht Umsetzungsbedarf hinsichtlich Artikel 18 Absatz 1 Satz 3 RbDatenschutz. Danach ist der betroffenen Person schriftlich mitzuteilen und ist sie auf die nach innerstaatlichem Recht vorgesehenen Möglichkeiten einer Beschwerde oder eines Rechtsmittels hinzuweisen, wenn der für die Verarbeitung Verantwortliche die Berichtigung, Löschung oder Sperrung ablehnt. Allerdings sind weder das Schriftlichkeitserfordernis noch die genannte Hinweispflicht in den Dateiregelungen der §§ 483 bis 491 StPO sowie den Vorgaben für das ZStV in den §§ 492 ff. StPO vorgesehen. Dem soll durch die Änderungen in § 489 Absatz 10 und § 494 Absatz 3 StPO-E Rechnung getragen werden.

Darüber hinaus besteht hinsichtlich der Vorgaben des Artikels 18 RbDatenschutz in der Strafprozessordnung kein Umsetzungsbedarf:

Das in Artikel 18 Absatz 1 Satz 1 RbDatenschutz statuierte Recht der betroffenen Person, dass der für die Datenverarbeitung Verantwortliche den Pflichten des Rahmenbeschlusses zur Berichtigung, Löschung oder Sperrung nachkommt, ist durch die in §§ 489 und 494 StPO enthaltenen Verpflichtungen umgesetzt. Denn sie geben der betroffenen Person zugleich einen entsprechenden Anspruch gegen die speichernde Stelle.

Nach Artikel 18 Absatz 1 Satz 2 RbDatenschutz legen die Mitgliedstaaten fest, ob die betroffene Person dieses Recht direkt gegenüber dem für die Verarbeitung Verantwortlichen oder über die zuständige nationale Kontrollstelle geltend machen kann. Nach § 489 StPO und § 494 StPO kann die betroffene Person ihre Ansprüche direkt gegenüber der speichernden Stelle geltend machen. Daneben kann die betroffene Person sich auch an den jeweils zuständigen Beauftragten für den Datenschutz wenden, wenn sie der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch öffentliche Stellen in ihren Rechten verletzt worden zu sein (§ 21 BDSG und z. B. § 29 Absatz 1 Landesdatenschutzgesetz Rheinland-Pfalz). Die Entscheidung über die beantragte Berichtigung, Löschung oder Sperrung bleibt jedoch bei der speichernden Stelle bzw. im Rechtsbehelfsverfahren bei dem zuständigen Gericht. Damit ist nach innerstaatlichem Recht festgelegt, dass die betroffene Person ihr subjektives Recht gegenüber dem für die Verarbeitung Verantwortlichen geltend machen kann. Durch die Möglichkeit, sich an den zuständigen Beauftragten für den Datenschutz zu wenden, besteht für die betroffene Person lediglich eine zusätzliche Anlaufstelle, um ihrem Begehren Nachdruck zu verleihen.

Artikel 18 Absatz 1 Satz 4 RbDatenschutz bestimmt, dass die betroffene Person bei der Prüfung der Beschwerde oder des Rechtsbehelfs davon in Kenntnis gesetzt wird, ob der für die Verarbeitung Verantwortliche ordnungsgemäß gehandelt hat oder nicht. Dies wird bereits durch § 35 StPO vorgegeben, der die Bekanntmachung von gerichtlichen Entscheidungen normiert. Für die durch Artikel 18 Absatz 1 Satz 5 RbDatenschutz vorgesehene Möglichkeit, es der zuständigen nationalen Kontrollstelle aufzugeben, die betroffene Person darüber zu informieren, dass eine Überprüfung stattgefunden hat, besteht daher kein Bedarf.

Die nach Artikel 18 Absatz 2 RbDatenschutz mögliche Kennzeichnung in ihrer Richtigkeit bestrittener Daten ist als Kann-Regelung ausgestaltet und löst damit keine Pflicht zur Umsetzung aus. Für das Strafverfahren erscheint es nicht erforderlich, eine Kennzeichnung für den Fall vorzusehen, dass die betroffene Person die Richtigkeit eines personenbezogenen Datums bestreitet und nicht ermittelt werden kann, ob es richtig ist oder nicht. Für das Strafverfahren erforderliche personenbezogene Daten müssen (immer wieder) von Amts wegen auf ihre Richtigkeit überprüft werden. Dies geschieht durch die Staatsanwaltschaft und/oder das Gericht im Rahmen des Strafverfahrens, in denen die Daten erhoben wurden bzw. für das sie genutzt werden. Stellt sich hierbei heraus, dass das Datum unrichtig ist, ist es auch in der Datei gemäß § 489 Absatz 1 bzw. dem ZStV gemäß § 494 Absatz 1 StPO zu berichtigen. Ein praktisches Bedürfnis für eine Regelung zur Kennzeichnung in den Fällen, in denen die Richtigkeit des Datums nicht im Strafverfahren geklärt werden kann, ist nicht ersichtlich.

Artikel 19 RbDatenschutz garantiert dem Betroffenen ein Recht auf Schadensersatz. Ein Umsetzungsbedarf besteht nicht. Nach § 7 BDSG hat der Betroffene gegen die verantwortliche Stelle einen – verschuldensabhängigen – Anspruch auf Ersatz sämtlicher materieller Schäden. Eine Verpflichtung, Vorschriften vorzusehen, nach denen ein Anspruch auf Ersatz immaterieller Schäden besteht, ergibt sich – ebenso wenig wie aus dem inhaltlich insoweit gleichen Artikel 23 der Richtlinie 95/46/EG (vgl. dazu Gola/Schomerus, Bundesdatenschutzgesetz, 11. Auflage 2012, § 7 BDSG, Rn. 12) – aus Artikel 19 RBDatenschutz nicht. Dessen ungeachtet kann auf Grund der allgemeinen Schadensersatz- (§§ 823 ff. des Bürgerlichen Gesetzbuchs (BGB)) und Staatshaftungsvorschriften (Artikel 34 des Grundgesetzes (GG) i. V. m. § 839 BGB), die durch die Haftungsvorschriften des Bundesdatenschutzgesetzes nicht verdrängt werden, ein Anspruch auf Ersatz immaterieller Schäden bestehen. Schließlich ist auch § 8 BDSG anwendbar, der – verschuldensunabhängig – einen Ersatz materieller und immaterieller Schäden vorsieht. Eine über den in § 8 Absatz 3 BDSG vorgesehenen Haftungshöchstbetrag von 130 000 Euro hinausgehende Haftung fordert Artikel 19 RbDatenschutz nicht. Artikel 19 Absatz 2 Satz 1 RbDatenschutz sieht ausdrücklich vor, dass die Haftung „nach Maßgabe des innerstaatlichen Rechts“ erfolgt.

Artikel 19 Absatz 2 RbDatenschutz sieht auch für die Fälle einen Schadensersatzanspruch gegen die deutsche Behörde vor, in denen der Schaden durch die Verwendung von unrichtig übermittelten Daten verursacht wurde, der Fehler mithin bei der übermittelnden ausländischen Stelle liegt. Auch insofern besteht kein Umsetzungsbedarf. Das Tatbestandsmerkmal der unrichtigen Verarbeitung oder Nutzung in den §§ 7 und 8 BDSG umfasst auch die Verarbeitung oder Nutzung unrichtiger Daten (vgl. dazu Gola/Schomerus, Bundesdatenschutzgesetz, 11. Auflage 2012, § 7 BDSG, Rn. 11). Bei der Auslegung von § 7 Absatz 2 BDSG ist die in Artikel 19 Absatz 2 Satz 1 RbDatenschutz vorgenommene Risikoverteilung zu berücksichtigen.

Artikel 20 RbDatenschutz garantiert dem Betroffenen gerichtlichen Rechtsschutz bei Verletzung seiner im innerstaatlichen Recht vorgesehenen Rechte. Ein Umsetzungsbedarf besteht nicht.

Artikel 21 RbDatenschutz über die Vertraulichkeit der Erhebung, Verarbeitung und Nutzung der Daten beschränkt den Zugang zu personenbezogenen Daten auf Personen, die Angehörige der datenverarbeitenden Behörde sind oder auf deren Weisung arbeiten. Auftragnehmer unterliegen ebenfalls den Vorschriften, die für die zuständige Auftrag gebende Behörde gelten. Ein Umsetzungsbedarf besteht nicht (vgl. §§ 5 und 11 BDSG).

Artikel 22 RbDatenschutz betrifft die Datensicherheit und insbesondere die technischen und organisatorischen Maßnahmen zum Schutz gegen Vernichtung, Verlust, unberechtigte Änderung, Weitergabe oder unberechtigten Zugang und jede andere Form der unerlaubten Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Die Vorgaben gehen nicht über das geltende innerstaatliche Recht hinaus und werden von § 9 BDSG sowie von der Anlage zu § 9 Satz 1 BDSG mit ihren Grundsätzen der Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle und der getrennten Verarbeitung zu unterschiedlichen Zwecken erhobener Daten umfasst. Soweit Artikel 22 Absatz 3 RbDatenschutz zudem Anforderungen an den Auftragsverarbeiter stellt, enthält § 11 BDSG entsprechende innerstaatliche Regelungen.

Artikel 23 RbDatenschutz bestimmt, dass die nationalen Kontrollstellen unter bestimmten Voraussetzungen vor der Verarbeitung personenbezogener Daten in neu zu errichtenden Dateien konsultiert werden (sogenannte Vorabkonsultation). Eine Vorabkonsultation ist für die Fälle vorzusehen, in denen besondere Kategorien von Daten

nach Artikel 6 RbDatenschutz (die im innerstaatlichen Recht in § 3 Absatz 9 BDSG benannt sind) verarbeitet werden oder in denen die Art der Verarbeitung spezifische Risiken birgt. Das Bundeskriminalamtgesetz schreibt für die beim Bundeskriminalamt zur Erfüllung seiner Aufgaben geführten automatisierten Dateien mit personenbezogenen Daten in § 34 eine Errichtungsanordnung vor, vor deren Erlass der BfDI als nationale Kontrollstelle im Sinne des RbDatenschutz anzuhören ist. Vergleichbare Regelungen treffen § 36 BPolG für die Bundespolizei und § 41 ZFdG für die Zollfahndung. Die Vorschriften gelten jedoch nicht für nicht-automatisierte Dateien; zudem lassen § 34 Absatz 3 Satz 1 BKAG, § 36 Absatz 2 Satz 2 BPolG und § 41 Absatz 3 Satz 1 ZFdG bei besonderer Dringlichkeit Ausnahmen von der vorherigen Beteiligung des BfDI zu. Der Anwendungsbereich der Normen und die Ausnahmen des § 34 BKAG lassen sich im Ergebnis aber mit der ratio legis der Vorabkonsultation des Artikels 23 RbDatenschutz vereinbaren.

Die vorgegebene Vorabkonsultation kann, auch wenn der Wortlaut des Artikels 23 RbDatenschutz nur von neu zu errichtenden „Dateien“ spricht, vom Sinn und Zweck des Artikels 23 RbDatenschutz her nur für die automatisierte Datenverarbeitung im Rahmen einer „Datei im eigentlichen Sinn“ (wie z. B. einer Vorgangsverwaltung) gelten. Soweit innerhalb eines – regelmäßig verfahrensübergreifenden – Dateiablagesystems einzelne „Dateien“ wie z. B. ein Word-Dokument oder eine Akte angelegt werden, kann sich Artikel 23 RbDatenschutz nur auf das System als solches und nicht jedes einzelne in ihm angelegte Dokument beziehen. Denn nur in den vorgenannten Bereichen entstehen abstrakte Gefahren beim Umgang mit Daten, die eine Mitwirkung des jeweils zuständigen Landes- oder Bundesbeauftragten für den Datenschutz rechtfertigen, um kontrollierend, beratend und ggf. begrenzend einzuwirken. Auch Erwägungsgrund 32 betont vor allem, dass die Notwendigkeit zur Vorabkonsultation dann besteht, wenn aufgrund des Umfangs oder der Art der Verarbeitung, z. B. bei der Verarbeitung mit Hilfe neuer Technologien, Mechanismen oder Verfahren, spezifische Risiken für die Grundrechte und -freiheiten bestehen. Ein solches verfahrensübergreifendes Dateisystem wird in der heutigen Zeit nur noch automatisiert (neu) errichtet und ist auch nur in dieser Form sinnvoll. Ein praktisches Bedürfnis für eine Regelung für die Errichtung nicht-automatisierter Dateien ist nicht ersichtlich. Ergänzungsbedarf besteht mit Blick auf § 490 StPO, der bisher bei der Errichtung automatisierter Dateien keine Vorabkonsultation vorsah.

Gemäß Artikel 24 RbDatenschutz sind „geeignete Maßnahmen“ zur Sicherstellung der Anwendung der Bestimmungen des Rahmenbeschlusses zu treffen, insbesondere Sanktionen festzulegen. Dies wird im innerstaatlichen Recht durch die vorhandenen Straf- und Bußgeldvorschriften und das Disziplinarwesen gewährleistet.

Artikel 25 Absatz 1 RbDatenschutz sieht vor, dass unabhängige nationale Kontrollstellen die Anwendung der Vorschriften des Rahmenbeschlusses überwachen und hierbei beratend tätig werden. Diese Kontrollstellen sollen gemäß Artikel 25 Absatz 2 RbDatenschutz über Untersuchungsbefugnisse, Einwirkungsbefugnisse und ein Klagerecht oder eine Anzeigebefugnis verfügen. Jeder Betroffene soll sich gemäß Artikel 25 Absatz 3 RbDatenschutz an jede Kontrollstelle wenden können.

Erwägungsgrund 34 des Rahmenbeschlusses ergänzt Artikel 25 RbDatenschutz durch die Empfehlung, dass die nach der Richtlinie 95/46/EG in den Mitgliedstaaten bereits errichteten Kontrollstellen auch die Aufgaben der nach diesem Rahmenbeschluss zu errichtenden nationalen Kontrollstellen übernehmen können. Satz 3 des Erwägungsgrundes 35 stellt zudem klar, dass die Befugnisse der Kontrollstellen weder die speziellen Vorschriften für Strafverfahren noch die Unabhängigkeit der Gerichte berühren dürfen. Damit bleibt auch die Entscheidungsbefugnis der Strafverfolgungsbehörden und Strafgerichte über die Datenverarbeitung unberührt. Umsetzungsbedarf besteht nicht.

Artikel 26 RbDatenschutz regelt die Beziehung des Rahmenbeschlusses zu Übereinkünften mit Drittstaaten. Danach werden vor der Annahme dieses Rahmenbeschlusses abgeschlossene bi- und multilaterale Übereinkünfte durch den Rahmenbeschluss nicht berührt.

Artikel 27 RbDatenschutz enthält Bestimmungen zur Evaluierung, die keiner rechtlichen Umsetzung bedürfen.

Artikel 28 RbDatenschutz regelt die Beziehung des Rahmenbeschlusses zu bereits früher angenommenen EU-Rechtsakten über den Austausch von personenbezogenen Daten zwischen Mitgliedstaaten oder den Zugang zu europäischen Informationssystemen. Sofern diese spezifische Bestimmungen für die Verwendung der Daten durch den Empfängermitgliedstaat enthalten, haben sie Vorrang gegenüber den entsprechenden Bestimmungen des RbDatenschutz. Dies bedeutet: Regeln die früher angenommenen Rechtsakte die Verwendung der Daten nicht, gelten die Regelungen des RbDatenschutz; regeln die früher angenommenen Rechtsakte die Verwendung der Daten, gelten diese Rechtsakte, nicht jedoch die Regelungen des RbDatenschutz.

Artikel 29 RbDatenschutz schließlich enthält Bestimmungen zur Umsetzung, insbesondere zur Umsetzungsfrist.

IV. Gründe für die Umsetzung des RbDatenschutz im Bundeskriminalamtgesetz, im Bundespolizeigesetz, im Zollfahndungsdienstgesetz, im Gesetz über die internationale Rechtshilfe in Strafsachen und in der Strafprozessordnung

Der RbDatenschutz betrifft den Schutz personenbezogener Daten bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Dieser Bereich wird bislang im Bundeskriminalamtgesetz, im Bundespolizeigesetz, im Zollfahndungsdienstgesetz, im Gesetz über die internationale Rechtshilfe in Strafsachen und in der Strafprozessordnung geregelt; deren Regelungen sind daher anzupassen.

1. Bundeskriminalamtgesetz

Die Änderungen im Bundeskriminalamtgesetz aufgrund der Vorgaben des RbDatenschutz betreffen den Abschnitt 2 Unterabschnitt 1 des Bundeskriminalamtgesetzes zur Zentralstellenaufgabe (hier die Bestimmungen zur Datenübermittlung im innerstaatlichen Bereich, § 10 BKAG), den Abschnitt 2 Unterabschnitt 2 des Bundeskriminalamtgesetzes zur internationalen Zusammenarbeit (hier die §§ 14 und 14a BKAG) sowie die Gemeinsamen Bestimmungen in Abschnitt 3 des Bundeskriminalamtgesetzes (hier die §§ 27a und 32 BKAG).

2. Bundespolizeigesetz

Die Änderungen im Bundespolizeigesetz betreffen dessen Abschnitt 2 Unterabschnitt 2. Zum einen werden die Bestimmungen zur Datenübermittlung und Datennutzung bei der internationalen Zusammenarbeit geändert bzw. ergänzt (hier §§ 32, 33 und 33a BPolG). Zudem werden die Regelungen über Berichtigung, Löschung und Sperrung personenbezogener Daten (hier § 35 BPolG) modifiziert.

3. Zollfahndungsdienstgesetz

Die Änderungen im Zollfahndungsdienstgesetz betreffen die dortigen Kapitel 2 und 4, Hier sind die Bestimmungen zum Zollfahndungsinformationssystem (§ 11 ZFdG) zur Datenübermittlung im innerstaatlichen Bereich (§ 33 ZFdG), diejenigen zur internationalen Zusammenarbeit und der Zusammenarbeit mit den Mitgliedstaaten der Europäischen Union (§§ 34 und 34a ZFdG) sowie diejenigen zum Umgang mit Daten (§§ 35a und 39 ZFdG) betroffen.

4. Gesetz über die internationale Rechtshilfe in Strafsachen

Umsetzungsbedarf im Gesetz über die internationale Rechtshilfe in Strafsachen lösen vor allem Artikel 3 Absatz 2 Satz 2, Artikel 8 und 9 sowie Artikel 11 bis 14 RbDatenschutz aus. Schon bisher sind bereichsspezifische und allgemeine datenschützende Vorschriften im Rechtshilfeverfahren zu beachten. Ergänzend dazu sollen künftig die bereichsspezifischen Vorschriften für den grenzüberschreitenden Datenaustausch im Rahmen der strafrechtlichen Zusammenarbeit innerhalb der Europäischen Union im Elften Teil des IRG (§§ 97a bis 97d IRG-E) gelten. Mit den bereichsspezifischen Regelungen im IRG wird dem Umstand Rechnung getragen, dass der Datenaustausch innerhalb der Europäischen Union stark an Bedeutung zugenommen hat. In den vergangenen Jahren wurde eine Vielzahl europäischer Rechtsinstrumente geschaffen, die die strafrechtliche Zusammenarbeit unter den Mitgliedstaaten und mit den europäischen Agenturen wie z. B. Eurojust und Europol vereinfachen sollen. Regelmäßig geht damit – rechtlich geregelt oder jedenfalls als Folge eines erhöhten Fallaufkommens – ein erhöhter Austausch von personenbezogenen Daten einher, vgl. nur die erweiterten Unterrichtungspflichten nach Artikel 13 des Beschlusses 2009/426/JI des Rates vom 16. Dezember 2008 zur Stärkung von Eurojust und zur Änderung des Beschlusses 2002/187/JI über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität (ABl. L 138 vom 4.6.2009, S. 14).

Ausdrückliche datenschützende Vorschriften im IRG lenken das Augenmerk der Rechts-praxis auf datenschutzrechtliche Belange. Nicht erforderlich ist dagegen, aus Anlass der Umsetzung des RbDatenschutz auch Regelungen für den Rechtshilfeverkehr mit Dritt-staaten in das IRG aufzunehmen. Dies ginge zum einen über die Vorgaben des RbDatenschutz hinaus. Zum anderen kann im Bereich der Rechtshilfe mit Drittstaaten grundsätzlich weiterhin mit den klassischen Sicherungsinstrumentarien wie Bedingungen und Zusicherungen gearbeitet werden, mittels derer sich die nationalen datenschutzrechtlichen Erfordernisse durchsetzen lassen. Im Bereich der strafrechtlichen Zusammenarbeit mit den Mitgliedstaaten und Einrichtungen der Europäischen Union, die maßgeblich durch den Grundsatz der gegenseitigen Anerkennung bzw. den Grundsatz der Verfügbarkeit geprägt ist, sind

solche Bedingungen dagegen nur noch eingeschränkt möglich. Für die Rechtspraxis könnte deshalb nicht ausreichend transparent sein, welcher datenschutzrechtliche Standard hier gilt und wie dieser durchzusetzen ist. Für diesen Bereich sollen deshalb bereichsspezifische Regelungen geschaffen werden.

Ebenfalls nicht erforderlich ist es, die papiergeführte Akte in den Anwendungsbereich der neuen Regelungen einzubeziehen. Der Wortlaut von Artikel 1 Absatz 3 RbDatenschutz erfasst die papiergeführte Strafakte im Sinne einer bloßen Blattsammlung nicht. Soweit in der staatsanwaltschaftlichen Praxis Akten elektronisch geführt oder eingescannt werden und dann computergestützt ausgewertet werden können oder personenbezogene Daten anderweitig automatisiert verarbeitet werden, ist der Anwendungsbereich der §§ 97a ff. IRG-E eröffnet. Erfasst werden grundsätzlich auch alle elektronischen Daten-übermittlungen, insbesondere per E-Mail.

Die Regelungen des Elften Teils ergänzen die bisherigen datenschützenden Vorschriften im IRG, lassen diese also grundsätzlich unberührt. Soweit das IRG bereits datenschützende Vorschriften enthält, die strenger sind als die des Elften Teils, bleiben erstere zu beachten. Der RbDatenschutz will lediglich ein datenschutzrechtliches Mindestniveau schaffen; Artikel 1 Absatz 5 RbDatenschutz lässt den Fortbestand strengerer nationaler Vorschriften ausdrücklich zu. Unberührt bleiben somit beispielsweise die Voraussetzungen, die § 92c IRG in Verbindung mit § 61a IRG für die sogenannten Spontanübermittlungen vorsieht. Insbesondere gilt weiterhin die verbindliche Regelung aus § 92 Absatz 2 in Verbindung mit § 61a Absatz 2 Buchstabe a IRG, wonach Datenübermittlungen ohne Er-suchen durch deutsche Behörden mit der Bedingung versehen werden müssen, dass die nach nationalem Recht geltenden Löschungs- oder Löschungsprüffristen einzuhalten sind. Diese verpflichtende Vorgabe geht der lediglich fakultativen Regelung aus § 97c Absatz 2 Nummer 4 IRG-E vor. Auch die besonderen Vorschriften, die gemäß § 92b IRG für den Datenaustausch auf der Grundlage der sogenannten Schwedischen Initiative gelten, behalten neben dem Elften Teil ihre Gültigkeit.

Für personenbezogene Daten, die im Wege der Rechtshilfe ausgetauscht werden, werden mit dem Elften Teil des IRG bereichsspezifische Regelungen eingeführt, welche die datenschützenden Vorschriften der Strafprozessordnung, dort insbesondere die Regelungen des Achten Buches, und die des Gesetzes über Ordnungswidrigkeiten, dort insbesondere die Regelungen im Zweiten Abschnitt des Zweiten Teils, ergänzen und damit zusätzlich zu berücksichtigen sind.

