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

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. In § 10 Absatz 3 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 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 die Daten zu löschen, zu sperren oder daraufhin zu überprüfen hat, ob ihre Speicherung noch erforderlich ist.

*) Dieses Gesetz dient der Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. No-vember 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).

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 folgende 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 Gesetz über das Zollkriminalamt und die Zollfahndungsämter 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 zugrundeliegende 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 folgende 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

§ 97a Anwendungsbereich

§ 97b Verwendung von Daten

§ 97c Übermittlung oder Bereitstellung von Daten

§ 97d Weiterleitung von Daten an Drittstaaten sowie an zwischen- oder überstaatliche Einrichtungen“.

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

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,

Anlage 4

Gegenäußerung der Bundesregierung zu der Stellungnahme des Bundesrates

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.