Die Geltung des RbDatenschutz ist nicht trennscharf auf den Bereich des grenzüber-schreitenden Datenverkehrs begrenzt. So wirken die Verwendungsregelungen des RbDatenschutz – insbesondere die Zustimmungserfordernisse aus Artikel 11 Satz 1 Buchstabe d, Artikel 13 Absatz 1 Buchstabe c und Artikel 14 Absatz 1 Buchstabe a – für personenbezogene Daten, die den nationalen Behörden von einem anderen Mitgliedstaat übermittelt wurden, auch in das weitere innerstaatliche Strafverfahren hinein, wenn die Daten in die nationale Strafakte eingehen. Für die jeweils betroffenen Daten ist das Zustimmungserfordernis auch innerstaatlich zu beachten, wenn eine verfahrensübergreifende Verwendung der Daten beabsichtigt ist. Die Regelungen im Elften Teil des IRG können sich somit ebenfalls nicht auf das rechtshilferechtliche Verfahren beschränken, sondern knüpfen an die konkreten personenbezogenen Daten an. Insoweit werden aber keine neuen Befugnisnormen für die zuständigen Behörden geschaffen, sondern die Vorschriften grenzen bestehende Ermächtigungen zur Datenübermittlung ein. Die Regelungen des Elften Teils sind als bereichsspezifische Verwendungsregelungen gemäß § 487 Absatz 1 Satz 2 i. V. m. § 477 Absatz 2 Satz 1 StPO sowie bei der Übermittlung personenbezogener Daten von Amts wegen gemäß § 12 Absatz 3 EGGVG von den Strafverfolgungsbehörden zu beachten, auch nachdem personenbezogene Daten, die deutsche Behörden im Wege der strafrechtlichen Zusammenarbeit aus dem Ausland erhalten haben, Teil eines im Inland geführten Strafverfahrens geworden sind. Eine sachgerechte Handhabung der datenschützenden Regelungen wird in der Rechtspraxis bedeuten, dass die betroffenen personenbezogenen Daten gegebenenfalls zu kennzeichnen sind.

Dies entspricht dem schon bisher geltenden Verhältnis zwischen dem Rechtshilferecht und dem nationalen Verfahrensrecht. Insbesondere sind rechtshilferechtliche Bedingungen, die ein anderer Staat an eine grenzüberschreitende Übermittlung von personenbezogenen Daten knüpft, nicht nur im Rechtshilfeverfahren, sondern auch im (weiteren) innerstaatlichen Umgang mit den Daten zu beachten, § 72 IRG. Die datenschützenden Vorgaben aus dem Rechtshilfeverfahren können damit ein engeres Korsett bilden als etwa die Vorschriften der Strafprozessordnung, und dieses Korsett kann gemäß § 477 Absatz 2 Satz 1 und § 487 Absatz 1 Satz 2 StPO i. V. m. § 72 IRG auch im innerstaatlichen Umgang mit den Daten nicht abgelegt werden. Dies hat aber nicht zur Folge, dass die datenschützenden Regelungen der Strafprozessordnung durch das IRG verdrängt würden, wenn die betroffenen personenbezogenen Daten grenzüberschreitend erlangt wurden. Bei ausgehenden personenbezogenen Daten ist

über § 59 Absatz 3 IRG sichergestellt, dass innerstaatliche Vorgaben zum Umgang mit den Daten auch im grenzüberschreitenden Verkehr beachtet werden. Die bereichsspezifischen datenschützenden Vorschriften des IRG – insbesondere § 61a Absatz 2 IRG, wonach Datenübermittlungen ohne Ersuchen obligatorisch mit bestimmten Bedingungen zu verbinden sind – sind im Rechtshilfeverkehr zusätzlich zu den Vorgaben der Strafprozessordnung zu beachten.

Soweit das IRG keine bereichsspezifischen datenschützenden Vorschriften enthält, bleibt wie bisher ein Rückgriff auf die Strafprozessordnung, das Gesetz über Ordnungswidrigkeiten und auch auf die allgemeinen datenschützenden Vorschriften des Bundesdatenschutzgesetzes möglich.

5. Strafprozessordnung

Die Änderungen in der Strafprozessordnung betreffen im dortigen Achten Buch die Abschnitte 2 (§§ 488, 489 und 490 StPO-E) und 3 (§§ 493 und 494 StPO-E). Dort werden die Regelungen zur Protokollierung oder Dokumentierung von Übermittlungen, zum Verwendungszweck der Protokolldaten, zur Berichtigung, Löschung und Sperrung personenbezogener Daten sowie zur Vorabkonsultation bei neu zu errichtenden automatisierten Dateien modifiziert.

V. Verhältnis zu anderen bi- und multilateralen Übereinkommen

Nach seinem Artikel 26 berührt der RbDatenschutz Verpflichtungen und Zusagen von Mitgliedstaaten und der Europäischen Union, die sich aus vor der Annahme des RbDatenschutz abgeschlossenen bilateralen und/oder multilateralen Übereinkünften mit Drittstaaten ergeben, nicht. Bei der Anwendung solcher Übereinkünfte hat allerdings die Weiterleitung personenbezogener Daten, die von einem anderen Mitgliedstaat übermittelt wurden, an einen Drittstaat unter Einhaltung der Vorgaben des Artikels 13 RbDatenschutz zu erfolgen. Das bedeutet insbesondere, dass eine Übermittlung der Daten nach solchen Übereinkünften grundsätzlich nur mit Zustimmung des anderen Mitgliedstaates zulässig ist.

VI. Gesetzgebungskompetenz

Die zur Umsetzung erforderlichen Änderungen des Bundeskriminalamtgesetzes (Artikel 1) sowie des Bundespolizeigesetzes (Artikel 2) fallen in den Bereich der internationalen Verbrechensbekämpfung und damit nach Artikel 73 Absatz 1 Nummer 10 GG in die ausschließliche Gesetzgebungskompetenz des Bundes. Für das Zollfahndungsdienstgesetz (Artikel 3) ergibt sich die ausschließliche Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 5 GG. Nach Artikel 32 GG ist die internationale Zusammenarbeit in strafrechtlichen Angelegenheiten Teil der Pflege der auswärtigen Beziehungen. Die durch die Umsetzung des RbDatenschutz erforderlichen Änderungen des Gesetzes über die internationale Rechtshilfe in Strafsachen (Artikel 4) fallen deshalb in den Bereich der ausschließlichen Gesetzgebungskompetenz des Bundes nach Artikel 73 Absatz 1 Nummer 1 GG. Die Gesetzgebungskompetenz des Bundes zur Änderung der Strafprozessordnung (Artikel 5) und des Gesetzes über Ordnungswidrigkeiten (Artikel 6) folgt aus Artikel 74 Absatz 1 Nummer 1 GG.

VII. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Die vorgeschlagenen Neuregelungen dienen der Umsetzung des RbDatenschutz. Sie sind mit dem Recht der Europäischen Union und mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.

VIII. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Die vorgeschlagenen Änderungen konkretisieren den bereichsspezifischen Datenschutz und erleichtern so den zuständigen Behörden im Rahmen der grenzüberschreitenden strafrechtlichen und polizeilichen Zusammenarbeit innerhalb der Europäischen Union den angemessenen Umgang mit personenbezogenen Daten.

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Nationalen Nachhaltigkeitsstrategie, indem innerhalb der Europäischen Union die grenzüberschreitende Zusammenarbeit auf dem Gebiet der Kriminalitätsbekämpfung um klare datenschützende Regelungen ergänzt wird. Dies schafft einheitliche Maßstäbe und mehr Transparenz nicht nur für die beteiligten Behörden, sondern auch für die Bürgerinnen und Bürger, deren personenbezogenen Daten betroffen sind. Der Datenschutz wird verbessert und die Rechtspositionen von betroffenen Bürgerinnen und Bürgern der Europäischen Union werden geschützt und gestärkt.

Die Verbesserung der Zusammenarbeit im Bereich der Strafverfolgung und der Schutz von Grundrechten sind wichtige Bestandteile der Entwicklung eines europäischen Raums der Freiheit, der Sicherheit und des Rechts, der mit dem sogenannten Stockholmer Programm des Europäischen Rates bestätigt und fortgeschrieben wurde.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Haushaltsausgaben ohne Erfüllungsaufwand sind nicht zu erwarten.

4. Erfüllungsaufwand

a) Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand. Es werden keine Informationspflichten für die Wirtschaft oder für Bürgerinnen und Bürger eingeführt, geändert oder abgeschafft.

b) Bund und Länder

Durch die Umsetzung des RbDatenschutz wird sich auf Bundesebene der Verwaltungsaufwand für das Bundeskriminalamt (BKA), die Behörden der Bundespolizei, die Behörden des Zollfahndungsdienstes, das Bundesamt für Justiz (BfJ), den Generalbundesanwalt (GBA) und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie auf Landesebene der Verwaltungsaufwand für die Staatsanwaltschaften und die Polizeibehörden der Länder moderat erhöhen.

aa) Bundeskriminalamtgesetz, Bundespolizeigesetz, Zollfahndungsdienstgesetz

Für die Verwaltung werden für das Bundeskriminalamt, die Bundespolizei und die Behörden des Zollfahndungsdienstes keine Vorgaben aufgehoben und die nachfolgend aufgezählten Vorgaben neu eingeführt:

§ 10 Absatz 3 Satz 2 BKAG-E, § 33 Absatz 2a Satz 1 2. Alternative BPolG-E, § 33 Absatz 5 Satz 2 ZFdG-E	Einholung der Zustimmung der zuständigen Behörde eines anderen Mitgliedstaates vor einer Datenübermittlung an nicht-öffentliche Stellen
§ 14 Absatz 8 Satz 1 BKAG-E, § 33 Absatz 2a Satz 1 1. Alternative BPolG-E, § 34 Absatz 5 ZFdG-E	Einholung der Zustimmung der zuständigen Behörde eines anderen Mitgliedstaates vor einer Datenübermittlung an Drittstaaten
§ 14 Absatz 9 Satz 2 BKAG-E, § 33 Absatz 2a Satz 3 BPolG-E, § 34 Absatz 6 Satz 2 ZFdG-E	Unterrichtung der zuständigen Behörde eines anderen Mitgliedstaates nach einer Datenübermittlung im Eilfall
§ 14 Absatz 10 Satz 1 BKAG-E, § 33 Absatz 9 Satz 1 BPolG-E, § 34 Absatz 7 Satz 1 ZFdG-E	Überprüfung von Daten vor ihrer Übermittlung
§ 14 Absatz 10 Satz 2 BKAG-E, § 33 Absatz 9 Satz 2 BPolG-E, § 34 Absatz 7 Satz 2 ZFdG-E	Beifügung von Informationen für den Empfänger von Daten
§ 14 Absatz 10 Satz 3 BKAG, § 34 Absatz 7 Satz 3 ZFdG	Angabe von Aufbewahrungsfristen für die Daten
§ 14 Absatz 10 Satz 4 BKAG-E, § 34 Absatz 7 Satz 4 ZFdG-E	Hinweis an den Empfänger auf besondere bundesgesetzliche Verwendungsregelungen für den Datenaustausch

§ 14 Absatz 10 Satz 5 BKAG-E, § 34 Absatz 7 Satz 5 ZFdG-E	Ersuchen an Empfänger, den Betroffenen nicht ohne vorherige Zustimmung der übermittelnden Stelle zu informieren
§ 14a Absatz 7 BKAG, § 34a Absatz 7 ZFdG-E	Übermittlung personenbezogener Daten an nicht-öffentliche Stellen in Mitgliedstaaten der EU
§ 27a Absatz 1 Satz 2 BKAG-E, § 33a Absatz 2 Satz 1 BPolG-E, § 35a Absatz 1 Satz 2 ZFdG-E	Einholung der vorherigen Zustimmung des übermittelnden Mitgliedstaates
§ 27a Absatz 3 BKAG-E, § 37 Absatz 2 Satz 2 BPolG-E, § 35a Absatz 3 ZFdG-E	Auskunfterteilung zur Datenverwendung auf Ersuchen des übermittelnden Staates
§ 33 Absatz 8 Satz 1 BPolG-E, § 11 Absatz 4 Satz 1 ZFdG-E	Protokollierung aller Abrufe bei automatisierten Abrufverfahren
§ 33 Absatz 3 Satz 3 ZFdG-E	Hinweis an den Empfänger auf Verwendungsbeschränkungen
§ 33 Absatz 6 ZFdG-E	Einholung der Zustimmung vor Datenübermittlung

Für das BKA ist durch die Änderungen von einer – mangels statistischer Erhebungen des Auslandsverkehrs – nicht genau bezifferbaren, insgesamt jedoch moderaten Erhöhung des Verwaltungsaufwandes auszugehen. Soweit § 27a Absatz 1 Satz 1 BKAG-E eine Nutzung aus dem Ausland übermittelter Daten außerhalb der Zweckbindung ohne Zustimmung des übermittelnden Staates gestattet, ist von einer – ebenfalls nicht zu bezifferbaren – Entlastung auszugehen.

Auch für die Behörden der Bundespolizei ist die durch die Änderungen bewirkte Erhöhung des Mehraufwandes nicht bezifferbar. Schätzungen innerhalb der Bundespolizei ergeben, dass der zeitliche Mehraufwand bei der Bearbeitung eines einzelnen Vorgangs zwischen 20 und 35 Minuten beträgt. Eine statistische Erhebung des Informationsaustauschs mit ausländischen Staaten findet innerhalb der Bundespolizei, wo im Eilfall jeder einzelne Ermittlungsbeamte auch einen direkten Austausch mit dem Ausland autorisieren kann, nicht statt.

Der Zollfahndungsdienst wendet überwiegend das so genannte Neapel II-Übereinkommen (Übereinkommen aufgrund von Artikel K3 des Vertrags über die Europäische Union über gegenseitige Amtshilfe und Zusammenarbeit der Zollverwaltungen (BGBl. II 2002, S. 1387)) für einen Austausch personenbezogener Daten mit anderen EU-Mitgliedstaaten an. Die hier in Artikel 25 enthaltenen Datenschutzregelungen, die mit den Regelungen des RbDatenschutz vergleichbar sind, gehen dem RbDatenschutz vor (Artikel 28 RbDatenschutz).

Da die Bestimmungen im Wesentlichen auch im Neapel II-Übereinkommen enthalten sind, stellen sie bereits die gängige Praxis dar.

bb) IRG

Durch die Änderungen im IRG fällt für die Länder ein insgesamt moderater Erfüllungsaufwand an, der sich allerdings nicht konkret beziffern lässt. Für den Bereich der grenzüberschreitenden strafrechtlichen Zusammenarbeit innerhalb der Europäischen Union gilt der unmittelbare Geschäftsverkehr zwischen den beteiligten Justizbehörden der Länder, insbesondere der Staatsanwaltschaften und auch der Gerichte. Die zuständigen Länderbehörden sind somit ein Hauptadressat der neu eingeführten datenschutzrechtlichen Verpflichtungen im Rechtshilfeverkehr mit anderen Mitgliedstaaten der Europäischen Union oder mit Stellen oder Informationssystemen nach dem Dritten Teil Titel V Kapitel 4 und 5 AEUV sowie mit Schengen-assoziierten Staaten. Zu diesen Verpflichtungen zählen insbesondere die nachstehend aufgeführten Informations- und Kommunikationspflichten:

§ 97b Absatz 2 Satz 2 Nummer 1, Satz 3 IRG-E	Verpflichtung zur Einholung der Zustimmung der zuständigen Behörde eines anderen Mitgliedstaates vor einer Datenübermittlung an nicht-öffentliche Stellen
§ 97c Absatz 2 Nummer 3 IRG-E	Verpflichtung, die empfangende Stelle auf besondere Verwendungsregelungen für den Datenaustausch hinzuweisen

§ 97c Absatz 2 Nummer 5 IRG-E	Verpflichtung, die empfangende Stelle zu unterrichten, wenn sich herausstellt, dass Daten nicht hätten übermittelt werden dürfen oder dass unrichtige Daten übermittelt wurden
§ 97d Absatz 1 Nummer 3, Absatz 2 Satz 2 IRG-E	Verpflichtung zur Einholung einer vorherigen Zustimmung des übermittelnden Mitgliedstaates zur Weiterleitung von Daten an zwischen- oder überstaatliche Stellen oder zur nachträglichen Unterrichtung über die Weiterleitung

Die Informations- und Kommunikationspflichten führen zu einem gewissen Mehraufwand bei den zuständigen Behörden. Fallzahlen lassen sich nicht vorhersagen. Amtliche Rechtshilfestatistiken existieren weder auf Bundes- noch auf Länderebene, so dass sich bereits die Gesamtzahl aller Rechtshilfevorgänge, die Mitgliedstaaten der Europäischen Union betreffen, nicht belastbar ermitteln lässt. Darüber hinaus lässt sich nicht generell sagen, wie oft es im Rahmen eines konkreten Rechtshilfevorgangs zu einem Austausch von personenbezogenen Daten kommt; dies hängt jeweils von den Umständen des Einzelfalls ab und divergiert entsprechend stark. Konkrete Angaben oder belastbare Schätzungen zu den zusätzlichen Kosten, die sich für die Landesbehörden aus den zusätzlichen Pflichten ergeben, können deshalb nicht gemacht werden. Insgesamt ist aber zu erwarten, dass ein Mehraufwand mit den bestehenden personellen und sachlichen Ressourcen aufgefangen werden kann: Die Einrichtung neuer Organisationsstrukturen in den Ländern ist nicht erforderlich. Schon bislang sind im Bereich der strafrechtlichen Zusammenarbeit – nicht nur innerhalb der Europäischen Union – datenschutzrechtliche Vorschriften zu beachten, auch wenn diese bisher nicht sämtlich eine ausdrückliche Regelung im IRG erfahren haben. Die bestehenden Vorschriften werden durch die neuen bereichsspezifischen Regelungen lediglich ergänzt, siehe die Anmerkungen unter Ziffer IV.4. Zudem verstehen sich die Neuregelungen teilweise als bloße Klarstellung einer bereits geltenden Rechtslage oder Rechtspraxis; auf die Anmerkungen im Besonderen Teil der Begründung zu § 97c Absatz 2 Nummer 5 und § 97d Absatz 1 Nummer 3 IRG-E wird beispielhaft verwiesen. Insoweit stellt sich etwa die Frage, ob bestimmte Kennzeichnungs- oder Protokollierungspflichten für die beteiligten Behörden erforderlich sind, damit datenschützende Vorgaben tatsächlich eingehalten werden können, nicht erst durch die Neuregelung des Elften Teils des IRG. Ebenso wenig dürfte ein erhöhter Einarbeitungsaufwand bei den zuständigen Behörden anfallen. Vielmehr können ausdrückliche bereichsspezifische Vorschriften zum Datenschutz im IRG den zuständigen Behörden den Umgang mit personenbezogenen Daten in der grenzüberschreitenden strafrechtlichen Zusammenarbeit innerhalb der Europäischen Union erleichtern. Auch lässt das Europarecht ausdrücklich Möglichkeiten unberührt, den Organisationsaufwand für einzelne Behörden durch standardisierte Lösungsansätze zu minimieren, vgl. die Anmerkungen im Besonderen Teil der Begründung zu § 97d Absatz 1 Nummer 3 IRG-E.

Für den Bund fällt durch die Neuregelungen im Elften Teil des IRG ein insgesamt verhältnismäßig geringer Erfüllungsaufwand an, der sich mangels vorhersehbarer Fallzahlen ebenfalls nicht beziffern lässt (s. o.). Maßgeblich sind insoweit die Kosten, die beim BfJ und beim GBA anfallen. Das BfJ ist insbesondere dann Normadressat, wenn es als zuständige Behörde in die grenzüberschreitende strafrechtliche Zusammenarbeit innerhalb der Europäischen Union aktiv eingebunden ist, etwa als zentrale Bewilligungsbehörde des Bundes für eingehende und ausgehende Ersuchen nach den §§ 86 ff. IRG. Aber auch, soweit das BfJ etwa von den Länderbehörden unter bestimmten Umständen über Einzelfälle unterrichtet wird und insoweit personenbezogene Daten führt, ist es an die datenschutzrechtlichen Vorgaben gebunden. Der GBA nimmt als Strafverfolgungsbehörde des Bundes an der strafrechtlichen Zusammenarbeit innerhalb der Europäischen Union teil. Sowohl für das BfJ als auch für den GBA gelten die Ausführungen zum Mehraufwand bei den Länderbehörden entsprechend. Insgesamt ist davon auszugehen, dass ein Mehraufwand, der sich aus den neuen Informations- und Kommunikationsverpflichtungen ergibt, mit den bestehenden personellen und sachlichen Ressourcen aufgefangen werden kann. Sollte ein Mehrbedarf an Sach- und Personalmitteln durch zusätzlichen Erfüllungsaufwand für den Bund entstehen, soll er im Einzelplan des Bundesministeriums der Justiz und für Verbraucherschutz ausgeglichen werden.

cc) Strafprozessordnung

Im Bereich der Strafprozessordnung ergeben sich folgende Änderungen:

§ 488 Absatz 3 Satz 4 und 5, Absatz 4 StPO-E	Verpflichtende Protokollierung durch die speichernde Stelle bei jeder Übermittlung im automatisierten Abrufverfahren und im automatisierten Anfrage- und Auskunftsverfahren nach § 488 Absatz 1 StPO-E statt bisheriger „Soll-Regelung“ der Speicherung der Protokolldaten bei jedem zehnten Abruf
§ 489 Absatz 10 StPO-E	Neueinführung einer Pflicht der speichernden Stelle, der betroffenen Person eine Nichtvornahme einer beantragten Berichtigung, Löschung oder Sperrung schriftlich mitzuteilen sowie sie auf bestehende Rechtsbehelfe hinzuweisen
§ 490 Satz 2 StPO-E	In Fällen der Neuerrichtung automatisierter Dateien Neueinführung einer Verpflichtung zur Anhörung des zuständigen Datenschutzbeauftragten vor der Verarbeitung personenbezogener Daten in diesen
§ 493 Absatz 3 StPO-E	Verpflichtende Protokollierung durch die Registerbehörde bei jedem Abruf statt bisher bei jedem zehnten Abruf
§ 494 Absatz 3 StPO-E	Neueinführung einer Pflicht der Registerbehörde, der betroffenen Person eine Nichtvornahme einer beantragten Berichtigung, Löschung oder Sperrung schriftlich mitzuteilen sowie sie auf bestehende Rechtsbehelfe hinzuweisen

Bund

Der Verwaltungsaufwand, der durch die verpflichtende Anhörung des zuständigen Datenschutzbeauftragten im Fall der Neuerrichtung automatisierter Dateien anfällt, ist als lediglich geringfügig einzuschätzen. Soweit das BfJ als Registerbehörde für das zentrale staatsanwaltschaftliche Verfahrensregister nunmehr nach § 493 Absatz 3 StPO-E verpflichtet ist, jeden – statt wie bisher jeden zehnten – Abruf im automatisierten Abrufverfahren und im automatisierten Anfrage- und Auskunftsverfahren zu protokollieren, werden hierfür keine zusätzlichen einmaligen oder dauerhaften Kosten entstehen, da lediglich einmalig eine Änderung der Programmierung erfolgen muss. Im Übrigen dürfte sich der Verwaltungsaufwand des BfJ für die neu eingeführte Pflicht zur schriftlichen Bescheidung der Antragsteller aus § 494 Absatz 3 StPO-E aufgrund der bereits derzeit üblichen schriftlichen Kommunikation mit Antragstellern allenfalls geringfügig und in derzeit nicht quantifizierbarem Umfang erhöhen. Eine Erhöhung der Anzahl der Anträge betroffener Personen ist durch die Neuregelung nicht zu erwarten.

Der GBA ist von der Änderung in § 488 Absatz 3 Satz 4 und 5, Absatz 4 StPO-E nicht betroffen, da er in diesem Bereich derzeit keine automatisierte Datenübermittlung durchführt. Hinsichtlich der neu eingeführten Pflicht zur schriftlichen Bescheidung der Antragsteller aus § 489 Absatz 10 StPO-E gelten die Ausführungen zum BfJ entsprechend.

Länder

Auch die Länder dürften hauptsächlich von der sich aus § 489 Absatz 10 StPO-E ergebenden Verpflichtung betroffen sein. Der Verwaltungsaufwand dürfte sich aufgrund der auch dort bereits derzeit üblichen schriftlichen Kommunikation mit Antragstellern ebenso allenfalls geringfügig und in derzeit nicht quantifizierbarem Umfang erhöhen. Soweit sich einzelne Länder im Rahmen der Abstimmung zum entstehenden Mehraufwand geäußert haben, haben sie ausgeführt, dass dieser derzeit nicht abschätzbar, nicht quantifizierbar oder – bedingt durch einzelne Anpassungen der EDV – moderat sei.

5. Weitere Kosten

Für die Wirtschaft, insbesondere für kleinere und mittlere Unternehmen, entstehen keine Kosten. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

6. Weitere Gesetzesfolgen

Auswirkungen von gleichstellungspolitischer oder verbraucherpolitischer Bedeutung sind nicht zu erwarten.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Bundeskriminalamtgesetzes)

Zu Nummer 1

Es handelt sich um eine Folgeänderung zur Neufassung der Überschrift von § 27a BKAG (Nummer 5 Buchstabe a).

Zu Nummer 2

Nummer 2 dient der Umsetzung von Artikel 14 RbDatenschutz über die Übermittlung von Daten an nicht-öffentliche Stellen in Mitgliedstaaten. Es werden gegenüber dem bisherigen § 10 Absatz 3 BKAG zusätzliche einschränkende Voraussetzungen vorgesehen, unter denen personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates für Zwecke der Gefahrenabwehr übermittelt oder bereitgestellt wurden, an nicht-öffentliche Stellen weitergeleitet werden dürfen.

Die in Artikel 11 RbDatenschutz ebenfalls vorgesehenen Verwendungsbeschränkungen für personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen übermittelt oder bereitgestellt wurden, gelten zwar ebenfalls für sonstige innerstaatliche Übermittlungen im Anwendungsbereich des § 10 BKAG, haben darüber hinaus aber einen weiteren Anwendungsbereich, da sie sonstige Formen der Verarbeitung und der Nutzung der Daten einschließen. Als Regelungsstandort für die Umsetzung des Artikels 11 RbDatenschutz wurde daher nicht § 10, sondern § 27a BKAG gewählt.

Die Änderung ergänzt § 10 Absatz 3 BKAG über Datenübermittlungen an innerstaatliche nicht-öffentliche Stellen um einschränkende Voraussetzungen. § 10 Absatz 3 Satz 1 in Verbindung mit Absatz 2 BKAG enthält die Voraussetzungen einer Übermittlung an nicht-öffentliche Stellen. Nach geltender Rechtslage ist eine Übermittlung danach zulässig zur Erfüllung der Aufgaben des Bundeskriminalamts nach dem Bundeskriminalamtgesetz, für Zwecke der Strafverfolgung, der Strafvollstreckung, des Strafvollzugs und der Gnadenverfahren, für Zwecke der Gefahrenabwehr oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner. Mit Nummer 2 wird ein neuer Satz 2 in § 10 Absatz 3 BKAG-E eingefügt, nach dem eine Übermittlung zur Gefahrenabwehr nach Absatz 2 Nummer 3 nur zulässig ist, wenn sie zur Verhütung von Straftaten oder sonst zur Abwehr einer gegenwärtigen und erheblichen Gefahr erfolgt. Gemeint sind damit Gefahren für nicht strafrechtlich geschützte Rechtsgüter der öffentlichen Sicherheit.

Die Abwehr sonstiger Gefahren außerhalb des strafrechtlich geschützten Bereichs wird damit an strengere Voraussetzungen geknüpft. Diese Unterscheidung ist notwendig, weil Artikel 14 Absatz 1 Buchstabe c RbDatenschutz als Übermittlungsvoraussetzungen zum einen in Ziffer ii die Verhütung von Straftaten als Übermittlungsvoraussetzung nennt und zum anderen in Ziffer iii die Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit, also beides Voraussetzungen, die nach dem innerstaatlichen Recht unter den Begriff der Gefahrenabwehr und damit unter § 10 Absatz 2 Nummer 3 BKAG zu fassen sind. Für diejenige Gefahrenabwehr, die von Artikel 14 Absatz 1 Buchstabe c RbDatenschutz als Verhütung von Straftaten erfasst ist, gilt damit § 10 Absatz 2 Nummer 3 BKAG insoweit ohne Einschränkungen; für sonstige Gefahrenabwehr müssen die qualifizierten Voraussetzungen des RbDatenschutz in deutsche Rechtsbegriffe übertragen werden. Dabei ist allgemein anerkannt, dass eine „unmittelbare“ einer gegenwärtigen Gefahr entspricht und eine „ernsthafte“ einer erheblichen Gefahr.

Nach Artikel 14 Absatz 1 Buchstabe a RbDatenschutz ist für eine Übermittlung an nicht-öffentliche Stellen stets die Zustimmung der zuständigen Behörde des Mitgliedstaates, von dem die Daten stammen, erforderlich. Dementsprechend sieht der neu einzufügende § 10 Absatz 3 Satz 2 BKAG weiterhin vor, dass eine Übermittlung von Daten nur zulässig ist, wenn die zuständige Behörde des anderen Staates, der die Daten übermittelt oder bereitgestellt hat, zugestimmt hat. Die Zustimmung kann nach Erwägungsgrund 20 RbDatenschutz auch in allgemeine Form erteilt sein.

Zu Nummer 3

Nummer 3 enthält die notwendigen Änderungen des § 14 BKAG über Befugnisse im internationalen Bereich. Nummer 3 ergänzt § 14 BKAG zunächst um einen eigenen Absatz 8 zur Umsetzung von Artikel 13 RbDatenschutz über die Weiterleitung von Daten an die zuständigen Behörden in Drittstaaten oder an internationale Einrichtungen. Artikel 13 RbDatenschutz sieht im Zusammenhang mit der Übermittlung von Daten, die von einer Behörde eines anderen Mitgliedstaates der Europäischen Union übermittelt oder bereitgestellt wurden, an Drittstaaten besondere Übermittlungsbeschränkungen vor. Grundsätzlich ist eine Übermittlung von Daten an Drittstaaten im Anwendungsbereich des RbDatenschutz nur zulässig zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen sowie nach Zustimmung der zuständigen Behörde des Mitgliedstaates.

Demgegenüber ist nach § 14 BKAG eine Übermittlung an Drittstaaten auch und gerade zu anderen polizeilichen Zwecken möglich. Der Anwendungsbereich des § 14 BKAG ist daher für die Übermittlung von Daten, die dem Bundeskriminalamt zuvor von der zuständigen Stelle eines Mitgliedstaates der Europäischen Union zum Zwecke der Verhütung und Verfolgung von Straftaten übermittelt oder bereitgestellt worden sind, auf diese Übermittlungszwecke zu beschränken. Diese Aufgabe übernimmt der neu eingefügte Absatz 8.

Nummer 3 sieht zudem den neu geschaffenen § 14 Absatz 9 BKAG-E vor. Satz 1 setzt dabei, ergänzt um die Verfahrensregelung des Satzes 2, die Ermächtigung des Artikels 13 Absatz 2 RbDatenschutz an den übermittelnden Mitgliedstaat um, die Übermittlung auch ohne vorherige Zustimmung des Herkunftsstaates vorzunehmen, wenn sie zur Abwehr einer gegenwärtigen erheblichen Gefahr oder für wesentliche Interessen eines Mitgliedstaates erforderlich ist. Die Übermittlung für Zwecke der Gefahrenabwehr, soweit es sich um Zwecke der Verhütung von Straftaten handelt, ist bereits in der bestehenden Regelung des § 14 Absatz 1 Satz 1 Nummer 3 BKAG auf die Abwehr einer erheblichen Gefahr beschränkt. Einzufügen ist daher insoweit nur die Ermächtigung, abweichend vom Regelfall ausnahmsweise ohne vorherige Zustimmung an einen Drittstaat zu übermitteln. Die Regelung ermöglicht zudem eine Übermittlung ohne vorherige Zustimmung, wenn sie für wesentliche Interessen eines Mitgliedstaates erforderlich ist, und entspricht auch insoweit dem Rahmenbeschluss.

Schließlich wird ein neuer § 14 Absatz 10 BKAG angefügt. Damit werden Regelungen aus den Artikeln 8, 9, 12 und 16 RbDatenschutz umgesetzt, wobei der neue § 14 Absatz 10 BKAG nicht auf Datenübermittlungen an EU-Mitgliedstaaten und Schengen-assoziierte Staaten beschränkt wird, sondern auch für Übermittlungen an Drittstaaten gilt.

§ 14 Absatz 10 Satz 1 und 2 BKAG-E setzt Artikel 8 RbDatenschutz zur Sicherstellung einer hohen Qualität der übermittelten Daten um.

Außerdem wird in § 14 Absatz 10 Satz 3 BKAG-E die Regelung des Artikels 9 RbDatenschutz umgesetzt, wonach die Behörde, die Daten im Anwendungsbereich des RbDatenschutz übermittelt, bei der Übermittlung oder Bereitstellung von Daten Fristen für die Aufbewahrung der Daten vorgeben kann. Hiermit soll gewährleistet werden, dass die innerstaatlichen Vorschriften zur Löschung, Sperrung oder Überprüfung der Daten auch bei ihrer Weiterleitung Berücksichtigung finden. Mit dieser Vorschrift korrespondiert die Verpflichtung des empfangenen Mitgliedstaates, derartige Vorgaben zu beachten. Sie wird für das Bundeskriminalamt in Nummer 6 umgesetzt, der den § 32 BKAG um einen entsprechenden Absatz 10 ergänzt.

Durch den neu einzufügenden § 14 Absatz 10 Satz 4 BKAG-E wird entsprechend Artikel 12 RbDatenschutz dafür Sorge getragen, dass das Bundeskriminalamt den Empfänger zur Wahrung innerstaatlicher Verarbeitungsbeschränkungen auf besondere bundesstaatliche Verwendungsregelungen hinweist.

Durch § 14 Absatz 10 Satz 5 BKAG-E wird das Bundeskriminalamt dazu ermächtigt, den empfangenden Staat zu ersuchen, den Betroffenen nicht ohne vorherige Zustimmung des Bundeskriminalamts über die Erhebung und Verarbeitung der Daten zu informieren, wenn das Bundeskriminalamt ebenfalls – allgemein oder nach den Umständen des Einzelfalls – zu einer Auskunft nicht verpflichtet wäre. Damit macht der Gesetzgeber von der ihm durch Artikel 16 Absatz 2 RbDatenschutz eingeräumten Möglichkeit Gebrauch, den Auskunftsanspruch zu übermittelten Daten zu limitieren.

Zu Nummer 4

Nummer 4 enthält eine Regelung für Datenübermittlungen an nicht-öffentliche Stellen in Mitgliedstaaten und Schengen-assoziierten Staaten. Diese Regelung trägt dem Umstand Rechnung, dass im Anwendungsbereich der Richtlinie 95/46/EG und des RbDatenschutz ein vergleichsweise hohes Datenschutzniveau verwirklicht ist, das

sich auch auf nicht-öffentliche Stellen erstreckt. Deshalb können Daten an nicht-öffentliche Stellen in anderen Mitgliedstaaten unter denselben Bedingungen wie an nationale nicht-öffentliche Stellen übermittelt werden. Die Voraussetzungen für die Übermittlung an nicht-öffentliche Stellen wurden durch Artikel 14 RbDatenschutz geändert. Für die Übermittlung an nicht-öffentliche Stellen im Inland werden diese Änderungen durch Aufnahme eines neuen Satzes 2 in § 10 Absatz 3 BKAG-E (Nummer 2) umgesetzt. Für die Übermittlung von Daten an nicht-öffentliche Stellen in Mitgliedstaaten bedarf es ebenfalls einer Umsetzung der Vorgaben des RbDatenschutz. Dies erfolgt durch die Aufnahme einer Verweisung auf § 10 Absatz 3 Satz 2 BKAG in einem neu aufzunehmenden § 14a Absatz 7 BKAG.

Eine Übermittlung zum Zwecke der Gefahrenabwehr (§ 14a Absatz 7 BKAG-E in Verbindung mit § 10 Absatz 2 Nummer 3 BKAG) ist danach nur zulässig, wenn sie zur Verhütung von Straftaten erfolgt. Ist das bedrohte Rechtsgut der öffentlichen Sicherheit nicht strafrechtlich geschützt, ist die Übermittlung nur zulässig, wenn die Gefahr gegenwärtig und erheblich ist. Diese Regelung entspricht der Systematik des Artikels 14 Absatz 1 Buchstabe c RbDatenschutz, der in Ziffer ii die Übermittlung zur Verhütung von Straftaten unter keine besonderen Voraussetzungen stellt. Gleichberechtigt und alternativ steht zu dieser Voraussetzung die Ziffer iii für die Fälle der Abwehr einer (qualifizierten) Gefahr. Da in der innerstaatlichen Rechtsordnung die Verhütung von Straftaten ebenfalls vom Begriff der Gefahrenabwehr umfasst ist, in Ziffer ii aber selbständig und ohne Qualifikation erwähnt wird, kann Ziffer iii nur die Fälle des § 10 Absatz 2 Nummer 3 BKAG betreffen, die nicht Verhütung von Straftaten sind.

Zu Nummer 5

Nummer 5 ergänzt die mit dem Gesetz zur Umsetzung des Rahmenbeschlusses 2006/960/JI über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union vom 21. Juli 2012 (BGBl. I S. 1566, 1568) eingefügte Regelung zur Verwendung von aus einem anderen Mitgliedstaat übermittelten oder zum Abruf bereitgestellten Daten und dient der Umsetzung der Artikel 11, 12 und 15 RbDatenschutz.

Zu Buchstabe a

Nummer 5 Buchstabe a passt die Überschrift an den erweiterten Regelungsgegenstand an.

Zu Buchstabe b und c

Durch die Buchstaben b und c wird der bisherige Absatz 1 zur Verwendung von nach dem Rahmenbeschluss 2006/960/JI übermittelten Daten zu Absatz 2. Dieser enthält für seinen Anwendungsbereich teilweise vom RbDatenschutz abweichende die Verwendung beschränkende Regelungen, die vom RbDatenschutz auch nicht abgelöst werden. Die allgemeineren Regelungen, die aus dem RbDatenschutz folgen, werden der spezielleren Regelung nunmehr vorangestellt. Der neue Absatz 1 überführt die Zweckbeschränkungen und die Möglichkeiten einer zweckändernden Verwendung nach Artikel 11 RbDatenschutz in das Bundeskriminalamtgesetz. Absatz 1 Satz 3 stellt sicher, dass eine Nutzung zu Forschungszwecken möglich bleibt wie dies durch Artikel 11 Satz 2 RbDatenschutz ausdrücklich ermöglicht wird. Satz 4 ergänzt die in Nummer 3 (§ 14 Absatz 10 BKAG-E) getroffene Regelung zur Berücksichtigung innerstaatlicher Verwendungsbeschränkungen. Während in Nummer 3 der Hinweis auf deutsche bundesrechtliche Verwendungsbeschränkungen an den Mitgliedstaat normiert wird, wird nun in Nummer 5 Buchstabe b die damit korrespondierende Pflicht zur Wahrung innerstaatlicher Verwendungsbeschränkungen eines anderen Mitgliedstaates festgeschrieben.

Zu Buchstabe d

Nummer 5 Buchstabe d setzt die Unterrichtungspflicht des Artikels 15 RbDatenschutz um.

Zu Nummer 6

Nummer 6 dient der Umsetzung von Artikel 9 RbDatenschutz. In dem neu angefügten Absatz 10 Satz 1 werden die Regelungen des § 32 BKAG zur Berichtigung, Löschung und Sperrung von personenbezogenen Daten in Dateien aufgrund der innerstaatlich geltenden Fristen ergänzt um eine Pflicht zur Wahrung auch der vom übermittelnden Staat mitgeteilten Fristen. Das Bundeskriminalamt hat – ungeachtet eigener ebenfalls zur Anwendung kommender Löschungsfristen – die mit den Daten übermittelten, im Einklang mit dem innerstaatlichen Recht des übermittelnden Staates stehenden Fristen zu beachten.

Die Ausnahmeregelung in Absatz 10 Satz 2 entspricht der Bestimmung in Artikel 9 Absatz 1 Satz 2 RbDatenschutz. Die Löschungspflicht steht gemäß § 32 Absatz 10 Satz 2 BKAG-E unter einem Nutzungsvorbehalt. Solange die Daten für laufende Ermittlungen, die Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen erforderlich sind, ist keine Löschung erforderlich.

Zu Artikel 2 (Änderung des Bundespolizeigesetzes)

Zu Nummer 1

Es handelt sich um eine Folgeänderung zur Neufassung der Überschrift von § 33a BKAG (Nummer 4 Buchstabe a).

Zu Nummer 2

Die Übermittlung von Daten der Mitgliedstaaten der Europäischen Union oder der Schengen-assoziierten Staaten an Drittstaaten oder zwischenstaatliche Einrichtungen darf nach Artikel 13 Absatz 1 Buchstabe a RbDatenschutz nur zur Verhütung, Ermittlung, Feststellung oder Verfolgung strafrechtlicher Sanktionen erfolgen. Dies stellt eine Verschärfung der bestehenden Ermächtigung des § 32 Absatz 3 BPolG zur Übermittlung solcher Daten dar. Sie wird daher systematisch als Spezialfall in § 32 Absatz 3 Satz 2 BPolG-E geregelt.

Zu Nummer 3

Zu Buchstabe a

Der neu eingefügte Absatz 2a soll die Umsetzung der Regelungen der Artikel 13 und 14 RbDatenschutz zum Zustimmungserfordernis der Mitgliedstaaten hinsichtlich der Weiterleitung ihrer Daten gewährleisten. Die Einschränkung der Weitergabe von Daten aus Mitgliedstaaten der Europäischen Union und aus Schengen-assoziierten Staaten an nicht-öffentliche Stellen in den Mitgliedstaaten wird durch Artikel 14 RbDatenschutz unter den Vorbehalt gewisser Erfordernisse gestellt. Hervorzuheben ist insbesondere die Zustimmung des Mitgliedstaates, welcher die Daten geliefert hat. Die Regelung, dass bei einer Übermittlung die schutzwürdigen Interessen einer Person zu berücksichtigen sind, ist insoweit schon in § 33 Absatz 3 BPolG Rechnung getragen. Die weiteren, in Artikel 14 Buchstabe c RbDatenschutz genannten, notwendigen Voraussetzungen sind in § 32 Absatz 4 BPolG bereits geregelt, wobei dieser die Befugnisse zur Übermittlung schon im Vorhinein weiter einschränkt. Demnach ist letztlich nur das Zustimmungserfordernis zu regeln.

Zu beachten ist, dass Artikel 13 RbDatenschutz ebenfalls ein Zustimmungserfordernis vorsieht, soweit Daten aus dem Anwendungsbereich des RbDatenschutz an Drittstaaten oder zwischenstaatliche Einrichtungen weitergegeben werden. Diesem Zustimmungserfordernis soll durch Absatz 2a gebündelt Rechnung getragen werden. Da die Möglichkeit der Weitergabe ohne Zustimmung nur für den Fall der Weiterleitung an die zuständigen Behörden in Drittstaaten oder an zwischenstaatliche Einrichtungen (Artikel 13 RbDatenschutz) vorgesehen ist, ist diesem durch besondere Regelung nur für diesen Fall Rechnung getragen worden.

Zu Buchstabe b

Durch die in Absatz 6 neu eingefügten Sätze 5, 6 und 7 wird die Möglichkeit eines Ersuchens des Empfängerstaates um den Verzicht der Information des Betroffenen ermöglicht. Dies soll die Bundespolizei zu einer Abstimmung mit dem Empfängerstaat befähigen, um eventuelle polizeiliche Maßnahmen nicht zu gefährden. Diese Möglichkeit wird durch Artikel 16 Absatz 2 RbDatenschutz gegeben.

Zu Buchstabe c

Die Änderung folgt der entsprechenden Vorschrift des § 11 Absatz 6 BKAG, so dass künftig nicht mehr wie bisher lediglich jede zehnte, sondern jede Abfrage protokolliert wird. Entsprechend wird in diesem Gesetzentwurf auch die Bestimmung des § 488 Absatz 3 Satz 5 StPO-E von einer Soll-Bestimmung von zehn Prozent auf eine Vollprotokollierung umgestellt. Eine abweichende Protokollierungsquote zu den Bestimmungen des Bundeskriminalamtgesetzes und der Strafprozessordnung wäre sachlich nicht nachvollziehbar. Auch der weitere Zweck der Protokolldatenauswertung, die Verwendung zur Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person, kann sinnvoll nur mit einer Vollprotokollierung erfüllt werden.

Zu Buchstabe d

Der neu einzufügende Absatz 9 soll die vom Rahmenbeschluss geforderte Datenqualität von zu übersendenden Daten sichern. Diese Vorgabe wird in Artikel 8 Absatz 1 RbDatenschutz gemacht.

Als Regelungsstandort wurde hier § 33 BPolG gewählt, da hierdurch zentrale Regelungen vorgenommen werden können. Dies ist insbesondere vor dem Hintergrund der Regelung zur Datenqualität erforderlich, da somit eine generelle Regelung für die Versendung der Daten geschaffen wird. Auch sind die Regelungen hier systematisch sinnvoll, da es sich um ergänzende Regelungen zur Übermittlung von Daten handelt. So regelt Absatz 2 das Zustimmungserfordernis bei einer Übermittlung von Daten der Mitgliedstaaten vollumfänglich. Die Sätze 5, 6 und 7 präzisieren den Absatz 6 hinsichtlich der Vorgaben des Rahmenbeschlusses an den Empfänger von Daten. Absatz 9 regelt die Vorgaben des Rahmenbeschlusses zur Datenqualität ebenfalls zentral und umfänglich.

Zu Nummer 4

Die Ergänzungen des aufgrund des Rahmenbeschlusses 2006/960/JI eingeführten § 33a BPolG ergeben sich aufgrund der Erweiterung von Regelungen, welche für die Verwendung von aus Mitgliedstaaten der Europäischen Union oder aus Schengen-assoziierter Staaten übermittelten Daten gelten. Zu nennen sind insbesondere die Artikel 11, 12 und 15 RbDatenschutz.

Da diese Regelungen des RbDatenschutz neben den Regelungen bestehen, die durch den Rahmenbeschluss 2006/960/JI eingeführt worden sind, jedoch auch die Verwendung von Daten betreffen, die aus Mitgliedstaaten der Europäischen Union oder aus Schengen-assoziierten Staaten übermittelt worden sind, ist eine Regelung in § 33a BPolG zusammen mit diesen Regelungen sinnvoll. Der RbDatenschutz gilt nicht alternativ, sondern zusätzlich zum Rahmenbeschluss 2006/960/JI, so lange nicht dessen Spezialregelungen Vorrang beanspruchen. Der Rahmenbeschluss 2006/960/JI hat einen engeren Anwendungsbereich als der RbDatenschutz. Die allgemeinere Regelung stellt daher der RbDatenschutz dar. Demnach sind diese Regelungen voranzustellen.

Zu Buchstabe a

Nummer 4 Buchstabe a passt die Überschrift an den erweiterten Regelungsgegenstand an.

Zu Buchstabe b

Umgesetzt werden in Absatz 1 und Absatz 2 Satz 1 und 2 zunächst die Einschränkungen der Verwendung personenbezogener Daten, welche durch einen Mitgliedstaat der Europäischen Union oder durch einen Schengen-assoziierten Staat bereitgestellt wurden (Artikel 11 RbDatenschutz). Die Regelung eines Zustimmungserfordernisses ist hier, getrennt von dem generellen Zustimmungserfordernis in § 33 Absatz 2 BPolG, sinnvoll. Dies begründet sich dadurch, dass hier der Sonderfall der Verwendung der Daten für andere Zwecke geregelt wird, als bei der Übermittlung vorgesehen waren.

Absatz 2 Satz 3 stellt sicher, dass die Verwendung, wie in Artikel 12 RbDatenschutz gefordert, im Rahmen des Rechts des sendenden Mitgliedstaates oder des Schengen-assoziierten Staates bleibt, auf das dieser hinweist.

Zu Buchstabe c

Es handelt sich um eine redaktionelle Folgeänderung zu Buchstabe b.

Zu Buchstabe d

Nummer 4 Buchstabe d setzt die Unterrichtungspflicht des Artikels 15 RbDatenschutz um.

Zu Nummer 5

Die Ergänzung von § 35 BPolG um einen Absatz 10 dient der Umsetzung von Artikel 9 RbDatenschutz. Die in § 35 BPolG bereits bestehenden Regelungen der Berichtigung, Löschung und Sperrung personenbezogener Daten in Dateien aufgrund der innerstaatlich geltenden Fristen werden ergänzt um eine Pflicht zur Wahrung auch der vom übermittelnden Staat mitgeteilten Fristen. Die Bundespolizei hat diese, ungeachtet eigener ebenfalls zur Anwendung kommender Löschungsfristen, zu beachten. Die Ausnahmeregelung in Absatz 10 Satz 2 entspricht der Bestimmung in Artikel 9 Absatz 1 Satz 2 RbDatenschutz. Hiernach ist keine Löschung erforderlich, solange die Daten für laufende Ermittlungen, die Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen erforderlich sind.

Zu Artikel 3 (Änderung des Zollfahndungsdienstgesetz)

Zu Nummer 1

Es handelt sich um eine Folgeänderung zur Neufassung der Überschrift von § 35a ZFdG (Nummer 5 Buchstabe a).

Zu Nummer 2

Artikel 10 Absatz 1 RbDatenschutz schreibt die Protokollierung oder Dokumentierung jeder Übermittlung von personenbezogenen Daten zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung und der Sicherstellung der Integrität und Sicherheit der Daten vor. Nach § 11 Absatz 4 Satz 1 ZFdG muss bislang lediglich bei jedem zehnten Abruf eine Protokollierung erfolgen.

Die danach erforderliche Änderung entspricht der bereits bestehenden Regelung in der Parallelvorschrift des § 11 Absatz 6 BKAG, nach der dort jede Abfrage protokolliert wird. Entsprechend den Vorgaben des RbDatenschutz werden in diesem Gesetzentwurf auch die Bestimmungen des § 33 Absatz 8 Satz 1 BPolG-E sowie des § 488 Absatz 3 Satz 5 StPO-E auf eine Vollprotokollierung umgestellt. Eine abweichende Protokollierungsquote zu diesen Bestimmungen wäre sachlich nicht nachvollziehbar.

Auch die Verwendungszwecke der protokollierten Daten können sinnvoll nur mit einer Vollprotokollierung erfüllt werden. Zugleich werden somit also die Voraussetzungen dafür geschaffen, dass die nach Artikel 22 Absatz 2 Buchstabe f RbDatenschutz für die automatisierte Datenverarbeitung zu gewährleistende Übermittlungskontrolle durchgeführt werden kann.

Die Regelung des § 11 Absatz 4 Satz 1 ZFdG-E gilt für die Datenübermittlung im innerstaatlichen Bereich durch den Verweis in § 33 Absatz 4 Satz 3 ZFdG entsprechend.

Zu Nummer 3

Nummer 3 dient vordringlich der Umsetzung von Artikel 14 RbDatenschutz über die Übermittlung von Daten an nicht-öffentliche Stellen in Mitgliedstaaten.

Zu Buchstabe a

Die Hinweispflicht des Artikels 14 Absatz 2 RbDatenschutz war bereits im BKAG enthalten und wird nunmehr durch Nummer 1 Buchstabe a in § 33 Absatz 3 Satz 3 ZFdG-E neu eingefügt.

Zu Buchstabe b

Die Änderung entspricht der Änderung in Artikel 1 Nummer 2 und dient für das Zollfahndungsdienstgesetz der Umsetzung von Artikel 14 RbDatenschutz über die Übermittlung von Daten an nicht-öffentliche Stellen in Mitgliedstaaten. Es werden gegenüber dem bisherigen § 33 Absatz 5 ZFdG zusätzliche einschränkende Voraussetzungen vorgesehen, unter denen personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates für Zwecke der Gefahrenabwehr übermittelt oder bereitgestellt wurden, an nicht-öffentliche Stellen weitergeleitet werden dürfen.

Die in Artikel 11 RbDatenschutz ebenfalls vorgesehenen Verwendungsbeschränkungen für personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaates im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen übermittelt oder bereitgestellt wurden, gelten zwar ebenfalls für sonstige innerstaatliche Übermittlungen im Anwendungsbereich des § 33 ZFdG, haben darüber hinaus aber einen weiteren Anwendungsbereich, da sie sonstige Formen der Verarbeitung und der Nutzung der Daten einschließen. Als Regelungsstandort für die Umsetzung des Artikels 11 RbDatenschutz wurde daher nicht § 33, sondern § 35a ZFdG gewählt.

Die Änderung ergänzt § 33 Absatz 5 ZFdG über Datenübermittlungen an innerstaatliche nicht-öffentliche Stellen um einschränkende Voraussetzungen. § 33 Absatz 5 Satz 1 i. V. m. Absatz 1 Satz 2 ZFdG enthält die Voraussetzungen einer Übermittlung an nicht-öffentliche Stellen. Nach geltender Rechtslage ist eine Übermittlung danach zulässig zur Erfüllung der Aufgaben der Behörden des Zollfahndungsdienstes nach dem Zollfahndungsdienstgesetz, für Zwecke der Strafverfolgung, der Strafvollstreckung, des Strafvollzugs und der Gnadenverfahren, für Zwecke der Gefahrenabwehr oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner. Mit Nummer 3 Buchstabe b wird ein neuer Satz 2 in § 33 Absatz 5 ZFdG eingefügt, nach dem eine Übermittlung zur Gefahrenabwehr nach Absatz 1 Satz 2 Nummer 3 nur zulässig ist, wenn sie zur Verhütung von Straftaten oder

sonst zur Abwehr einer gegenwärtigen und erheblichen Gefahr erfolgt. Gemeint sind damit Gefahren für nicht strafrechtlich geschützte Rechtsgüter der öffentlichen Sicherheit.

Die Abwehr sonstiger Gefahren außerhalb des strafrechtlich geschützten Bereichs wird damit an strengere Voraussetzungen geknüpft. Diese Unterscheidung ist notwendig, weil Artikel 14 Absatz 1 Buchstabe c RbDatenschutz als Übermittlungsvoraussetzungen zum einen in Ziffer ii die Verhütung von Straftaten als Übermittlungsvoraussetzung nennt und zum anderen in Ziffer iii die Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit, also beides Voraussetzungen, die nach dem innerstaatlichen Recht unter den Begriff der Gefahrenabwehr und damit unter § 33 Absatz 1 Satz 2 Nummer 3 ZFdG zu fassen sind. Für diejenige Gefahrenabwehr, die von Artikel 14 Absatz 1 Buchstabe c RbDatenschutz als Verhütung von Straftaten erfasst ist, gilt damit § 33 Absatz 1 Satz 2 Nummer 3 ZFdG insoweit ohne Einschränkungen; für sonstige Gefahrenabwehr müssen die qualifizierten Voraussetzungen des RbDatenschutz in deutsche Rechtsbegriffe übertragen werden. Dabei ist allgemein anerkannt, dass eine „unmittelbare“ einer gegenwärtigen Gefahr entspricht und eine „ernsthafte“ einer erheblichen Gefahr.

Nach Artikel 14 Absatz 1 Buchstabe a RbDatenschutz ist für eine Übermittlung an nicht-öffentliche Stellen stets die Zustimmung der zuständigen Behörde des Mitgliedstaates, von dem die Daten stammen, erforderlich. Dementsprechend sieht der neu einzufügende § 33 Absatz 5 Satz 2 ZFdG-E weiterhin vor, dass eine Übermittlung von Daten nur zulässig ist, wenn die zuständige Behörde des anderen Staates, der die Daten übermittelt oder bereitgestellt hat, zugestimmt hat. Die Zustimmung kann nach Erwägungsgrund 20 RbDatenschutz auch in allgemeine Form erteilt sein.

Zu Buchstabe c

Die Regelung entspricht § 10 Absatz 4 BKAG. Sie erfolgt außerhalb der Umsetzung des RbDatenschutz hinaus und wird in das Zollfahndungsdienstgesetz aufgenommen, damit dessen Regelungen zum Datenaustausch auch in dieser Frage so weit wie möglich denjenigen des Bundeskriminalamtgesetzes entsprechen.

Zu Buchstabe d

Es handelt sich um eine Folgeänderung zu Buchstabe c.

Zu Nummer 4

Nummer 4 enthält die notwendigen Änderungen des § 34 ZFdG über Befugnisse im internationalen Bereich. Nummer 4 ergänzt § 34 ZFdG zunächst um einen eigenen Absatz 5 zur Umsetzung von Artikel 13 RbDatenschutz über die Weiterleitung von Daten an die zuständigen Behörden in Drittstaaten oder an internationale Einrichtungen. Artikel 13 RbDatenschutz sieht im Zusammenhang mit der Übermittlung von Daten, die von einer Behörde eines anderen Mitgliedstaates der Europäischen Union übermittelt oder bereitgestellt wurden, an Drittstaaten besondere Übermittlungsbeschränkungen vor. Grundsätzlich ist eine Übermittlung von Daten an Drittstaaten im Anwendungsbereich des RbDatenschutz nur zulässig zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen sowie nach Zustimmung der zuständigen Behörde des Mitgliedstaates.

Demgegenüber ist nach § 34 ZFdG eine Übermittlung an Drittstaaten auch und gerade zu anderen polizeilichen Zwecken möglich. Der Anwendungsbereich des § 34 ZFdG ist daher für die Übermittlung von Daten, die den Behörden des Zollfahndungsdienstes zuvor von der zuständigen Stelle eines Mitgliedstaates der Europäischen Union zum Zwecke der Verhütung und Verfolgung von Straftaten übermittelt oder bereitgestellt worden sind, auf diese Übermittlungszwecke zu beschränken. Diese Aufgabe übernimmt der neu eingefügte Absatz 5.

Nummer 4 sieht zudem den neu geschaffenen § 34 Absatz 6 ZFdG-E vor. Satz 1 setzt dabei, ergänzt um die Verfahrensregelung des Satzes 2, die Ermächtigung des Artikels 13 Absatz 2 RbDatenschutz an den übermittelnden Mitgliedstaat um, die Übermittlung auch ohne vorherige Zustimmung des Herkunftsstaates vorzunehmen, wenn sie zur Abwehr einer gegenwärtigen erheblichen Gefahr oder für wesentliche Interessen eines Mitgliedstaates erforderlich ist. Die Übermittlung für Zwecke der Gefahrenabwehr, soweit es sich um Zwecke der Verhütung von Straftaten handelt, ist bereits in der bestehenden Regelung des § 34 Absatz 1 Satz 1 Nummer 3 ZFdG auf die Abwehr einer erheblichen Gefahr beschränkt. Einzufügen ist daher insoweit nur die Ermächtigung, abweichend vom Regelfall ausnahmsweise ohne vorherige Zustimmung an einen Drittstaat zu übermitteln. Die Regelung ermöglicht zudem eine Übermittlung ohne vorherige Zustimmung, wenn sie für wesentliche Interessen eines Mitgliedstaates erforderlich ist, und entspricht auch insoweit dem Rahmenbeschluss.

Schließlich wird ein neuer § 34 Absatz 7 ZFdG-E angefügt. Damit werden Regelungen aus den Artikeln 8, 9, 12 und 16 RbDatenschutz umgesetzt, wobei der neue § 34 Absatz 7 ZFdG nicht auf Datenübermittlungen an EU-Mitgliedstaaten und Schengen-assoziierte Staaten beschränkt wird, sondern auch für Übermittlungen an Drittstaaten gilt.

§ 34 Absatz 7 Satz 1 und 2 ZFdG-E setzt Artikel 8 RbDatenschutz zur Sicherstellung einer hohen Qualität der übermittelten Daten um.

Außerdem wird in § 34 Absatz 7 Satz 3 ZFdG-E die Regelung des Artikels 9 RbDatenschutz umgesetzt, wonach die Behörde, die Daten im Anwendungsbereich des RbDatenschutz übermittelt, bei der Übermittlung oder Bereitstellung von Daten Fristen für die Aufbewahrung der Daten vorgeben kann. Hiermit soll gewährleistet werden, dass die innerstaatlichen Vorschriften zur Löschung, Sperrung oder Überprüfung der Daten auch bei ihrer Weiterleitung Berücksichtigung finden. Mit dieser Vorschrift korrespondiert die Verpflichtung des empfangenen Mitgliedstaates, derartige Vorgaben zu beachten. Sie wird für die Behörden des Zollfahndungsdienstes in Nummer 7 umgesetzt, der den § 39 ZFdG um einen entsprechenden Absatz 11 ergänzt.

Durch den neu einzufügenden § 34 Absatz 7 Satz 4 ZFdG-E wird entsprechend Artikel 12 RbDatenschutz dafür Sorge getragen, dass die Behörden des Zollfahndungsdienstes den Empfänger zur Wahrung innerstaatlicher Verarbeitungsbeschränkungen auf besondere bundesstaatliche Verwendungsregelungen hinweist.

Durch § 34 Absatz 7 Satz 5 ZFdG-E werden die Behörden des Zollfahndungsdienstes dazu ermächtigt, den empfangenden Staat zu ersuchen, den Betroffenen nicht ohne vorherige Zustimmung der Behörden des Zollfahndungsdienstes über die Erhebung und Verarbeitung der Daten zu informieren, wenn die Behörden des Zollfahndungsdienstes ebenfalls – allgemein oder nach den Umständen des Einzelfalls – zu einer Auskunft nicht verpflichtet wären. Damit macht der Gesetzgeber von der ihm durch Artikel 16 Absatz 2 RbDatenschutz eingeräumten Möglichkeit Gebrauch, den Auskunftsanspruch zu übermittelten Daten zu limitieren.

Zu Nummer 5

Nummer 5 enthält eine Regelung für Datenübermittlungen an nicht-öffentliche Stellen in Mitgliedstaaten und Schengen-assoziierten Staaten. Diese Regelung trägt dem Umstand Rechnung, dass im Anwendungsbereich der Richtlinie 95/46/EG und des RbDatenschutz ein vergleichsweise hohes Datenschutzniveau verwirklicht ist, das sich auch auf nicht-öffentliche Stellen erstreckt. Deshalb können Daten an nicht-öffentliche Stellen in anderen Mitgliedstaaten unter denselben Bedingungen wie an nationale nicht-öffentliche Stellen übermittelt werden. Die Voraussetzungen für die Übermittlung an nicht-öffentliche Stellen wurden durch Artikel 14 RbDatenschutz geändert. Für die Übermittlung an nicht-öffentliche Stellen im Inland werden diese Änderungen durch Aufnahme eines neuen Satzes 2 in § 33 Absatz 5 ZFdG-E (Nummer 3) umgesetzt. Für die Übermittlung von Daten an nicht-öffentliche Stellen in Mitgliedstaaten bedarf es ebenfalls einer Umsetzung der Vorgaben des RbDatenschutz. Dies erfolgt durch die Aufnahme einer Verweisung auf § 33 Absatz 5 Satz 2 ZFdG in einem neu aufzunehmenden § 34a Absatz 7 ZFdG-E.

Eine Übermittlung zum Zwecke der Gefahrenabwehr (§ 34a Absatz 7 ZFdG-E i. V. m. § 33 Absatz 1 Satz 2 Nummer 3 ZFdG) ist danach nur zulässig, wenn sie zur Verhütung von Straftaten erfolgt. Ist das bedrohte Rechtsgut der öffentlichen Sicherheit nicht strafrechtlich geschützt, ist die Übermittlung nur zulässig, wenn die Gefahr gegenwärtig und erheblich ist. Diese Regelung entspricht der Systematik des Artikels 14 Absatz 1 Buchstabe c RbDatenschutz, der in Ziffer ii die Übermittlung zur Verhütung von Straftaten unter keine besonderen Voraussetzungen stellt. Gleichberechtigt und alternativ steht zu dieser Voraussetzung die Ziffer iii für die Fälle der Abwehr einer (qualifizierten) Gefahr. Da in der innerstaatlichen Rechtsordnung die Verhütung von Straftaten ebenfalls vom Begriff der Gefahrenabwehr umfasst ist, in Ziffer ii aber selbständig und ohne Qualifikation erwähnt wird, kann Ziffer iii nur die Fälle des § 33 Absatz 1 Satz 2 Nummer 3 ZFdG betreffen, die nicht Verhütung von Straftaten sind.

Zu Nummer 6

Nummer 6 ergänzt die mit dem Gesetz zur Umsetzung des Rahmenbeschlusses 2006/960/JI über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union vom 21. Juli 2012 (BGBl. I S. 1566) eingefügte Regelung zur Verwendung von aus einem anderen Mitgliedstaat übermittelten oder zum Abruf bereitgestellten Daten und dient der Umsetzung von Artikel 11, 12 und 15 RbDatenschutz.

Zu Buchstabe a

Nummer 6 Buchstabe a passt die Überschrift an den erweiterten Regelungsgegenstand an.

Zu Buchstabe b und c

Durch die Buchstaben b und c wird der bisherige Absatz 1 zur Verwendung von nach dem Rahmenbeschluss 2006/960/JI übermittelten Daten zu Absatz 2. Dieser enthält für seinen Anwendungsbereich teilweise vom RbDatenschutz abweichende die Verwendung beschränkende Regelungen, die vom RbDatenschutz auch nicht abgelöst werden. Die allgemeineren Regelungen, die aus dem RbDatenschutz folgen, werden der spezielleren Regelung nunmehr vorangestellt. Der neue Absatz 1 überführt die Zweckbeschränkungen und die Möglichkeiten einer zweckändernden Verwendung nach Artikel 11 RbDatenschutz in das Zollfahndungsdienstgesetz. Absatz 1 Satz 4 stellt sicher, dass eine Nutzung zu Forschungszwecken möglich bleibt, wie dies durch Artikel 11 Satz 2 RbDatenschutz ausdrücklich ermöglicht wird. Satz 5 ergänzt die in Nummer 3 getroffene Regelung zur Berücksichtigung innerstaatlicher Verwendungsbeschränkungen. Während in Nummer 4 (§ 34 Absatz 7 ZFdG-E) der Hinweis auf bundesrechtliche Verwendungsbeschränkungen an den Mitgliedstaat normiert wird, wird nun in Nummer 6 Buchstabe b die damit korrespondierende Pflicht zur Wahrung innerstaatlicher Verwendungsbeschränkungen eines anderen Mitgliedstaates begründet.

Zu Buchstabe d

Nummer 6 Buchstabe d setzt die Unterrichtungspflicht des Artikels 15 RbDatenschutz um.

Zu Nummer 7

Nummer 7 dient der Umsetzung von Artikel 9 RbDatenschutz. In dem neu angefügten § 39 Absatz 11 Satz 1 ZFdG-E werden die Regelungen des § 39 ZFdG zur Berichtigung, Löschung und Sperrung von personenbezogenen Daten in Dateien aufgrund der innerstaatlich geltenden Fristen ergänzt um eine Pflicht zur Wahrung auch der vom übermittelnden Staat mitgeteilten Fristen. Die Behörden des Zollfahndungsdienstes haben – ungeachtet eigener ebenfalls zur Anwendung kommender Löschungsfristen – die mit den Daten übermittelten, im Einklang mit dem innerstaatlichen Recht des übermittelnden Staates stehenden Fristen zu beachten.

Die Ausnahmeregelung in Absatz 11 Satz 2 entspricht der Bestimmung in Artikel 9 Absatz 1 Satz 2 RbDatenschutz. Die Löschungspflicht steht gemäß § 39 Absatz 11 Satz 2 ZFdG-E unter einem Nutzungsvorbehalt. Solange die Daten für laufende Ermittlungen, die Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen erforderlich sind, ist keine Löschung erforderlich.

Zu Artikel 4 (Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen)

Zu Nummer 1

Die Anpassung der Inhaltsübersicht ist aufgrund der Änderungen erforderlich, die im IRG vorgenommen werden.

Zu Nummer 2

In den Elften Teil des IRG werden datenschützende Regelungen eingestellt, die zur bereichsspezifischen Umsetzung des RbDatenschutz erforderlich sind.

Der Elfte Teil differenziert dabei nicht nach „eingehenden“ und „ausgehenden“ Ersuchen, sondern lediglich nach eingehenden und ausgehenden personenbezogenen Daten. Die dortigen Regeln zum Schutz personenbezogener Daten sind damit grundsätzlich sowohl auf die Erledigung eingehender Rechtshilfeersuchen als auch auf ausgehende Ersuchen anwendbar. Sowohl bei eingehenden Ersuchen als auch bei ausgehenden Ersuchen kommt es regelmäßig zu einer Datenübermittlung durch die nationalen Strafverfolgungsbehörden der beteiligten Staaten oder Institutionen. Beispielsweise zielen Ersuchen, die Deutschland aus einem Mitgliedstaat der Europäischen Union erhält, vor allem darauf ab, dass die deutschen Behörden in Erledigung des Ersuchens Daten an das Ausland übermitteln. Bereits das Ersuchen selbst enthält aber regelmäßig ebenfalls personenbezogene Daten, die dann von den deutschen Behörden verwendet werden könnten. Umgekehrt übermitteln deutsche Behörden in einem Ersuchen an einen anderen Mitgliedstaat regelmäßig personenbezogene Daten und erhalten in Erledigung des Ersuchens gegebenenfalls weitere personenbezogene Daten. Für das Recht einer betroffenen Person auf einen angemessenen Schutz ihrer Daten ist es ohne Bedeutung, ob die Daten bei eingehenden oder ausgehenden Ersuchen

erlangt oder verwendet wurden. Dementsprechend behandelt der Gesetzentwurf die Verwendung von Daten im Rahmen von eingehenden und ausgehenden Ersuchen im Grundsatz gleich.

Bezüglich des Verhältnisses der Regelungen im Elften Teil zu den bereits bestehenden datenschützenden Vorschriften im IRG sowie zu den datenschützenden Vorschriften ins-besondere der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten wird auf die Anmerkungen im Allgemeinen Teil der Begründung verwiesen.

Zur Überschrift

Die Überschrift ist allgemein gehalten und spricht – vergleichbar der Formulierung in § 1 Absatz 1 IRG – vereinfachend vom Datenschutz im Zusammenhang mit dem Rechtshilfeverkehr innerhalb der Europäischen Union und mit den Schengen-assoziierten Staaten. Der Begriff „Rechtshilfeverkehr" nimmt auf § 1 Absatz 1 IRG Bezug und meint also den Rechtshilfeverkehr in strafrechtlichen Angelegenheiten im Sinne des IRG. Dies sind gemäß § 1 Absatz 2 IRG auch Verfahren wegen einer Tat, die nach deutschem Recht als Ordnungswidrigkeit mit Geldbuße oder die nach ausländischem Recht mit einer vergleichbaren Sanktion bedroht ist, sofern über deren Festsetzung ein auch für Strafsachen zuständiges Gericht entscheiden kann. Der Begriff erfasst den Aus- und Durchlieferungsverkehr ebenso wie die Vollstreckungshilfe und die sonstige Rechtshilfe, gleichgültig, ob sie auf der Grundlage der tradierten Rechtshilfe oder auf der Grundlage des Prinzips der gegenseitigen Anerkennung erfolgen oder welche Strafverfolgungsbehörden und Gerichte tätig werden. Abweichend von dem bisherigen Sprachgebrauch im IRG wird bewusst nicht die Formulierung „Rechtshilfe mit den Mitgliedstaaten der Europäischen Union" verwendet. Damit wird dem Umstand Rechnung getragen, dass die Vorgaben des RbDatenschutz auch dann einzuhalten sind, wenn personenbezogene Daten an Behörden oder Informationssysteme nach dem Dritten Teil Titel V Kapitel 4 und 5 AEUV übermittelt oder für diese bereitgestellt oder von diesen empfangen werden. Die Formulierung „im Zusammenhang mit dem Rechtshilfeverkehr" soll verdeutlichen, dass die Regelungen des Elften Teils nicht nur im Rechtshilfeverfahren gelten sollen, sondern dass insbesondere die Verwendungsregelungen auch innerstaatlich wirken, siehe die Anmerkungen im Allgemeinen Teil der Begründung.

Zu § 97a IRG-E – Anwendungsbereich

Die Vorschrift umschreibt den Anwendungsbereich der §§ 97a ff. IRG-E.

Zu Absatz 1

Nach Nummer 1 ist eine Voraussetzung dafür, dass der Anwendungsbereich des Elften Teils eröffnet ist, zunächst, dass personenbezogene Daten ganz oder teilweise automatisiert erhoben, verarbeitet oder genutzt werden (Buchstabe a). Dies ist beispielsweise der Fall bei elektronisch geführten Akten, soweit sie eingeführt sind. Auch Übermittlungen von personenbezogenen Daten, die per E-Mail erfolgen, fallen in den Anwendungsbereich, da die Übermittlung eine Form der Verarbeitung von Daten ist.

Alternativ dazu ist der Anwendungsbereich des Elften Teils auch dann eröffnet, wenn personenbezogene Daten zwar nicht automatisiert erhoben, verarbeitet oder genutzt werden, aber in einer Datei gespeichert sind oder werden sollen (Buchstabe b). Im letztgenannten Fall ist darauf abzustellen, ob der deutschen Stelle im Zeitpunkt des Umgangs mit personenbezogenen Daten bekannt ist, ob eine Speicherungsabsicht besteht. Eine Pflicht, dies aktiv in Erfahrung zu bringen, sieht der RbDatenschutz nicht vor. Regelmäßig wird deshalb eine Schlüssigkeitsprüfung ausreichen und eine vertiefte Überprüfung nur anlassbezogen erforderlich sein. Praktische Bedeutung kann der Regelung beispielsweise zukommen, wenn deutsche Strafverfolgungsbehörden auf der Grundlage von § 6 des Eurojust-Gesetzes (EJG) personenbezogene Daten, die nicht in Dateien gespeichert sind, etwa per Post an Eurojust übermitteln, da diese Informationen im Fallbearbeitungssystem von Eurojust gespeichert werden, §§ 4a, 4b Absatz 1 EJG. Der Anwendungsbereich der datenschützenden Regelungen im Elften Teil ist also unabhängig davon eröffnet, ob die Informationen von den deutschen Behörden in elektronischer Form an Eurojust übermittelt werden oder ob die Informationen bereits in Deutschland elektronisch gespeichert waren.

Im Übrigen liegt der Regelung in Übereinstimmung mit dem Wortlaut von Artikel 1 Absatz 3 RbDatenschutz das Verständnis zugrunde, dass die papiergeführte Akte als eine bloße Blattsammlung nicht von dem Anwendungsbereich des Rahmenbeschlusses erfasst wird, siehe die Anmerkungen im Allgemeinen Teil der Begründung.

Nummer 2 ergänzt die Nummer 1 und enthält weitere Eingrenzungen des Anwendungs-bereichs. Die personenbezogenen Daten müssen grenzüberschreitend „übermittelt" oder „bereitgestellt" werden. Beide Begriffe, die aus Artikel 1 Absatz 2 RbDatenschutz übernommen werden, setzen ein bewusstes Handeln der übermittelnden oder bereitstellenden Stelle voraus. Ein bloßes Bekanntwerden von personenbezogenen Daten eröffnet den Anwendungsbereich der §§ 97a ff. IRG-E nicht. Die Formulierung „übermitteln" ist dabei im Sinne eines gezielten Zur-

Verfügung-Stellens von Daten zu verstehen. Die Formulierung „bereitstellen“ erfasst das unspezifische Zur-Verfügung-Stellen von Daten zur Einsicht oder zum Abruf, beispielsweise durch Einstellen von Daten in eine Datenbank (vgl. insoweit § 3 Absatz 4 Nummer 3 BDSG).

Als Gegenstück zur aktiven grenzüberschreitenden „Übermittlung“ und „Bereitstellung“ nennt Absatz 1 Nummer 2 auch das passive „Empfangen“ der personenbezogenen Daten. Dies entspricht den Vorgaben von Artikel 1 Absatz 2 Buchstabe a bis c RbDatenschutz, die jeweils den Datenaustausch zwischen den Mitgliedstaaten untereinander und zwischen den Mitgliedstaaten und den genannten Institutionen der Europäischen Union erfassen, so dass beide Seiten eines Datenaustauschs, die Übermittlung oder Bereitstellung ebenso wie das Empfangen, erfasst sind.

Als weitere Voraussetzung dafür, dass der Anwendungsbereich des Elften Teils eröffnet ist, sieht die Regelung in Nummer 2 vor, dass die Daten nach Nummer 1 mit den Mitglied-staaten der Europäischen Union oder mit den europäischen Behörden oder Informations-systemen nach dem Dritten Teil Titel V Kapitel 4 und 5 AEUV ausgetauscht werden. Der Norm liegt dabei das Verständnis zugrunde, dass bei eingehenden personenbezogenen Daten nur echte „Fremddaten“ erfasst werden. Stammen die aus dem europäischen Ausland erhaltenen personenbezogenen Daten dagegen ursprünglich aus Deutschland, verpflichtet der RbDatenschutz nicht dazu, seine Vorgaben – insbesondere die Zustimmungserfordernisse – einzuhalten. Erwägungsgrund 9 zum RbDatenschutz weist hierauf ausdrücklich hin. Zu den europäischen Behörden oder Informationssystemen im Sinne der Norm zählen zum Beispiel Europol, Eurojust, das Schengener Informationssystem (SIS) oder das Zollinformationssystem (ZIS). Während Artikel 1 Absatz 1 RbDatenschutz solche Stellen erfasst, die aufgrund von Titel VI EUV errichtet wurden, soll hier der AEUV als das jüngere Regelwerk in Bezug genommen werden. Damit wird der Anwendungsbereich der nationalen datenschützenden Regelungen gegenüber den Vorgaben des RbDatenschutz leicht erweitert, weil in dem Dritten Teil Titel V Kapitel 4 und 5 AEUV beispielsweise auch die neu einzurichtende Europäische Staatsanwaltschaft enthalten ist. Diese Erweiterung erscheint sachgerecht, weil für den gesamten Rechtshilfeverkehr zwischen deutschen Behörden und anderen Mitgliedstaaten oder Einrichtungen der Europäischen Union ein einheitliches Datenschutzniveau herrschen soll.

Aus Erwägungsgrund 39 zum RbDatenschutz ergibt sich, dass die Vorgaben geschlossener datenschützender Regelwerke der Europäischen Union Vorrang haben gegenüber den Regelungen des RbDatenschutz. Beispielhaft werden insoweit die Datenschutzvorschriften von Eurojust, Europol, des SIS oder des ZIS genannt. Der nationale Gesetzgeber ist also gehindert, Regelungen zu treffen, die mit den vorhandenen europäischen Regelwerken kollidieren oder in Kompetenzen der europäischen Rechtsetzung eingreifen. Er darf aber regeln, welche datenschützenden Vorschriften einzuhalten sind, wenn die nationalen Behörden personenbezogene Daten zum Beispiel an Eurojust übermitteln oder wenn sie solche Daten von Eurojust erhalten.

Außerhalb der vorstehend beschriebenen geschlossenen europarechtlichen Regelwerke zum Datenschutz sollen die datenschutzrechtlichen Vorschriften früherer europäischer Rechtsakte nur dann zur Anwendung gelangen, wenn sie – unter dem Gesichtspunkt des Datenschutzes – strenger sind als die Bestimmungen des RbDatenschutz, siehe Artikel 28 und Erwägungsgrund 40 zum RbDatenschutz. Strengere Bestimmungen, die keine bereichsspezifische Umsetzung erfahren haben, sind nicht ersichtlich. Insbesondere reichen die datenschützenden Bestimmungen aus Artikel 23 Absatz 1 des Übereinkommens vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (EU-RhÜbk) nicht weiter als die des RbDatenschutz. Dagegen ist Artikel 8 Absatz 3 des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (RbDatA, ABl. L 386 vom 29.12.2006, S. 89), der bereichsspezifisch durch § 92b IRG umgesetzt wurde, enger. § 92b IRG bleibt deshalb unberührt, vgl. auch die Anmerkungen im Allgemeinen Teil der Begründung.

Zu Absatz 2

Mit Absatz 2 werden die Schengen-assoziierten Staaten (derzeit: Island, Liechtenstein, Norwegen und Schweiz) den Mitgliedstaaten der Europäischen Union gleichgestellt. Damit sind die §§ 97a bis 97d IRG-E auch dann anwendbar, wenn ein Austausch von personenbezogenen Daten mit Schengen-assoziierten Staaten erfolgt. Insbesondere müssen die zuständigen deutschen Behörden das Zustimmungserfordernis nach § 97d Absatz 1 Nummer 3 IRG-E beachten, wenn personenbezogene Daten, die aus einem Schengen-assoziierten Staat stammen, an einen Drittstaat oder an eine zwischen- oder überstaatliche Einrichtung weitergeleitet werden sollen.

Die Gleichstellung der Schengen-assoziierten Staaten erfolgt mit Blick auf die Erwägungsgründe 45 bis 47 zum RbDatenschutz. Zudem entspricht es den Interessen der Rechtspraxis, dass für den praktisch bedeutsamen Rechtshilfeverkehr mit den Schengen-Staaten dieselben Datenschutzregeln gelten wie mit den Mitgliedstaaten der Europäischen Union.

Zu § 97b IRG-E – Verwendung von Daten

Zu Absatz 1

Absatz 1 sieht für personenbezogene Daten, die deutsche Behörden von anderen Mitgliedstaaten der Europäischen Union erhalten haben, Verwendungsbeschränkungen vor. Die Regelung setzt Artikel 11 Satz 1 RbDatenschutz bereichsspezifisch um. Zwar entspricht Artikel 11 Satz 1 RbDatenschutz weitgehend Artikel 23 Absatz 1 EU-RhÜbk, der keine ausdrückliche Umsetzung erfahren hat. Wegen der Bedeutung von Zweckbindungen für den Datenschutz und aufgrund des zunehmenden Datentransfers innerhalb der Europäischen Union soll nun aber eine gesetzliche Regelung im IRG erfolgen. Der Datenschutz im grenzüberschreitenden Datentransfer berührt ganz wesentlich die Frage, wann die Verwendung bereits erhobener personenbezogener Daten zu verfahrensübergreifenden Zwecken zulässig ist.

Daten, die deutsche Behörden von Institutionen der Europäischen Union erhalten, werden von der Regelung in Absatz 1 – mit Blick auf den klaren Wortlaut von Artikel 11 Satz 1 RbDatenschutz – nicht erfasst. Dadurch unterscheidet sich der Anwendungsbereich der Norm von den Absätzen 3 und 4.

Abweichend von dem Wortlaut des Artikels 11 RbDatenschutz soll es jedoch im nationalen Recht für den Schutz der personenbezogenen Daten nicht darauf ankommen, dass die übermittelten Daten von den „zuständigen Behörden“ eines anderen Mitgliedstaates übermittelt werden. Maßgeblich ist allein, dass die Daten „von einem anderen Mitglied-staat“ übermittelt oder bereitgestellt werden. Grund dafür ist, dass die Frage der Zuständigkeit von Behörden im europäischen Ausland von der empfangenden deutschen Stelle unter Umständen nicht zweifelsfrei beurteilt werden kann. Auch soll der Schutz der personenbezogenen Daten nicht geringer sein, wenn sie (sogar) von einer unzuständigen Behörde übermittelt wurden. Dies ist freilich auch nicht die Intention des RbDatenschutz, der den Begriff der „zuständigen Behörden“ vor allem in Abgrenzung zum privaten Bereich verwendet. Diese Abgrenzung ist auch bereits in der hier gewählten Formulierung enthalten, die erkennbar auf „staatliche“ Daten hindeutet.

Die Regelung in Absatz 1 versteht sich als eine reine Verwendungsregelung, also nicht als Befugnisnorm bzw. als Leistungsermächtigung. Die Befugnis zur Datenverwendung und auch die Reichweite der Befugnis muss sich aus den einschlägigen rechtshilferechtlichen Vorschriften ergeben, beispielsweise aus § 59 Absatz 1 und 3 IRG oder § 92c IRG. Die Formulierung „soweit dies gesetzlich vorgesehen ist“ stellt dies klar. Insoweit bedarf auch der allgemeine Zweckbindungsgrundsatz aus Artikel 3 RbDatenschutz – mit Ausnahme von dessen Absatz 2 Satz 2, siehe dazu die Anmerkungen zu dem nachfolgenden Absatz 2 – hier keiner ausdrücklichen Umsetzung. Insbesondere ist gewährleistet, dass eine Verwendung von personenbezogenen Daten nicht zu Zwecken erfolgen kann, die mit dem Zweck der Datenerhebung nicht in Einklang stehen, und dass keine neuen Befugnisse zur Datenverwendung geschaffen werden (vgl. Artikel 3 Absatz 2 Buchstabe a und b RbDatenschutz). In Übereinstimmung mit Artikel 11 RbDatenschutz wird die Verwendung (also die Verarbeitung und die Nutzung) empfangener Daten zu anderen Zwecken als denen, für die die Daten ursprünglich übermittelt oder bereitgestellt wurden, ausschließlich unter folgenden – alternativen – Voraussetzungen zugelassen:

Nach Nummer 1 ist die Verwendung von personenbezogenen Daten, die aus einem anderen Mitgliedstaat stammen, zulässig für die Verhütung und Verfolgung von Straftaten und von Ordnungswidrigkeiten, die der Datenübermittlung nicht zugrunde lagen. Die Ordnungswidrigkeiten werden hier ausdrücklich mit einbezogen, auch wenn Artikel 11 Satz 1 Buchstabe a RbDatenschutz lediglich von „Straftaten“ spricht und insoweit auch eine engere Auslegung denkbar erschiene. Das deutsche Rechtshilferecht bezieht über § 1 Absatz 2 IRG die Bußgeldverfahren in den Begriff der „strafrechtlichen Angelegenheit“ mit ein. Darüber hinaus gibt es im nationalen Recht mit Blick auf Datenverwendungsregelungen eine weitgehende Parallelität zwischen der Strafprozessordnung und dem Gesetz über Ordnungswidrigkeiten, die gewährleistet, dass der notwendige Übergang zwischen beiden Verfahrensarten nicht unnötig kompliziert zu handhaben ist. Auch im Rahmen der Verwendungsregelung in Nummer 1 können deshalb die Ordnungswidrigkeiten mit einbezogen werden.

Nummer 2 erlaubt die Verwendung von personenbezogenen Daten, die aus einem anderen Mitgliedstaat stammen, auch für die Vollstreckung und den Vollzug von strafrechtlichen Sanktionen, die der Datenübermittlung nicht zugrunde lagen. Der Strafvollzug wird hier in Anlehnung an existierende allgemeine datenschutzrechtliche Regelungen ausdrücklich erwähnt, auch wenn das IRG ansonsten lediglich von „Vollstreckung“ spricht.

Nach Nummer 3 können die Daten für justizielle und verwaltungsbehördliche Verfahren verwendet werden, die mit den in Nummer 1 oder 2 genannten Zwecken unmittelbar zusammenhängen. Bei der Beantwortung der Frage, ob ein unmittelbarer Zusammenhang im Sinne der Norm besteht, wird regelmäßig ein enger Maßstab anzulegen sein (vgl. Schomburg/Lagodny/Gleß/Hackner, Internationale Rechtshilfe in Strafsachen, 5. Auflage, § 59, Rn. 10). Verfahrensübergreifende Mitteilungen von Amts wegen gemäß den §§ 12 ff. EGGVG – auch in Verbindung mit der Anordnung über Mitteilungen in Strafsachen (MiStra) – sind auch bei Anlegung eines engen Maßstabs zulässig, denn hiervon erfasst werden im Wesentlichen Fälle, in denen sich gerade aus den in einem Strafverfahren gewonnenen Erkenntnissen ergibt, dass möglicherweise andere behördliche Maßnahmen erforderlich werden. Damit ist ein unmittelbarer Zusammenhang mit dem Strafverfahren gegeben. Zulässig sein dürfte außerdem auch die Übermittlung von Informationen zum Zwecke der Vorbereitung eines Schadensersatzprozesses, der mit dem Strafverfahren in Zusammenhang steht.

Nummer 4 lässt die Datenverwendung zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit zu. Artikel 11 Satz 1 Buchstabe c RbDatenschutz, der hiermit umgesetzt wird, spezifiziert nicht, ob es sich um eine innerstaatliche Gefahr handeln muss oder ob eine zweckändernde Datenverwendung auch in Betracht kommt, wenn in einem anderen Staat eine Gefahr besteht. Die offene Formulierung des Europarechts wird in das nationale Recht übernommen, so dass beide Situationen erfasst werden. Hierfür spricht unter anderem, dass die Möglichkeit für deutsche Behörden, bei Gefahrsituationen im Ausland unter den Voraussetzungen von § 92c IRG Spontanübermittlungen vorzunehmen, durch § 97b IRG-E nicht ausgeschlossen werden soll. Die Formulierung „gegenwärtig und erheblich“ lehnt sich an den im IRG eingeführten Sprachgebrauch an (vgl. § 92b IRG) und entspricht der in der deutschen Textfassung des RbDatenschutz verwendeten Formulierung „unmittelbar und ernsthaft“. Eine ausdrückliche Umsetzung der Voraussetzung einer „gegenwärtigen und erheblichen“ Gefahr ist erforderlich, weil das nationale Strafprozessrecht die Verwendung von personenbezogenen Daten aus Strafverfahren für polizeiliche Zwecke unter davon abweichenden, im Grundsatz weniger engen Voraussetzungen zulässt (vgl. § 481 Absatz 1 Satz 1, § 477 Absatz 2 Satz 3 StPO).

Nummer 5 erlaubt den deutschen Behörden eine Verwendung der erhaltenen Daten zu jedem anderen Zweck, wenn der Mitgliedstaat, von dem die Daten stammen, zuvor zugestimmt hat oder wenn die Zustimmung der Person, um deren Daten es geht, vorliegt. Den begrenzenden Rahmen für die Nutzung zu anderen Zwecken bildet freilich – auch bei Vorliegen einer Zustimmung durch den betroffenen Staat oder durch die betroffene Person – die Zuständigkeit der empfangenden Stelle; die Vorschrift will insoweit keine neuen Zuständigkeiten oder Befugnisse begründen, siehe oben. Artikel 11 Satz 1 Buchstabe d RbDatenschutz verwendet sowohl den Begriff der „vorherigen Zustimmung“ (in Bezug auf Staaten) als auch den Begriff der „Einwilligung“ (in Bezug auf Personen). Inhaltliche Unterschiede sind damit nicht verbunden. Im nationalen Recht soll – in Anlehnung an die beispielsweise bereits in § 92 Absatz 2 und § 92b Satz 3 IRG verwendete Terminologie – ausschließlich der Begriff der „(vorherigen) Zustimmung“ verwendet werden. Die Regelung erfasst beispielsweise den Fall, dass Daten, die im Wege der Rechtshilfe im Rahmen eines Steuerstrafverfahrens erlangt wurden, für das Besteuerungsverfahren verwendet werden sollen. Laut Erwägungsgrund 20 zum RbDatenschutz können die Mitgliedstaaten die Modalitäten für die Zustimmung selbst bestimmen und beispielsweise eine allgemeine Zustimmung für bestimmte Weiterverarbeitungskategorien vorsehen.

Die Vorgabe des RbDatenschutz, dass die Zustimmung durch den Mitgliedstaat oder durch die betroffene Person im Einklang mit der innerstaatlichen Rechtsordnung stehen muss, bedarf im nationalen Recht keiner Umsetzung. Zwar lässt der Wortlaut von Artikel 11 Satz 1 Buchstabe d RbDatenschutz offen, auf welches innerstaatliche Recht Bezug genommen wird. Bezüglich der Zustimmung für eine Datenverwendung durch einen anderen Mitgliedstaat können jedoch vergleichend Artikel 13 Absatz 1 Buchstabe c RbDatenschutz und Artikel 14 Absatz 1 Buchstabe a RbDatenschutz herangezogen werden, die ausdrücklich auf das innerstaatliche Recht des anderen Mitgliedstaates verweisen. Normadressat sind insoweit die ausländischen Stellen. Bezüglich der Zustimmung der Person, um deren Daten es geht, wird dagegen – gleich, ob sich die Person im Inland oder im Ausland befindet – auf das Recht des Staates abzustellen sein, der die Daten verwenden will. Wollen also deutsche Behörden auf der Grundlage von Nummer 5 vorgehen, müssen sie überprüfen, ob die betroffene Person auf der Grundlage der nationalen Rechtsordnung wirksam zugestimmt hat. Auch insoweit bedarf es aber keiner gesonderten Umsetzung, insbesondere mit Blick auf die allgemeine Rechtsbindung von Behörden. Es kann auf allgemeine Rechtsgrundsätze zurückgegriffen werden.

Die besondere Verwendungsregelung aus § 92b IRG bleibt unberührt, siehe die Anmerkungen zu § 97a Absatz 1 IRG-E.

Bezüglich des Verhältnisses der Verwendungsregelungen von § 97b IRG-E zu den daten-schützenden Vorschriften insbesondere der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten wird auf die Anmerkungen im Allgemeinen Teil der Begründung verwiesen.

Zu Absatz 2

Die Vorschrift regelt in Umsetzung von Artikel 14 RbDatenschutz, unter welchen Voraus-setzungen Daten, die deutsche Behörden von einem anderen Mitgliedstaat erhalten haben, an nicht-öffentliche Stellen weitergeleitet werden dürfen. Erwägungsgrund 17 zum RbDatenschutz erläutert, welche Fallgestaltungen der europäische Gesetzgeber dabei vor Augen hatte, nämlich beispielsweise Warnmeldungen zu gefälschten Wertpapieren an Kreditinstitute oder Mitteilungen an Versicherungsunternehmen, um im Bereich von Kfz-Kriminalität einen Handel mit gestohlenen Kraftfahrzeugen zu verhindern.

Auch Absatz 2 enthält – wie Absatz 1 – eine reine Verwendungsregelung und setzt voraus, dass eine Befugnis zur Datenweiterleitung besteht. Die sowohl in Satz 1 als auch Satz 2 verwendete Formulierung „soweit dies gesetzlich vorgesehen ist“ stellt dies klar, siehe die Anmerkungen zu Absatz 1.

Der in Absatz 2 verwendete Begriff der „nicht-öffentlichen Stellen“ lehnt sich an § 2 Ab-satz 4 BDSG an und bedarf als eingeführter Rechtsbegriff keiner bereichsspezifischen Definition. Erfasst werden natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie keine hoheitlichen Aufgaben wahrnehmen. Der Begriff „Weiterleiten“ wird in Übereinstimmung mit dem Sprachgebrauch des RbDatenschutz und in dem Verständnis verwendet, dass hiervon sowohl eine Datenübermittlung als auch eine Bereitstellung von Daten erfasst ist (siehe zu diesen Begriffen die Anmerkungen zu § 97a Absatz 1 Nummer 2 IRG-E).

Satz 1 stellt zunächst in Übereinstimmung mit Erwägungsgrund 18 zum RbDatenschutz klar, dass eine Datenweiterleitung im Zusammenhang mit Straf- und Bußgeldverfahren möglich ist. Die Verwendungsregelungen nach Artikel 14 RbDatenschutz bzw. nach Satz 2, mit dem Artikel 14 umgesetzt wird, finden hier keine Anwendung. Damit unterfallen insbesondere strafprozessuale Befugnisse zur Erteilung von Auskünften an Privatpersonen und andere nicht-öffentliche Stellen sowie zur Gewährung von Akteneinsicht nicht den Verwendungsbeschränkungen aus Satz 2. Neben den Strafverfahren werden – über den Wortlaut des Erwägungsgrundes 18 zum RbDatenschutz hinaus, der lediglich von „Strafverfahren“ spricht – auch die Bußgeldverfahren ausdrücklich erwähnt, siehe die Anmerkung zu Absatz 1 Nummer 1.

Satz 2 erfasst Fälle von Datenweiterleitungen außerhalb von Straf- und Bußgeldverfahren. Die Regelung begrenzt die Möglichkeiten zur Weiterleitung personenbezogener Daten an nicht-öffentliche Stellen in Übereinstimmung mit den europarechtlichen Vorgaben. Die Norm zählt abschließend die kumulativen Voraussetzungen auf, unter denen eine Datenweiterleitung möglich ist:

Nach Nummer 1 muss die Zustimmung der zuständigen Behörde des Mitgliedstaates vor-liegen, aus dem die Daten stammen. Die Vorgabe von Artikel 14 Absatz 1 Buchstabe a RbDatenschutz, dass die Zustimmung der ausländischen Behörde „unter Beachtung ihres innerstaatlichen Rechts“ erfolgen muss, bedarf im nationalen Recht keiner Umsetzung. Normadressat ist hier die ausländische Behörde.

Nach Nummer 2 dürfen außerdem keine überwiegenden schutzwürdigen Belange der Person, um deren Daten es geht, entgegenstehen.

Nach Nummer 3 schließlich muss die Datenweiterleitung für die Behörde, die die Daten weiterleitet, unerlässlich sein. Dies kann in fünf – alternativen – Fällen angenommen werden:

Nach Buchstabe a kommt eine Datenweiterleitung in Betracht, wenn dies in Erfüllung einer Aufgabe erfolgt, die der weiterleitenden Stelle zugewiesen wurde. Die in Artikel 14 Absatz 1 Buchstabe c Ziffer i RbDatenschutz verwendete Formulierung „rechtmäßig zugewiesene Aufgabe“ muss nicht ausdrücklich in das nationale Recht übernommen werden. Insoweit gelten die allgemeinen Regelungen, insbesondere der Rechtsbindungsgrundsatz der Verwaltung.

Buchstabe b lässt die Datenweiterleitung zum Zwecke der Verhütung oder der Verfolgung von anderen Straftaten oder anderen Ordnungswidrigkeiten als denen zu, für die die Daten übermittelt oder bereitgestellt wurden. Hinsichtlich der Einbeziehung von Ordnungs-widrigkeiten in diese Fallgruppe, die in Artikel 14 Absatz 1 Buchstabe c Ziffer ii RbDatenschutz nicht ausdrücklich vorgesehen ist, wird auf die Anmerkungen zu Absatz 1 Nummer 1 verwiesen.

Nach Buchstabe c ist die Datenweiterleitung zulässig, wenn es um die Vollstreckung und den Vollzug von anderen strafrechtlichen Sanktionen als denen geht, für die die Daten übermittelt oder bereitgestellt wurden.

Buchstabe d regelt den Fall der Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit. Bezüglich der Formulierung „gegenwärtige und erhebliche Gefahr“, die von dem Sprachgebrauch in Artikel 14 RbDatenschutz („unmittelbare und ernsthafte Gefahr“) leicht abweicht, wird auf die Anmerkungen zu Absatz 1 Nummer 4 verwiesen.

Buchstabe e schließlich nennt den Fall der Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner.

Mit Satz 3 wird Artikel 14 Absatz 2 RbDatenschutz umgesetzt. Die Behörde, die personenbezogene Daten an eine nicht-öffentliche Stelle weiterleitet, weist die empfangende Stelle darauf hin, zu welchen Zwecken die Daten ausschließlich verwendet werden dürfen.

Zu Absatz 3

Satz 1 setzt Artikel 3 Absatz 2 Satz 2 und Artikel 11 Satz 2 RbDatenschutz um und enthält eine weitere Verwendungsregelung. In Umsetzung von Artikel 3 Absatz 2 Satz 2 RbDatenschutz, dessen Anwendungsbereich sich im Gegensatz zu Artikel 11 Satz 2 RbDatenschutz nicht auf personenbezogene Daten beschränkt, die aus anderen Mitgliedstaaten stammen, sind von der Regelung auch Daten erfasst, die deutsche Behörden von Institutionen der Europäischen Union erhalten.

Über den Wortlaut von Artikel 11 Satz 2 RbDatenschutz hinaus, der lediglich „übermittelte“ Daten zu erfassen scheint, soll die Vorschrift auch dann gelten, wenn es sich um Daten handelt, die aus dem Ausland bereitgestellt wurden (zur Unterscheidung zwischen den Begriffen „übermitteln“ und „bereitstellen“ wird auf die Begründung zu § 97a Absatz 1 Nummer 2 IRG-E verwiesen). Da die Überschrift zu Artikel 11 RbDatenschutz sowohl die Datenübermittlung als auch das Bereitstellen von Daten erfasst, beruht die engere Formulierung in Artikel 11 Satz 2 RbDatenschutz offenbar auf einem bloßen redaktionellen Versehen.

Nach den Vorgaben der Artikel 3 und 11 RbDatenschutz ist eine Verwendung von personenbezogenen Daten für historische, statistische oder wissenschaftliche Zwecke zulässig, wenn geeignete Schutzmaßnahmen vorgesehen werden, zum Beispiel eine Anonymisierung der Daten. Der Begriff „historische Zwecke“ wird im RbDatenschutz nicht näher definiert. Das nationale Recht übernimmt die Formulierung in dem Verständnis, dass vor allem „geschichtswissenschaftliche Zwecke“ gemeint sein dürften. Bezüglich der einzuhaltenden Schutzmaßnahmen verweist die Vorschrift auf die geltenden innerstaatlichen Vorschriften. Für die Verwendung von Akteninhalten und gespeicherten Daten aus Strafakten zu wissenschaftlichen Zwecken wird damit auf § 476 StPO Bezug genommen. Bei einer Verwendung zu historischen und statistischen Zwecken sind die einschlägigen Archiv- und Statistikgesetze zu beachten.

Die Regelung beruht auf allgemeinen Verhältnismäßigkeitserwägungen und hat insoweit vor allem eine klarstellende Funktion. Ihr kann eine praktische Bedeutung insbesondere in den Fällen zukommen, in denen die Bewilligungsbehörde und die sachleitende Strafverfolgungsbehörde auseinanderfallen.

Zu Absatz 4

Die Regelung setzt Artikel 8 Absatz 1 Satz 4 RbDatenschutz um und betrifft die sogenannten Spontanübermittlungen. Die Norm greift – wie Absatz 3 – für personenbezogene Daten ein, die deutschen Behörden von anderen Mitgliedstaaten oder von Institutionen der Europäischen Union übermittelt werden. Daten, die lediglich bereitgestellt werden, sind nach dem Sinn und Zweck von Artikel 8 Absatz 1 Satz 4 RbDatenschutz, der allein die gezielte Datenübermittlung ohne Ersuchen aus dem europäischen Rechtsraum regelt, nicht erfasst. Die Vorschrift dient vor allem der Klarstellung. Schon bisher folgte aus dem allgemeinen Rechtsbindungsgrundsatz für deutsche Behörden, dass sie Daten, die im Wege von Spontanübermittlungen aus dem Ausland übermittelt werden, daraufhin überprüfen müssen, ob sie verwendet werden dürfen. Das IRG sieht hierzu allerdings bisher keine allgemeine bereichsspezifische Regelung vor; diese soll nunmehr wegen der zunehmenden Bedeutung des grenzüberschreitenden Datenaustauschs innerhalb der Europäischen Union aufgenommen und im Elften Teil verortet werden. Von einer Verortung der Norm in § 92c IRG wird Abstand genommen, weil dort bisher nur ausgehende Spontanübermittlungen erfasst sind.

Vorgaben dazu, wie mit solchen personenbezogenen Daten umzugehen ist, die im Wege der Spontanübermittlung übermittelt wurden und nicht benötigt werden, macht der RbDatenschutz nicht. Insbesondere beziehen sich die Mitteilungs- und Korrekturpflichten aus Artikel 8 Absatz 2 in Verbindung mit Artikel 4 RbDatenschutz nicht auf diesen Fall, sondern lediglich auf unrichtige oder unrechtmäßige Datenübermittlungen. Die Behandlung dieser Daten richtet sich damit nach dem nationalen Recht. In der Praxis bedeutet dies, dass Spontanübermittlungen von anderen Mitgliedstaaten oder von Institutionen der Europäischen Union, die personenbezogene Daten enthalten,

wie vergleichbare Mitteilungen, Schreiben oder Strafanzeigen, die Strafverfolgungsbehörden zum Beispiel von Privatpersonen erhalten, mit Blick auf die Gesetzmäßigkeit der Verwaltung und die Grund-sätze der Aktenwahrheit und Aktenklarheit regelmäßig veraktet werden, um sodann den Sachverhalt zu prüfen. Eine Speicherung der personenbezogenen Daten in Dateien setzt gemäß den §§ 483 bis 485 StPO voraus, dass sie für Zwecke des Strafverfahrens, für Zwecke künftiger Strafverfahren oder für Zwecke der Vorgangsverwaltung erforderlich sind. Stellt sich heraus, dass die übermittelten Daten nicht benötigt werden, weil der übermittelte Sachverhalt zum Beispiel keine Anhaltspunkte für das Vorliegen einer Straftat oder Ordnungswidrigkeit bietet, wird der Vorgang abgeschlossen. Die Aufbewahrungsdauer der Akte und die Speicherdauer der personenbezogenen Daten, die hierzu in der Vorgangsverwaltung erfasst werden, richten sich nach den einschlägigen innerstaatlichen Vorschriften.

Zu § 97c IRG-E – Übermittlung oder Bereitstellung von Daten

Zu Absatz 1

Die Regelung greift den Verantwortungsgedanken aus Artikel 8 RbDatenschutz auf und sieht – angesichts des ansteigenden Datenaustauschs innerhalb der Europäischen Union – nach dem Vorbild von § 4b Absatz 5 BDSG für den Rechtshilfeverkehr eine bereichs-spezifische Verantwortlichkeitsregelung vor. Zum Begriff „Rechtshilfeverkehr“ wird auf die Anmerkungen zur Überschrift verwiesen.

Für die Prüfung der Zulässigkeit einer grenzüberschreitenden Übermittlung oder Bereit-stellung von personenbezogenen Daten ist die Stelle verantwortlich, die die Daten an andere Mitgliedstaaten oder an eine europäische Einrichtung übermittelt oder diesen bereitstellt. Von der Vorschrift unberührt bleibt die Verantwortung der nationalen datenführenden Stelle für die Frage, ob die Daten innerstaatlich der übermittelnden Stelle zur Verfügung gestellt werden durften. Ebenfalls unberührt bleibt – selbstverständlich –, dass diejenige Stelle, die bereitgestellte Daten einsieht oder abruft, die Verantwortung für die Zulässigkeit dieses Vorgangs trägt.

Die übermittelnde Stelle soll – abweichend beispielsweise von dem Regelungsansatz, der § 477 Absatz 4 Satz 1 und § 487 Absatz 3 Satz 2 StPO für Datenübermittlungen zu verfahrensübergreifenden Zwecken zugrunde liegt – auch dann für die Prüfung der Zulässigkeit der Datenübermittlung verantwortlich sein, wenn die Übermittlung auf Ersuchen des Empfängers erfolgt. Dies erscheint für den grenzüberschreitenden Datenaustausch sachgerecht, weil die empfangende Stelle im Ausland letztlich nicht überprüfen kann, ob die Datenübermittlung nach den Vorgaben des deutschen Rechts zulässig ist.

Die Vorschrift dient primär Klarstellungs- bzw. Transparenzzwecken, insbesondere für den Fall, dass die datenführende und die datenübermittelnde Stelle auseinanderfallen. Dies ist immer dann gegeben, wenn nicht der unmittelbare Geschäftsweg gilt. Die Frage der Zulässigkeit der Datenübermittlung ist dann durch die datenübermittelnde Stelle zu prüfen. Kann die datenübermittelnde Stelle aus eigener Anschauung nicht oder jedenfalls nicht vollständig beurteilen, ob die Datenübermittlung zulässig ist, muss sie – sofern sich für sie konkrete Anhaltspunkte bieten – ihrer Prüfpflicht nachkommen, indem sie sich gegebenenfalls an die datenführende Stelle wendet und dort Informationen einholt.

Die Regelung schafft nicht nur für die nationalen Behörden Transparenz. Die klare Verantwortlichkeitsregelung erleichtert es auch den Personen, deren Daten betroffen sind, Rechtsschutz zu suchen.

Zu Absatz 2

Die Regelung enthält für die nationalen Behörden, die personenbezogene Daten grenz-überschreitend übermitteln oder bereitstellen, konkrete Vorgaben, die in Übereinstimmung mit den umzusetzenden Vorgaben des RbDatenschutz zum Teil verbindlich und zum Teil als Soll- oder Kann-Vorschrift ausgestaltet sind. Zudem wird – wie im Rahmenbeschluss – zwischen solchen Pflichten differenziert, die sowohl für die grenzüberschreitende Übermittlung als auch für die Bereitstellung von personenbezogenen Daten anfallen, und solchen, die ausschließlich für die Übermittlung solcher Daten gelten. Zu den Begriffen „übermitteln“ und „bereitstellen“ wird auf die Anmerkungen zu § 97a Absatz 1 Nummer 2 IRG-E verwiesen.

Nach Nummer 1 soll die übermittelnde Stelle vor der grenzüberschreitenden Übermittlung oder Bereitstellung von personenbezogenen Daten deren Qualität überprüfen. Artikel 8 Absatz 1 Satz 1 RbDatenschutz nennt als Qualitätskriterien die Richtigkeit, Vollständigkeit und Aktualität der Daten. Das nationale Recht übernimmt diese Kriterien. Nach dem RbDatenschutz besteht eine Verpflichtung zur Überprüfung nur, soweit dies der übermittelnden Stelle „praktisch möglich“ ist (vgl. auch die englische Textfassung: „as far as practicable“). Nummer 1 ist insoweit als Soll-Vorschrift ausgestaltet. Angaben dazu, unter welchen Voraussetzungen eine Überprüfung möglich ist, enthält der RbDatenschutz nicht; sie sind auch im nationalen Recht nicht erforderlich. Das nationale

Verfahrensrecht ist geprägt von dem Grundsatz der Aktenklarheit und der Aktenwahrheit, der die zuständigen Behörden verpflichtet, Akteninhalte jederzeit auf ihre Richtigkeit und Aktualität zu prüfen. Im Hinblick darauf dürfte es in der Regel genügen, die Daten auf ihre Schlüssigkeit hin zu überprüfen und eine vertiefte Prüfung lediglich anlassbezogen vorzunehmen. Bei der Auslegung der Norm wird die Rechtspraxis den Grundrechtsschutz betroffener Personen ebenso berücksichtigen wie die Belange einer effektiven grenzüberschreitenden Strafverfolgung.

Nummer 2 setzt Artikel 8 Absatz 1 Satz 3 RbDatenschutz um und gilt ausschließlich für den Fall der grenzüberschreitenden Übermittlung von personenbezogenen Daten, also nicht bei einer Bereitstellung solcher Daten. Die übermittelnde Stelle ist bei der Übermittlung der Daten gehalten, Informationen beizufügen, die es der empfangenden Stelle erlauben, die Qualität der Daten zu prüfen. Gegenüber der Vorschrift aus Nummer 1 enthält Nummer 2 ein weiteres Qualitätskriterium: Neben der Richtigkeit, Vollständigkeit und Aktualität wird hier auch die Zuverlässigkeit der Daten genannt. Diese Differenzierung entspricht den Vorgaben von Artikel 8 Absatz 1 Satz 1 bis 3 RbDatenschutz. Die Zuverlässigkeit von Daten im Sinne einer Vertrauenswürdigkeit oder Belastbarkeit (englischer Text: „reliability“) ist vor allem im Rahmen des Ermittlungs- oder Strafverfahrens von Belang. Deshalb ist es vorrangig die Aufgabe der empfangenden Stelle, die Zuverlässigkeit der Daten zu überprüfen. Die übermittelnde Stelle soll aber möglichst durch Beifügung von entsprechenden Informationen dazu beitragen, dass die empfangende Stelle diese Aufgabe wahrnehmen kann.

Die Verpflichtung aus Nummer 2 besteht nicht uneingeschränkt, sondern nur „nach Möglichkeit“. Diese Formulierung aus dem RbDatenschutz wird in dem Bestreben in das nationale Recht übernommen, einerseits die europarechtlichen Vorgaben eng umzusetzen, ohne andererseits die Rechtspraxis zu stark zu belasten. Entsprechend wurde beispielsweise bei § 14 Absatz 10 Satz 3 BKAG-E verfahren. Von einer Ausgestaltung der Norm als Soll-Vorschrift nach dem Vorbild von Nummer 1 wird abgesehen, weil bereits dies zu einem übermäßigen Mehraufwand für die Praxis führen würde; ein Verzicht auf die Übermittlung von Informationen zur Datenqualität wäre dann nur ausnahmsweise zulässig. Mit Blick auf den Grundsatz der Aktenklarheit und der Aktenwahrheit wird es regelmäßig ausreichend sein, dass die übermittelnde deutsche Stelle der empfangenden Stelle mitteilt, woher die Daten stammen und gegebenenfalls, auf welchem Wege die Daten erlangt wurden. Liegen der übermittelnden Stelle entsprechende Informationen jedoch selbst nicht vor, müssen diese in der Regel auch nicht eigens beschafft werden. Anderes gilt aber mit Blick auf den Grundrechtsschutz der Personen, deren Daten übermittelt werden, wenn bereits Zweifel an der Qualität der zu übermittelnden Daten bestehen, vgl. die Anmerkungen zu Nummer 1.

Nummer 3 enthält eine verbindliche Regelung und setzt den – ebenfalls verbindlichen – Artikel 12 Absatz 1 Satz 1 RbDatenschutz um. Gelten nach dem deutschen Recht besondere Verwendungsbeschränkungen für den Austausch der Daten, die die deutschen Behörden an Mitgliedstaaten oder an Institutionen der Europäischen Union übermitteln oder dafür bereitstellen wollen, muss die übermittelnde deutsche Behörde die empfangende Stelle darauf hinweisen. Dies entspricht dem Ansatz der Strafprozessordnung, für die vor allem Verwendungsbeschränkungen von Relevanz sind (siehe z. B. § 477 Absatz 2 StPO), während Löschungsfristen oder sogenannte Löschungsprüffristen bislang nur im Bereich von elektronische Dateien und von verdeckten Ermittlungsmaßnahmen eine besondere Bedeutung zukommt. Die empfangende Stelle ist nach Artikel 12 Absatz 1 Satz 2 RbDatenschutz verpflichtet sicherzustellen, dass die Verwendungsbeschränkungen eingehalten werden. Zur Beachtung von Verwendungsbeschränkungen, die den deutschen Behörden im Zuge einer Datenübermittlung bei eingehenden oder ausgehenden Ersuchen von anderen Mitgliedstaaten oder EU-Behörden auferlegt werden, bedarf es keiner gesonderten gesetzlichen Umsetzung. Es entspricht den Grundsätzen der Rechtshilfe, dass auf verfahrensrechtliche Erfordernisse oder sonstige Anliegen ersuchender oder ersuchter Staaten Rücksicht zu nehmen ist, vgl. § 72 IRG und Nummer 22 Absatz 1 Satz 2 der Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVASt).

Nach Nummer 4 kann die nationale Behörde, die personenbezogene Daten grenzüber-schreitend übermittelt oder bereitstellt, dabei im Einklang mit dem innerstaatlichen Recht eine Frist für die Aufbewahrung der Daten setzen. Es handelt sich um eine Form der Bedingung. Unter die Formulierung „Fristen für die Aufbewahrung“ fallen sowohl Löschungsfristen als auch Löschungsprüffristen.

Wie der umzusetzende Artikel 9 Absatz 1 Satz 1 RbDatenschutz sieht auch das nationale Recht eine lediglich fakultative Regelung vor. Die Strafprozessordnung kennt im Grundsatz keine festen Löschungsfristen. Daten dürfen grundsätzlich nur solange gespeichert werden, wie dies zur Erfüllung bestimmter, gesetzlich festgelegter Zwecke erforderlich ist. Einzelne Regelungen schreiben allerdings unter bestimmten Voraussetzungen eine „unverzügliche“ Löschung vor (siehe etwa § 100a Absatz 4 Satz 3, § 101 Absatz 8 Satz 1 StPO). Darüber hinaus enthält

das nationale Recht Fristen zur Überprüfung, ob ein gespeichertes Datum zu löschen ist, vgl. § 489 Absatz 4 StPO für Daten, die in einer Datei gespeichert sind. Eine obligatorische Mitteilung von Löschungsfristen oder Löschungsprüffristen bei der Datenübermittlung an das europäische Ausland wäre angesichts dessen nicht sachgerecht. Dagegen verschafft eine fakultative Regelung der Rechtspraxis einen angemessenen Handlungsspielraum, im Einzelfall der empfangenden Stelle Fristen mitzuteilen. Dieser Fall kann nicht nur aufgrund der Vorgaben der eigenen Rechtsordnung praktische Relevanz erlangen. Denkbar ist auch, dass deutsche Behörden Daten übermitteln, die sie ihrerseits von einem anderen Mitgliedstaat der Europäischen Union oder einem Drittstaat unter der Bedingung erhalten haben, bestimmte Löschungsfristen einzuhalten. Diese Bedingung wäre dann bei einer etwaigen Weitergabe der Daten an einen anderen Mitgliedstaat dadurch einzuhalten, dass der empfangenden Stelle die entsprechenden Löschungsfristen mitgeteilt werden.

Die Vorschrift hat vor allem klarstellende Funktion. Es entspricht den Grundsätzen der Rechtshilfe, dass die Leistung von Rechtshilfe von Bedingungen wie etwa der Einhaltung bestimmter Löschungsfristen abhängig gemacht werden kann. Der RbDatenschutz, der gemäß seinem Artikel 1 Absatz 5 lediglich ein datenschutzrechtliches Mindestniveau festschreibt und also weiterreichende datenschützende Maßnahmen erlaubt, ändert daran nichts. Die justizielle Zusammenarbeit in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union wird allerdings inzwischen wesentlich geprägt von europäischen Rechtsinstrumenten, die auf dem Grundsatz der gegenseitigen Anerkennung beruhen. Insoweit kann sich die Frage stellen, ob Bedingungen, die in den Rechtsinstrumenten der gegenseitigen Anerkennung nicht ausdrücklich vorgesehen sind, europarechtlich überhaupt zulässig sind, siehe die Anmerkungen im Allgemeinen Teil der Begründung. Die Regelung in Nummer 4 stellt deshalb in Übereinstimmung mit dem RbDatenschutz ausdrücklich fest, dass die deutschen Behörden die empfangenden Stellen im europäischen Ausland verpflichten können, bestimmte Löschungs- oder Löschungsprüffristen zu beachten. Andere Bedingungen als solche, die Löschungs- oder Löschungsprüffristen betreffen, werden dadurch nicht ausgeschlossen.

Nach Ablauf der mitgeteilten Aufbewahrungsfrist ist die empfangende ausländische Stelle verpflichtet, die Daten zu löschen, zu sperren oder zu prüfen, ob die Daten noch benötigt werden. Dies gilt nach Artikel 9 Absatz 1 Satz 2 RbDatenschutz nur dann nicht, wenn die Daten zum Zeitpunkt des Fristablaufs noch für eine laufende Strafverfolgung oder Strafvollstreckung benötigt werden. Sind die personenbezogenen Daten in einer justiziellen Entscheidung (siehe die englische Textfassung „judicial decision“, die in der deutschen Textfassung zu eng mit „Gerichtsbeschluss“ übersetzt wurde) oder einer Akte enthalten, die mit einer justiziellen Entscheidung verknüpft ist, erfolgt die Berichtigung, Löschung oder Sperrung zudem nur im Einklang mit der nationalen Prozessordnung, siehe Artikel 4 Absatz 4 RbDatenschutz.

Zur Beachtung von Löschungs- oder Löschungsprüffristen, die den deutschen Behörden im Zuge einer Datenübermittlung bei eingehenden oder ausgehenden Ersuchen von anderen Mitgliedstaaten oder EU-Behörden auferlegt werden, bedarf es keiner gesonderten gesetzlichen Umsetzung. Es entspricht den Grundsätzen der Rechtshilfe, dass auf verfahrensrechtliche Erfordernisse oder sonstige Anliegen ersuchender oder ersuchter Staaten Rücksicht zu nehmen ist, siehe bereits die Anmerkung zu Nummer 3. Insoweit bedarf auch die Ausnahmevorschrift aus Artikel 9 Absatz 1 Satz 2 RbDatenschutz keiner Umsetzung im IRG; sie würde insbesondere hinter § 72 IRG und damit hinter das existierende Datenschutzniveau im Rechtshilferecht zurückfallen. Eine europarechtliche Pflicht zur Umsetzung der Ausnahmeregelung besteht nicht, da Artikel 1 Absatz 5 RbDatenschutz ein strengeres Datenschutzniveau als das des RbDatenschutz ausdrücklich zulässt. Praktische Erwägungen zwingen ebenfalls nicht zu einer Umsetzung der Ausnahmevorschrift aus Artikel 9 Absatz 1 Satz 2 RbDatenschutz. In Bezug auf Löschungsprüffristen gilt bereits, dass die bloße Überprüfung von Daten daraufhin, ob sie für die Strafverfolgung oder Strafvollstreckung noch benötigt werden, etwaig noch laufende Verfahren nicht beeinträchtigen wird. In Bezug auf die im nationalen Recht seltener vorkommenden Löschungsfristen kann auf eingeübte Rechtshilfepraktiken zurückgegriffen werden: Die zuständigen Behörden achten darauf, dass die Leistung von Rechtshilfe nur mit solchen Bedingungen verknüpft werden, die nach ihrem eigenen, innerstaatlichen Recht beachtet werden können und nicht zu einer Sinnlosigkeit der Rechtshilfeleistung führen (Schomburg/Lagodny/Gleß/Hackner, IRG, 5. Auflage, § 72, Rn. 5). Rechtshilferechtliche Probleme sind hierzu bisher nicht bekannt geworden.

Mit Nummer 5 wird die die Mitteilungspflicht aus Artikel 8 Absatz 2 Satz 1 RbDatenschutz umgesetzt, die (nur dann) eingreift, wenn unrichtige personenbezogene Daten oder personenbezogene Daten unrichtig übermittelt wurden. Auch diese Vorschrift gilt nur für die grenzüberschreitende Übermittlung von personenbezogenen Daten, nicht für die Bereitstellung, da nur im ersten Fall die empfangende Stelle konkret bekannt ist. Die Regelung erfolgt vor allem aus Klarstellungsgründen. Eine Pflicht, der empfangenden Stelle mitzuteilen, dass Daten unrichtig oder unrechtmäßig übermittelt wurden, ergibt sich für die übermittelnde deutsche Behörde im Grundsatz bereits aus

der allgemeinen Rechtsbindung der Verwaltung. Eine bereichsspezifische Regelung im Elften Teil des IRG erscheint wegen der datenschützenden Bedeutung aber sachgerecht, da der grenzüberschreitende Datentransfer innerhalb der Europäischen Union insgesamt ansteigt. Zudem enthält das IRG – beschränkt auf Fälle der Spontanauskünfte – bereits eine vergleichbare Vorschrift, § 92 Absatz 2 in Verbindung mit § 61a Absatz 4 IRG. Der Wortlaut der Norm lehnt sich an § 61a Absatz 4 IRG an. Die empfangende Stelle, die eine entsprechende Mitteilung der deutschen übermittelnden Stelle erhält, ist nach Artikel 8 Absatz 2 Satz 2 in Verbindung mit Artikel 4 RbDatenschutz zur Berichtigung, Löschung oder Sperrung der betroffenen personenbezogenen Daten verpflichtet. Das von deutschen Behörden zu stellende Ersuchen knüpft an diese Regelung an.

Zu § 97d IRG-E – Weiterleitung von Daten an Drittstaaten sowie an zwischen- oder überstaatliche Einrichtungen

Zu Absatz 1

Die Regelung dient der Umsetzung von Artikel 13 Absatz 1 RbDatenschutz und gibt vor, unter welchen Voraussetzungen die deutschen Behörden personenbezogene Daten, die sie von einem anderen Mitgliedstaat erhalten haben, an Drittstaaten oder internationale Einrichtungen weiterleiten dürfen.

Die Vorschrift versteht sich als Verwendungsregelung, nicht als Befugnisnorm. Die Befugnis zur Datenverwendung und auch die Reichweite der Befugnis muss sich aus den einschlägigen rechtshilferechtlichen Vorschriften ergeben, beispielsweise aus § 59 Absatz 1 und 3 IRG oder § 92c IRG. Die Formulierung „soweit dies gesetzlich vorgesehen ist“ stellt dies klar. Unberührt bleiben insoweit allgemeine Voraussetzungen für die Verwendung von personenbezogenen Daten. Insbesondere muss der Zweck der Datenweiterleitung so gewichtig sein, dass er eine Erhebung der Daten nach innerstaatlichem Recht gerechtfertigt hätte.

Statt der im RbDatenschutz verwendeten Formulierung „internationale Einrichtungen“ wird hier eine Formulierung gewählt, die sich an die bereits in § 67a IRG eingeführte Wendung „zwischen- und überstaatliche Einrichtungen“ anlehnt. Die internationalen Strafgerichtshöfe sind hiervon mit umfasst. Der Begriff „Weiterleiten“ wird in Übereinstimmung mit dem Sprachgebrauch des RbDatenschutz und in dem Verständnis verwendet, dass hiervon sowohl eine Datenübermittlung als auch eine Bereitstellung von Daten erfasst ist (siehe zu diesen Begriffen die Anmerkungen zu § 97a Absatz 1 Nummer 2 IRG-E).

Als Drittstaaten im Sinne der Norm sind nicht die Schengen-assoziierten Staaten anzusehen; diese sind den Mitgliedstaaten der Europäischen Union gleichgestellt (§ 97a Absatz 2 IRG-E). Ebenso wenig zählen die europäischen Behörden und Informationssysteme gemäß § 97a Absatz 1 IRG-E zu den zwischen- oder überstaatlichen Einrichtungen im Sinne der Norm. Dies ergibt sich aus dem Sinn und Zweck von Artikel 13 RbDatenschutz, der erhöhte Anforderungen an eine Datenweiterleitung nur in dem Falle stellt, in dem die Daten Einrichtungen übermittelt werden, die nicht dem europäischen Datenschutzstandard verpflichtet sind.

Folgende – kumulative – Voraussetzungen müssen für eine Datenweiterleitung erfüllt sein:

– Nach Nummer 1 muss die Weiterleitung für Zwecke der Verhütung oder Verfolgung von Straftaten oder von Ordnungswidrigkeiten, zur Strafvollstreckung oder für Zwecke des Strafvollzugs erforderlich sein. Die Ordnungswidrigkeiten werden hier ausdrücklich mit einbezogen, auch wenn Artikel 13 Absatz 1 Buchstabe a RbDatenschutz lediglich von „Straftaten“ spricht. Auf die Anmerkungen zu § 97b Absatz 1 Nummer 1 IRG-E wird verwiesen.

– Nach Nummer 2 muss die empfangende Stelle für die in Nummer 1 genannten Auf-gaben jeweils zuständig sein. Die Vorschrift will Datenstreuungen vermeiden. Die deutschen Behörden müssen also die Zuständigkeit der empfangenden Stelle über-prüfen, bevor sie personenbezogene Daten an das außereuropäische Ausland oder an internationale Einrichtungen (z. B.: Europarat, Vereinte Nationen) weiterleiten. Dies wird mit Blick auf die internationalen Einrichtungen von praktischer Bedeutung sein, wenn diese nicht über eigene Strafverfolgungsbefugnisse verfügen.

– Nach Nummer 3 muss der Mitgliedstaat, von dem die deutschen Behörden die personenbezogenen Daten erhalten haben, der Weiterleitung vorher zustimmen, es sei denn, es greift die Ausnahmeregelung aus Absatz 2 ein. Ein solches Zustimmungserfordernis ist bislang im IRG nicht ausdrücklich geregelt, wird aber in der Praxis regel-mäßig bereits entsprechend gehandhabt. Um den Organisationsaufwand bei den nationalen Behörden gering zu halten, steht es den Mitgliedstaaten frei, Modalitäten für die Zustimmungserteilung fest-

zulegen, die den Erfordernissen der Rechtspraxis Rechnung tragen. Laut Erwägungsgrund 24 zum RbDatenschutz können die Mitgliedstaaten beispielsweise eine allgemeine Zustimmung für bestimmte Kategorien von Informationen oder für bestimmte Drittstaaten erteilen.

– Nummer 4 schreibt vor, dass der Drittstaat bzw. die zwischen- oder überstaatliche Einrichtung ein angemessenes Schutzniveau für die beabsichtigte Datenverarbeitung gewährleisten müssen. Vorgaben dazu, wie die Angemessenheit des Schutzniveaus festzustellen ist, enthält Artikel 13 Absatz 4 RbDatenschutz. Eine Umsetzung dieser Vorgaben im IRG ist nicht erforderlich. Der Begriff "angemessenes Datenschutzniveau" ist ein eingeführter Rechtsbegriff, der bereits im IRG (§ 61a Absatz 3) und in anderen Gesetzen, etwa § 4b Absatz 3 BDSG verwendet wird. § 4b Absatz 3 BDSG nennt als allgemeine datenschützende Norm ausdrücklich diejenigen Kriterien, die bei der Ermittlung der Angemessenheit vorrangig zu berücksichtigen sind. Hierauf kann zurückgegriffen werden; einer wiederholenden bereichsspezifischen Regelung bedarf es nicht.

Zu Absatz 2

Die Vorschrift setzt Artikel 13 Absatz 2 RbDatenschutz um.

Satz 1 sieht zwei Ausnahmen für den Fall vor, dass die deutsche Behörde die nach Absatz 1 Nummer 3 erforderliche Zustimmung des Mitgliedstaates, aus dem die Daten stammen, nicht rechtzeitig einholen kann. Die Daten dürfen dann auch ohne vorherige Zustimmung an Drittstaaten oder an zwischen- oder überstaatliche Einrichtungen weitergeleitet werden. Voraussetzung dafür ist allerdings, dass einer der beiden folgenden Fälle vorliegt:

– Die Datenweiterleitung ist unerlässlich zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Mitgliedstaates oder eines Drittstaates (Nummer 1). Der Begriff „gegenwärtige und erhebliche Gefahr“ entspricht dem eingeführten Sprachgebrauch des IRG, siehe die Anmerkungen zu § 97b Absatz 1 Nummer 3 IRG-E. Erwägungsgrund 25 zum RbDatenschutz legt eine Auslegung des Begriffs als „akute Bedrohung“ nahe.

– Die Datenweiterleitung ist unerlässlich zur Abwehr einer gegenwärtigen und erheblichen Gefahr für wesentliche Interessen eines Mitgliedstaates (Nummer 2). Die Interessen eines Drittstaates werden hier – anders als in Nummer 1, wo Drittstaaten einbezogen sind – in Umsetzung der Vorgaben von Artikel 13 Absatz 2 RbDatenschutz nicht erfasst. Laut Erwägungsgrund 25 zum RbDatenschutz sind unter den Begriff „wesentliche Interessen“ solche zu fassen, die in der Bedeutung der öffentlichen Sicherheit gleichkommen. Beispielhaft werden die unmittelbare und ernsthafte Bedrohung der kritischen Infrastruktur oder die erhebliche Störung des Finanzsystems eines Mitgliedstaates genannt.

Satz 2 sieht vor, dass die übermittelnde Stelle unverzüglich die zuständige Behörde des betroffenen Mitgliedstaates unterrichten muss, wenn sie personenbezogene Daten ohne vorherige Zustimmung dieser Behörde an Drittstaaten oder an zwischen- oder überstaatliche Einrichtungen weitergeleitet hat.

Zu Absatz 3

Die Regelung setzt die Ausnahmeregelung aus Artikel 13 Absatz 3 RbDatenschutz um. Danach dürfen deutsche Behörden personenbezogene Daten in drei – alternativen – Fällen auch dann an Drittstaaten oder an zwischen- oder überstaatliche Einrichtungen weiterleiten, wenn auf der Seite der Empfänger kein angemessenes Datenschutzniveau besteht. Hierzu gehört die Wahrung überwiegender schutzwürdiger Interessen der betroffenen Person (Nummer 1). Ein weiterer Ausnahmefall ist die Wahrung überwiegender Interessen (Nummer 2). Hiervon sind zum einen die Interessen von dritten Personen erfasst; dieser Fall kann beispielsweise in Entführungsfällen eine Rolle spielen. Zum anderen unterfällt die Wahrung von wichtigen öffentlichen Interessen der Ausnahmeregelung, was im Einklang mit den europarechtlichen Vorgaben ausdrücklich erwähnt wird. Der Regelung liegt – in Übereinstimmung mit der entsprechenden Vorschrift in § 4c Absatz 1 Nummer 4 BDSG – das Verständnis zugrunde, dass es sich bei den öffentlichen Interessen grundsätzlich um die Interessen der Bundesrepublik Deutschland handeln muss. Darüber hinaus kann die Datenweiterleitung zulässig sein, wenn der Drittstaat oder die zwischen- oder überstaatliche Einrichtung jeweils angemessene Garantien zum Datenschutz anbietet. Der Begriff der Garantie wird aus dem RbDatenschutz in dem Verständnis in das IRG übernommen, dass hierunter insbesondere die Abgabe von angemessenen Zusicherungen und das Beachten von Bedingungen fallen. Solche Garantien können also beispielsweise in der Abgabe einer Zusicherung seitens der empfangenden Stelle gegenüber der übermittelnden deutschen Stelle bestehen, dass bestimmte Löschungs- oder Löschungs-prüffristen eingehalten

werden. Ob die Garantien angemessen sind, hat die übermittelnde Stelle auf der Grundlage des innerstaatlichen Rechts zu beurteilen.

Zu Nummer 3

Die Änderung ist eine redaktionelle Folgeänderung der Änderungen aus Nummer 2. Der bisherige Elfte Teil wird – inhaltlich unverändert – zu einem neuen Zwölften Teil des IRG.

Zu Artikel 5 (Änderung der Strafprozessordnung)

Zu Nummer 1

Aufgrund der Änderungen in § 488 Absatz 3 Satz 4 StPO sind künftig bei der Übermittlung personenbezogener Daten im automatisierten Abrufverfahren oder im automatisierten Anfrage- und Auskunftsverfahren in allen Fällen zumindest der Zeitpunkt des Abrufs, die abgerufenen Daten, die Kennung der abrufenden Stelle und das Aktenzeichen des Empfängers zu protokollieren. Hierdurch werden die in Artikel 10 Absatz 1 RbDatenschutz aufgestellten Vorgaben umgesetzt und zugleich die Voraussetzungen dafür geschaffen, dass die nach Artikel 22 Absatz 2 Buchstabe f RbDatenschutz für die automatisierte Datenverarbeitung zu gewährleistende Übermittlungskontrolle durchgeführt werden kann. Artikel 10 Absatz 1 RbDatenschutz schreibt die Protokollierung oder Dokumentierung jeder Übermittlung von personenbezogenen Daten zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung und der Sicherstellung der Integrität und Sicherheit der Daten vor. Nach § 488 Absatz 3 Satz 3 und 4 StPO muss bislang nur gewährleistet werden, dass die Übermittlung personenbezogener Daten durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann und soll lediglich bei jedem zehnten Abruf eine Protokollierung erfolgen. Die durch den Entwurf für § 488 StPO nunmehr vorgesehene Vollprotokollierung ist z. B. in § 11 Absatz 6 Satz 1 BKAG für die polizeilichen Informationssysteme beim BKA vorgegeben und deshalb in der Arbeit mit Dateien bereits üblich. Aus diesem Grund – und weil es allgemein der Gewährleistung der Datenschutzkontrolle und Datensicherheit dient – beschränken sich die Änderungen nicht auf den Anwendungsbereich des RbDatenschutz, sondern werden für alle zu verarbeitenden Daten vorgesehen.

§ 488 Absatz 3 Satz 5 StPO-E legt den Verwendungszweck der Protokolldaten für die Datenschutzkontrolle, insbesondere der Zulässigkeit der Abrufe sowie der Datensicherheit fest und schreibt die Löschung der Protokolldaten nach Ablauf von zwölf Monaten vor. Neu ist gegenüber der bestehenden Regelung, dass die Verwendung der Protokolldaten nunmehr über die bislang bereits mögliche Zulässigkeitskontrolle der Abrufe hinaus auch für die Datenschutzkontrolle und zur Datensicherheit erlaubt wird. Zum einen wird der Verwendungszweck dadurch an die durch Artikel 10 Absatz 1 RbDatenschutz vorgegebenen Kontrollzwecke angepasst und auch allgemein sichergestellt, dass die getroffenen Maßnahmen zur Gewährleistung der Datensicherheit geeignet sind, um die in Artikel 22 RbDatenschutz genannten Anforderungen zu erfüllen. Zum anderen sieht unabhängig von den Vorgaben des RbDatenschutz § 488 Absatz 1 Satz 2 StPO vor, dass der Datenschutz und die Datensicherheit durch entsprechende Maßnahmen sichergestellt werden müssen. Konsequenterweise sollen deshalb die Protokolldaten, die über die Wirksamkeit dieser Maßnahmen Aufschluss geben können, auch insoweit genutzt werden dürfen.

Der neu angefügte § 488 Absatz 4 StPO-E entspricht § 493 Absatz 4 StPO für den Bereich des ZStV. Er stellt – wie auch § 493 Absatz 4 StPO für das ZStV – lediglich klar, dass auch das in § 488 Absatz 1 Satz 1 StPO neben dem automatisierten Abrufverfahren ausdrücklich genannte Anfrage- und Auskunftsverfahren als Abrufverfahren im Sinne des Datenschutzrechts zu werten ist (vgl. Weßlau in: Systematischer Kommentar zur StPO, 4. Auflage, § 488 StPO, Rn. 1) und deshalb die Vorgaben in § 488 Absatz 2 und 3 StPO Anwendung finden, die sprachlich – im Gegensatz zu § 488 Absatz 1 Satz 1 StPO – allein auf das automatisierte Abrufverfahren abstellen.

Zu Nummer 2

§ 489 Absatz 10 StPO-E setzt Artikel 18 Absatz 1 Satz 3 RbDatenschutz um, nach dem für die Fälle, in denen der für die Verarbeitung Verantwortliche eine beantragte Berichtigung, Löschung oder Sperrung ablehnt, dies der betroffenen Person schriftlich mitzuteilen und sie auf die nach innerstaatlichem Recht vorgesehenen Möglichkeiten einer Beschwerde oder eines Rechtsbehelfs hinzuweisen ist. Eine ausdrückliche Verpflichtung zur schriftlichen Mitteilung unter Hinweis auf eine Rechtsschutzmöglichkeit sieht die Strafprozessordnung in den Dateiregelungen bislang nicht vor. Zwar dürfte in der Praxis die schriftliche Korrespondenz mit dem Betroffenen der Regelfall sein und deshalb faktisch bezüglich des Schriftlichkeitserfordernisses kein Umsetzungsbedarf bestehen.

Aufgrund der ausdrücklichen Vorgabe des RbDatenschutz, der auch den Hinweis auf die Rechtsschutzmöglichkeiten fordert, soll aber mit § 489 Absatz 10 StPO-E eine ausdrückliche Regelung geschaffen werden, die für alle verarbeiteten Daten gilt und damit über den Anwendungsbereich des RbDatenschutz hinausgeht. Eine Differenzierung zwischen personenbezogenen Daten, die dem RbDatenschutz unterfallen, und sonstigen, insbesondere rein innerstaatlichen Daten, wäre nicht sachgerecht. Absatz 10 bestimmt deshalb zunächst, dass die speichernde Stelle der betroffenen Person schriftlich mitteilt, wenn sie einer von ihr beantragten Berichtigung, Löschung oder Sperrung nicht nachkommt, und setzt damit das Schriftlichkeitserfordernis um. Zugleich wird die geforderte Hinweispflicht auf die gegen die ablehnende Entscheidung der speichernden Stelle bestehenden Rechtsbehelfe normiert. Rechtsbehelf gegen Entscheidungen der Strafverfolgungsbehörden, der Staatsanwaltschaft, soweit sie als Vollstreckungsbehörde handelt, der Bewährungshelfer, der Aufsichtsstellen bei der Führungsaufsicht und der Gerichtshilfe ist der nach den §§ 23 ff. EGGVG eröffnete Rechtsweg bei Justizverwaltungsakten zu den Oberlandesgerichten (§ 25 EGGVG). Sind die personenbezogenen Daten in einer Datei eines Gerichts gespeichert und wird durch das Gericht die beantragte Berichtigung, Löschung oder Sperrung abgelehnt, ist die Beschwerde nach den §§ 304 ff. StPO der einschlägige Rechtsbehelf.

Zu Nummer 3

Zu Buchstabe a

§ 490 Satz 2 StPO-E setzt die in Artikel 23 RbDatenschutz vorgegebene Vorabkonsultation um, nach der zu gewährleisten ist, dass die zuständigen nationalen Kontrollstellen vor der Verarbeitung personenbezogener Daten in neu zu errichtenden Dateien angehört werden. Die Vorabkonsultation wird für neu zu errichtende automatisierte Dateien vorgesehen. Der Wortlaut des Artikels 23 RbDatenschutz beschränkt sich zwar nicht ausdrücklich auf automatisierte Dateien. Nur in diesem Bereich entstehen aber über den Einzelfall hinaus abstrakte Gefahren durch die Verarbeitung einer unbestimmten Vielzahl personenbezogener Daten, denen durch eine Mitwirkung des jeweils zuständigen Landes- oder Bundesbeauftragten für den Datenschutz entgegengewirkt werden soll. Hierfür spricht auch die bestehende Regelung einer Vorabkonsultation in § 4d BDSG, die sich ebenfalls auf die automatisierte Datenverarbeitung beschränkt und sie zudem nur dem jeweiligen (behördlichen) Datenschutzbeauftragten auferlegt.

Andererseits geht die Umsetzung insofern über die ausdrückliche Vorgabe des Artikels 23 RbDatenschutz hinaus, als sich die Vorabkonsultation nicht auf die praktisch schwierig abgrenzbaren Fälle beschränken soll, in denen besondere Kategorien von Daten nach Artikel 6 RbDatenschutz verarbeitet werden.

Als Folgeänderung zu der verpflichtenden Vorabkonsultation enthält Satz 3 eine Eilfallregelung. Diese gilt für Fälle, in denen aus Ermittlungsgründen zeitnah eine automatisierte Datei angelegt werden muss und die für den Datenschutz zuständige Stelle, z. B. am Wochenende, nicht rechtzeitig beteiligt werden kann. In diesen Fällen ist nach Satz 4 die Konsultation unverzüglich nachzuholen. Die Regelung orientiert sich an denjenigen in § 34 Absatz 3 BKAG, § 36 Absatz 2 Satz 2 BPolG und § 41 Absatz 3 ZFdG. Auf die Ausführungen zu diesen Vorschriften im Allgemeinen Teil zu Ziffer III. wird Bezug genommen.

Zu Buchstabe b

Als Folgeänderung wird der bisherige § 490 Satz 2 StPO in modifizierter Weise zu § 490 Satz 5 StPO-E und beschränkt damit die Pflicht zur Vorabkonsultation auf Dateien, die nicht nur vorübergehend vorgehalten und nicht innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden. Dies entspricht den Vorgaben des Artikels 23 RbDatenschutz, demzufolge eine Vorabkonsultation insbesondere dann erforderlich ist, wenn die Art der Verarbeitung, insbesondere aufgrund neuer Technologien, Mechanismen oder Verfahren, andernfalls spezifische Risiken für die Grundrechte und Grundfreiheiten und insbesondere der Privatsphäre der Betroffenen birgt.

Zu Nummer 4

Zu Buchstabe a

Wie in § 488 Absatz 3 Satz 4 StPO-E bewirkt die Änderung in § 493 Absatz 3 Satz 3 StPO-E, dass der Zeitpunkt des Abrufs, die abgerufenen Daten, die Kennung der abrufenden Stelle und das Aktenzeichen des Empfängers nicht nur zumindest bei jedem zehnten Abruf protokolliert werden müssen, sondern nunmehr bei jedem Abruf. Dies dient wie bei § 488 Absatz 3 Satz 4 StPO-E der Umsetzung der in Artikel 10 Absatz 1 RbDatenschutz

aufgestellten Vorgaben, nach denen die Protokollierung oder Dokumentierung jeder Übermittlung von personenbezogenen Daten zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung und der Sicherstellung der Integrität und Sicherheit der Daten vorgeschrieben ist. Zugleich werden so die Voraussetzungen dafür geschaffen, dass die nach Artikel 22 Absatz 2 Buchstabe f RbDatenschutz für die automatisierte Datenverarbeitung zu gewährleistende Übermittlungskontrolle durchgeführt werden kann. Wie auch bei § 488 Absatz 3 Satz 4 StPO-E beschränken sich die Änderungen nicht nur auf den Anwendungsbereich des RbDatenschutz, sondern gelten für alle zu verarbeitenden Daten.

Zu Buchstabe b

Wie bei § 488 Absatz 3 Satz 5 StPO-E legt § 493 Absatz 3 Satz 4 StPO-E den Verwendungszweck der Protokolldaten für die Datenschutzkontrolle, insbesondere der Zulässigkeit der Abrufe, sowie die Kontrolle der Datensicherheit fest und schreibt die Löschung der Protokolldaten nach Ablauf von sechs Monaten vor. Neu ist gegenüber der bestehenden Regelung, dass die Verwendung der Protokolldaten nunmehr über die bislang bereits mögliche Zulässigkeitskontrolle der Abrufe hinaus auch die Verwendung allgemein zur Datenschutzkontrolle und zur Datensicherheit erlaubt. Wie bei § 488 Absatz 3 Satz 5 StPO-E wird zum einen der Verwendungszweck dadurch an die durch Artikel 10 Absatz 1 RbDatenschutz vorgegebenen Kontrollzwecke angepasst und auch allgemein sichergestellt, dass die getroffenen Maßnahmen zur Gewährleistung der Datensicherheit geeignet sind, um die in Artikel 22 RbDatenschutz genannten Anforderungen zu erfüllen. Zum anderen sieht unabhängig von den Vorgaben des RbDatenschutz § 493 Absatz 1 Satz 2 StPO bereits vor, dass die beteiligten Stellen gewährleisten müssen, dass dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden müssen. Deshalb dürfen die Protokolldaten, die über die Wirksamkeit dieser Maßnahmen Aufschluss geben können, auch insoweit genutzt werden.

Zu Nummer 5

In § 494 Absatz 3 StPO wird zusätzlich der Verweis auf § 489 Absatz 10 StPO(-E) aufgenommen. § 489 Absatz 10 StPO-E setzt Artikel 18 Absatz 1 Satz 3 RbDatenschutz um, nach dem für die Fälle, in denen der für die Verarbeitung Verantwortliche eine beantragte Berichtigung, Löschung oder Sperrung ablehnt, dies der betroffenen Person schriftlich mitzuteilen und sie auf die nach innerstaatlichem Recht vorgesehenen Möglichkeiten einer Beschwerde oder eines Rechtsbehelfs hinzuweisen ist. Eine ausdrückliche Verpflichtung zur schriftlichen Mitteilung unter Hinweis auf eine Rechtsschutzmöglichkeit sieht die Strafprozessordnung für das ZStV bislang nicht vor. Zwar dürfte in der Praxis die schriftliche Korrespondenz mit dem Betroffenen der Regelfall sein und deshalb faktisch bezüglich des Schriftlichkeitserfordernisses kein zusätzlicher praktischer Umsetzungsbedarf bestehen. Aufgrund der ausdrücklichen Vorgabe des RbDatenschutz, der auch den Hinweis auf die Rechtsschutzmöglichkeiten fordert, soll über die entsprechende Anwendung des § 489 Absatz 10 StPO-E eine ausdrückliche Regelung geschaffen werden, die für alle im ZStV verarbeiteten Daten gilt und damit über den Anwendungsbereich des RbDatenschutz hinausgeht. Eine Differenzierung zwischen personenbezogenen Daten, die dem RbDatenschutz unterfallen, und sonstigen, insbesondere rein innerstaatlichen Daten, wäre – wie in § 489 Absatz 10 StPO-E – nicht sachgerecht. Über § 489 Absatz 10 StPO-E gilt für das ZStV, dass das BfJ als Registerbehörde (§ 492 Absatz 1 StPO) der betroffenen Person schriftlich mitteilt, wenn es einer von ihr beantragten Berichtigung, Löschung oder Sperrung nicht nachkommt; damit wird das Schriftlichkeitserfordernis umgesetzt. Zugleich wird die geforderte Hinweispflicht auf die gegen die ablehnende Entscheidung des BfJ bestehenden Rechtsbehelfe umgesetzt. Rechtsbehelf ist neben der Dienst- oder Fachaufsichtsbeschwerde der nach den §§ 23 ff. EGGVG bei Justizverwaltungsakten eröffnete Rechtsweg zum Oberlandesgericht (§ 25 EGGVG).

Zu Artikel 6 (Änderung des Gesetzes über Ordnungswidrigkeiten)

Die Änderung von § 110d Absatz 2 Satz 4 des Gesetzes über Ordnungswidrigkeiten ist eine redaktionelle Folgeänderung zur Änderung von § 488 Absatz 3 Satz 4 StPO.

Zu Artikel 7 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.

Anlage 2

Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKRG:

Entwurf eines Gesetzes zur Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (NKR-Nr. 3017)

Der Nationale Normenkontrollrat hat den Entwurf des oben genannten Regelungsvorhabens geprüft.

I. Zusammenfassung

Bürgerinnen und Bürger Erfüllungsaufwand:	Keine Auswirkungen
Wirtschaft Erfüllungsaufwand:	Keine Auswirkungen
Verwaltung Erfüllungsaufwand Bund und Länder:	Moderater, jedoch nicht abschätzbarer Mehraufwand
1:1-Umsetzung von EU-Recht (Gold plating)	Dem NKR liegen keine Anhaltspunkte dafür vor, dass mit den vorliegenden Regelungen über eine 1:1-Umsetzung hinausgegangen wird.
Die Regelungsmaterie des vorliegenden Gesetzentwurfs ist sehr komplex. Dies wirkt sich auch auf die Ermittlung und Darstellung möglichen zusätzlichen Erfüllungsaufwandes aus. So ist es äußerst schwierig, abzuschätzen, welche der Vorgaben über vorhandenes deutsches Datenschutzrecht (ob allgemein oder spezialgesetzlich geregelt) bzw. die bestehende Verwaltungspraxis hinausgehen und in welchen (Einzel)Fällen dies Auswirkungen auf den Erfüllungsaufwand hat. Die Aussage des Ressorts, dass insgesamt ein moderater Anstieg des Erfüllungsaufwandes für die Verwaltung von Bund und Ländern anzunehmen ist, erscheint glaubhaft. Dem Nationalen Normenkontrollrat liegen – auch Seitens der Länder – keine anderen Anhaltspunkte vor. Obgleich die Auswirkungen auf den Erfüllungsaufwand durch das Ressort nicht abschließend dargestellt wurden und konkrete Aussagen zu Fallzahlen und Kosten fehlen, macht der Nationale Normenkontrollrat im Rahmen seines gesetzlichen Auftrags keine Einwände gegen die Darstellungen der Gesetzesfolgen im vorliegenden Regelungsvorhaben geltend.	

II. Im Einzelnen

Mit dem Regelungsvorhaben soll der „EU-Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden“ umgesetzt werden. Der Rahmenbeschluss wurde bereits am 27. November 2008 vom Rat der Innen- und Justizminister der Europäischen Union angenommen. Der Rahmenbeschluss zielt darauf ab, dass bestimmte Datenschutzstandards bei der Übermittlung personenbezogener Daten zwischen Behörden einzelner Mitgliedsstaaten sichergestellt werden. Dieser Datenaustausch wurde zuvor mit „Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union“ ermöglicht.

Das geltende Bundesrecht enthält bereits zahlreiche bereichsspezifische Vorschriften zum Schutz personenbezogener Daten. Diese gewährleisten ein hohes Schutzniveau für in Deutschland bei Polizeibehörden, Staatsanwaltschaften und Strafgerichten verarbeitete personenbezogene Daten und verfolgen zumeist auch Regelungsansätze, die mit denen des Rahmenbeschlusses identisch sind. In einigen Fällen wird der Grundrechtsschutz für die von der Datenverarbeitung Betroffenen jedoch auf andere Weise als im Rahmenbeschluss vorgesehen verwirklicht. In Teilen war die Umsetzung der Vorgaben des Rahmenbeschlusses bisher auf dem Erlasswege geregelt worden. In diesen Fällen besteht ein Änderungsbedarf im innerstaatlichen Recht, der mit vorliegendem Gesetzentwurf umgesetzt werden soll.

Geändert werden sollen folgende Gesetze:

- Bundeskriminalamtgesetz
- Bundespolizeigesetz
- Zollfahndungsdienstgesetz
- Gesetz über die internationale Rechtshilfe in Strafsachen
- Strafprozessordnung

Für eine differenzierende Umsetzung des Rahmenbeschlusses in den betroffenen Einzelgesetzen an Stelle einer einheitlichen Regelung hat sich das Ressort auch deshalb entschieden, weil der Rahmenbeschluss nach den derzeitigen Planungen der Europäischen Union in absehbarer Zeit durch eine „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“ abgelöst werden soll.

III. Zum Erfüllungsaufwand

Bürgerinnen und Bürgern entsteht kein Erfüllungsaufwand. Betroffen ist Verwaltung von Bund und Ländern.

Durch die Umsetzung des Rahmenbeschlusses wird sich auf Bundesebene der Verwaltungsaufwand nach Einschätzung des Ressort nur moderat erhöhen. Betroffen sind das Bundeskriminalamt (BKA), die Behörden der Bundespolizei, die Behörden des Zollfahndungsdienstes, das Bundesamt für Justiz (BfJ), den Generalbundesanwalt (GBA) und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Gleiches gilt auf Landesebene für die Staatsanwaltschaften und die Polizeibehörden.

Bundeskriminalamtgesetz, Bundespolizeigesetz, Zollfahndungsdienstgesetz

Für das Bundeskriminalamt, die Bundespolizei und die Behörden des Zollfahndungsdienstes werden die nachfolgenden Vorgaben neu eingeführt.

- Einholung der Zustimmung der zuständigen Behörde eines anderen Mitgliedstaates vor einer Datenübermittlung an nicht-öffentliche Stellen
- Einholung der Zustimmung der zuständigen Behörde eines anderen Mitgliedstaates vor einer Datenübermittlung an Drittstaaten
- Unterrichtung der zuständigen Behörde eines anderen Mitgliedstaates nach einer Datenübermittlung im Eilfall
- Überprüfung von Daten vor ihrer Übermittlung
- Beifügung von Informationen für den Empfänger von Daten
- Angabe von Aufbewahrungsfristen für die Daten
- Hinweis an den Empfänger auf besondere bundesgesetzliche Verwendungsregelungen für den Datenaustausch

- Ersuchen an Empfänger, den Betroffenen nicht ohne vorherige Zustimmung der übermittelnden Stelle zu informieren
- Übermittlung personenbezogener Daten an nicht-öffentliche Stellen in Mitgliedstaaten der EU
- Einholung der vorherigen Zustimmung des übermittelnden Mitgliedstaates
- Auskunfterteilung zur Datenverwendung auf Ersuchen des übermittelnden Staates
- Protokollierung aller Abrufe bei automatisierten Abrufverfahren
- Hinweis an den Empfänger auf Verwendungsbeschränkungen
- Einholung der Zustimmung vor Datenübermittlung

Das Ressort geht davon aus, dass der Zollfahndungsdienst diese Anforderungen aufgrund bereichsspezifischer Datenschutzregelungen bereits erfüllt. Der Aufwand für Bundeskriminalamt und Bundespolizei sei in Ermangelung belastbarer Fallzahlen nicht bezifferbar.

Gesetz über die internationale Rechtshilfe in Strafsachen (IRG)

Es werden folgende Vorgaben neu eingeführt. Diese verstehen sich teilweise als bloße Klarstellung einer bereits geltenden Rechtslage oder Rechtspraxis.

- Verpflichtung zur Einholung der Zustimmung der zuständigen Behörde eines anderen Mitgliedstaates vor einer Daten-übermittlung an nicht-öffentliche Stellen
- Verpflichtung, die empfangende Stelle auf besondere Verwendungsregelungen für den Datenaustausch hinzuweisen
- Verpflichtung, die empfangende Stelle zu unterrichten, wenn sich herausstellt, dass Daten nicht hätten übermittelt werden dürfen oder dass unrichtige Daten übermittelt wurden
- Verpflichtung zur Einholung einer vorherigen Zustimmung des übermittelnden Mitgliedstaates zur Weiterleitung von Daten an zwischen- oder überstaatliche Stellen oder zur nachträglichen Unterrichtung über die Weiterleitung

Durch die Änderungen im IRG ergibt sich für die Justizbehörden der Länder (insbesondere Staatsanwaltschaften und Gerichte) ein insgesamt moderater Erfüllungsaufwand, der sich laut Ressort aufgrund nicht abschätzbarer Fallzahlen allerdings nicht konkret beziffern lässt. Die Einrichtung neuer Organisationsstrukturen in den Ländern ist nach Einschätzung des Ressorts nicht erforderlich.

Auch für den Bund (Bundesamt für Justiz, Generalbundesanwalt) fällt nach Einschätzung des Ressorts ein insgesamt verhältnismäßig geringer Erfüllungsaufwand an, der sich mangels vorhersehbarer Fallzahlen jedoch ebenfalls nicht beziffern lässt. Maßgeblich sind insoweit die Kosten, die beim BfJ und beim GBA anfallen

Strafprozessordnung

Im Bereich der Strafprozessordnung ergeben sich folgende Änderungen:

- Verpflichtende Protokollierung durch die speichernde Stelle bei jeder Übermittlung im automatisierten Abrufverfahren und im automatisierten Anfrage- und Auskunftsverfahren nach § 488 Absatz 1 StPO statt bisheriger „Soll-Regelung“ der Speicherung der Protokolldaten bei jedem zehnten Abruf
- Neueinführung einer Pflicht der speichernden Stelle, der betroffenen Person eine Nichtvornahme einer beantragten Berichtigung, Löschung oder Sperrung schriftlich mitzuteilen sowie sie auf bestehende Rechtsbehelfe hinzuweisen
- In Fällen der Neuerrichtung automatisierter Dateien Neueinführung einer Verpflichtung zur Anhörung des zuständigen Datenschutzbeauftragten vor der Verarbeitung personenbezogener Daten in diesen

- Verpflichtende Protokollierung durch die Registerbehörde bei jedem Abruf statt bisher bei jedem zehnten Abruf
- Neueinführung einer Pflicht der Registerbehörde, der betroffenen Person eine Nichtvornahme einer beantragten Berichtigung, Löschung oder Sperrung schriftlich mitzuteilen sowie sie auf bestehende Rechtsbehelfe hinzuweisen

Auch hier schätzt das Ressort den entstehenden Aufwand für Bund (Bundesamt für Justiz, Generalbundesanwalt) und Länder als gering ein und weist darauf hin, dass dieser in seiner konkreten Höhe zu beziffern sei. Diese Einschätzung speise sich auch aus den Rückmeldungen der Länder.

Fazit

Die Regelungsmaterie des vorliegenden Gesetzentwurfs ist sehr komplex. Dies wirkt sich auch auf die Ermittlung und Darstellung möglichen zusätzlichen Erfüllungsaufwandes aus. So ist es äußerst schwierig, abzuschätzen, welche der Vorgaben über vorhandenes deutsches Datenschutzrecht (ob allgemein oder spezialgesetzlich geregelt) bzw. die bestehende Verwaltungspraxis hinausgehen und in welchen (Einzel)Fällen dies Auswirkungen auf den Erfüllungsaufwand hat. Die Aussage des Ressorts, dass insgesamt ein moderater Anstieg des Erfüllungsaufwandes für die Verwaltung von Bund und Ländern anzunehmen ist, erscheint glaubhaft. Dem Nationalen Normenkontrollrat liegen – auch Seitens der Länder – keine anderen Anhaltspunkte vor.

Obgleich die Auswirkungen auf den Erfüllungsaufwand durch das Ressort nicht abschließend dargestellt wurden und konkrete Aussagen zu Fallzahlen und Kosten fehlen, macht der Nationale Normenkontrollrat im Rahmen seines gesetzlichen Auftrags keine Einwände gegen die Darstellungen der Gesetzesfolgen im vorliegenden Regelungsvorhaben geltend.

Grieser
Stellv. Vorsitzende

Prof. Dr. Kuhlmann
Berichterstatterin

Anlage 3

Stellungnahme des Bundesrates

Der Bundesrat hat in seiner 936. Sitzung am 25. September 2015 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

Zu Artikel 4 Nummer 2 (§ 97b Absatz 1 Satz 2 – neu – IRG)

In Artikel 4 Nummer 2 ist dem § 97b Absatz 1 folgender Satz anzufügen:

„Fristen zur Löschung, Sperrung und Aussonderung sowie zu Verwendungsbeschränkungen nach dem nationalen Recht der übermittelnden Behörde, auf die sie hingewiesen hat, sind zu beachten."

Begründung:

Nach den Artikeln 9 und 12 RbDatenschutz ist die empfangende Stelle verpflichtet, innerstaatliche Löschungsfristen und Verarbeitungsbeschränkungen der übermittelnden Stelle zu beachten. Für die Datenverarbeitung durch das Bundeskriminalamt, die Bundespolizei und den Zoll sieht der Gesetzentwurf daher entsprechende Regelungen vor (§ 27a Absatz 1 Satz 3 und § 32 Absatz 10 Satz 1 BKAG-E; § 33a Absatz 2 Satz 2 und § 35 Absatz 10 Satz 1 BPolG-E; § 35a Absatz 1 Satz 3 und § 39 Absatz 11 Satz 1 ZFahnDG-E).

Für das Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) hat die Bundesregierung auf eine explizite Umsetzung mit der Begründung verzichtet, es entspräche den Grundsätzen der Rechtshilfe, dass auf verfahrensrechtliche Erfordernisse oder sonstige Anliegen ersuchender oder ersuchter Staaten Rücksicht zu nehmen sei.

Allerdings sieht § 72 IRG vor, dass Bedingungen, die der ersuchte Staat an die Rechtshilfe geknüpft hat, zu beachten sind. In dem – wie bislang – weitgehend auf völkerrechtlicher Basis abgewickelten Rechtshilfeverkehr in Strafsachen ist daher die Bindungswirkung von Bedingungen bei ausgehenden Ersuchen offenkundig und entspricht dem Leitbild einer vertraglichen Beziehung zwischen den auf völkerrechtlicher Basis agierenden nationalen Strafverfolgungsorganen.

Dagegen stellen der mit dem EU-Recht eingeführte Grundsatz der gegenseitigen Anerkennung justizieller Entscheidungen und der Grundsatz der Verfügbarkeit eine Neukonzeption der strafrechtlichen Zusammenarbeit dar, die den Anspruch hat, die Rechtsbeziehungen zwischen Justizorganen der EU-Mitgliedstaaten unmittelbar zu regeln. Grundlage sind die in nationales Recht transponierten Rechtsakte des EU-Sekundärrechts, die umfassend und ausschließlich Befugnisse und Grenzen der strafrechtlichen Zusammenarbeit bestimmen; aus einer ursprünglich am Vertragsrecht orientierten völkerrechtlichen Beziehung, in der die Gewährleistung von Rechtshilfe im Kern das Ergebnis eines Einigungsprozesses zwischen anbietender und annehmender Vertragspartei war, ist eine durch das EU-Recht gestiftete und gestaltete Rechtsbeziehung geworden, die einen eigenen Entscheidungsspielraum im Sinne autonomer völkerrechtlicher Subjekte nicht mehr vorsieht.

Dies hat zur Folge, dass die Gewährung von Rechtshilfe im Rahmen der gegenseitigen Anerkennung beziehungsweise des Grundsatzes der Verfügbarkeit bedingungsfrei zu erfolgen hat, wenn nicht die im Einzelfall einschlägige EU-Rechtsgrundlage die Stellung einer Bedingung ausdrücklich vorsieht. Tatsächlich finden sich entsprechende Regelungen in einzelnen Rechtsinstrumenten, beispielsweise bei der grenzüberschreitenden Überwachung des Telekommunikationsverkehrs nach den Artikeln 30 Absatz 5 Satz 2 beziehungsweise 31 Absatz 3 Buchstabe b EEG.

Nicht ohne Grund hat sich daher der europäische Gesetzgeber entschieden, die Beachtung von innerstaatlichen Verarbeitungsbeschränkungen oder Löschungsfristen explizit in den RbDatenschutz aufzunehmen. Der Rahmenbeschluss findet auf jeglichen Datenaustausch zwischen den Mitgliedstaaten Anwendung, ganz gleich auf welcher Rechtsgrundlage dieser erfolgte, und unterwirft die automatisierte und dateiförmige Verarbeitung der übermittelten Daten – unabhängig davon, in welche Richtung sie übermittelt wurden – einem einheitlichen europäischen Regime. Er schafft damit nicht nur einen Mindeststandard, sondern begrenzt zugleich die sich aus den Rechtsakten zur gegenseitigen Anerkennung und Verfügbarkeit ergebende Kooperationsverpflichtung, soweit sie nicht speziellere datenschutzrechtliche Regelungen enthalten (Artikel 28 RbDatenschutz).

Entgegen der in dem Gesetzentwurf vertretenen Auffassung haben die vorgenannten Artikel 9 und 12 RbDatenschutz daher nicht einen rein deklaratorischen beziehungsweise klarstellenden Charakter, der lediglich einen ohnehin in den rechtshilferechtlichen Beziehungen zwischen den Mitgliedstaaten geltenden Grundsatz formuliert.

Die Beachtung einer europarechtlichen Regelung aus dem Bereich der ehemaligen Dritten Säule des Maastrichter Vertrags durch den nationalen Rechtsanwender setzt grundsätzlich die Umsetzung in nationales Recht voraus (Artikel 34 Absatz 2 Buchstabe b Satz 2 EUV a. F.). Sofern das IRG keine den Artikeln 9 und 12 RbDatenschutz entsprechende Vorschrift enthält, ist die Beachtung – zumindest bei der Zusammenarbeit auf Grundlage von Rechtsinstrumenten in Umsetzung der Grundsätze der gegenseitigen Anerkennung beziehungsweise der Verfügbarkeit – nicht zwingend, was jedoch nicht den Vorgaben des Rahmenbeschlusses entspräche und damit europarechtswidrig wäre.

Die Beachtung von entsprechenden Bedingungen ergibt sich auch nicht aus § 72 IRG. Zum einen kommt eine Anwendbarkeit von § 72 IRG im Bereich der gegenseitigen Anerkennung und des Grundsatzes der Verfügbarkeit wegen der grundsätzlichen Bedingungsfeindlichkeit – wie oben ausgeführt – nicht in Betracht. Hinzu kommt, dass sich § 72 IRG nur auf ausgehende Ersuchen bezieht (vgl. die Überschrift zum Sechsten Teil des IRG); die in den Artikeln 9 und 12 RbDatenschutz vorgesehene Verwendungsbindung regelt aber die Zurverfügungstellung jeglicher Daten, unabhängig davon, ob das Datum im Rahmen der Erledigung oder bei Stellung eines Ersuchens übermittelt wird.

Schließlich, worauf von Seiten der Praxis hingewiesen worden ist, legen Gründe der Gesetzessystematik eine einheitliche Fassung der Gesetze zur Umsetzung des RbDatenschutz nahe, da identische Datenschutzaspekte betroffen sind und sich die Gründe für die unterschiedliche Umsetzungslage in den für die präventive Datenübermittlung geltenden Polizeigesetzen des Bundes und dem für Strafverfolgungszwecke geltenden IRG der rechtanwendenden Person nicht erschließen.

Anlage 4

Gegenäußerung der Bundesregierung

Die Bundesregierung nimmt zu dem Vorschlag des Bundesrates wie folgt Stellung:

Zu Artikel 4 Nummer 2 (§ 97b Abs. 1 Satz 2 – neu – IRG)

Die Bundesregierung stellt sich dem Vorschlag des Bundesrates zur Ergänzung der Norm nicht grundsätzlich entgegen. Die Bundesregierung gibt aber zu bedenken, dass Bedingungen bereits nach den Vorschriften der klassischen Rechtshilfe zu beachten sind. Dies gilt sowohl im Rahmen von eingehenden als auch im Rahmen von ausgehenden Rechtshilfeersuchen (§ 72 IRG, Nummer 22 Absatz 1 Satz 2 RiVASt). Der umzusetzende Rahmenbeschluss ändert an der Gültigkeit dieser Vorschriften nichts. Der Rb Datenschutz ist kein Rechtsinstrument, das auf dem Grundsatz der gegenseitigen Anerkennung beruht und insoweit möglicherweise als „bedingungsfeindlich“ anzusehen wäre. Zudem regelt der Rahmenbeschluss ausdrücklich nur ein datenschutzrechtliches Mindestniveau, siehe Artikel 1 Absatz 5 Rb Datenschutz. Den Mitgliedstaaten bleibt es damit unbenommen, einen höheren datenschützenden Standard zu setzen. Dies kann durch die Mitteilung rechtshilferechtlicher Bedingungen erfolgen, die von den anderen Mitgliedstaaten zu beachten sind. Die Bundesregierung geht deshalb davon aus, dass die von dem Bundesrat vorgeschlagene Ergänzung von § 97b IRG-E lediglich klarstellende Funktion hat.

Mit Blick auf die konkrete Formulierung ist Sorge zu tragen, dass die klarstellende Regelung ausreichend weit gefasst ist, um alle praxisrelevanten Fälle abzudecken. Insbesondere sollten aus Sicht der Bundesregierung auch die sogenannten Löschungsprüffristen erwähnt werden. Die Bundesregierung wird im Laufe des weiteren Gesetzgebungsverfahrens einen Formulierungsvorschlag vorlegen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333