

## III

(In Anwendung des EU-Vertrags erlassene Rechtsakte)

IN ANWENDUNG VON TITEL VI DES EU-VERTRAGS ERLASSENE  
RECHTSAKTE

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**

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Europäische Union, insbesondere auf die Artikel 30, 31 und Artikel 34 Absatz 2 Buchstabe b,

auf Vorschlag der Kommission,

nach Stellungnahme des Europäischen Parlaments <sup>(1)</sup>,

in Erwägung nachstehender Gründe:

- (1) Die Europäische Union hat sich das Ziel gesetzt, die Union als einen Raum der Freiheit, der Sicherheit und des Rechts zu erhalten und weiterzuentwickeln in dem durch ein gemeinsames Vorgehen der Mitgliedstaaten bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen ein hohes Maß an Sicherheit gewährleistet werden soll.
- (2) Ein gemeinsames Vorgehen im Bereich der polizeilichen Zusammenarbeit gemäß Artikel 30 Absatz 1 Buchstabe b des Vertrags über die Europäische Union und ein gemeinsames Vorgehen im Bereich der justiziellen Zusammenarbeit in Strafsachen gemäß Artikel 31 Absatz 1 Buchstabe a des Vertrags über die Europäische Union setzen voraus, dass einschlägige Informationen verarbeitet werden; dies sollte nach Maßgabe geeigneter Bestimmungen über den Schutz personenbezogener Daten erfolgen.
- (3) Die im Rahmen von Titel VI des Vertrags über die Europäische Union erlassenen Rechtsvorschriften sollen die polizeiliche und justizielle Zusammenarbeit in Strafsachen in Bezug auf ihre Effizienz und Rechtmäßigkeit sowie die Achtung der Grundrechte — insbesondere des Rechts auf den Schutz der Privatsphäre und den Schutz personenbezogener Daten — verbessern. Gemeinsame Normen für die Verarbeitung und den Schutz personenbezogener Daten, die zum Zwecke der Kriminali-

tätsverhütung und -bekämpfung verarbeitet werden, tragen zur Erreichung dieser Ziele bei.

- (4) Im Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, das der Europäische Rat am 4. November 2004 angenommen hat, wurde die Notwendigkeit eines innovativen Konzepts für den grenzüberschreitenden Austausch von strafverfolungsrelevanten Informationen unter strenger Einhaltung bestimmter Kernbedingungen für den Datenschutz hervorgehoben und die Kommission ersucht, bis spätestens Ende 2005 entsprechende Vorschläge vorzulegen. Dieser Aufforderung wurde mit dem Aktionsplan des Rates und der Kommission zur Umsetzung des Haager Programms zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union entsprochen <sup>(2)</sup>.
- (5) Der Austausch personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, insbesondere nach dem im Haager Programm festgelegten Grundsatz der Verfügbarkeit von Informationen, sollte durch klare Bestimmungen unterstützt werden, die das gegenseitige Vertrauen zwischen den zuständigen Behörden fördern und sicherstellen, dass die betreffenden Informationen so geschützt werden, dass eine Diskriminierung dieser Zusammenarbeit zwischen den Mitgliedstaaten ausgeschlossen ist und gleichzeitig die Grundrechte der betroffenen Personen in vollem Umfang gewahrt bleiben. Die geltenden Rechtsvorschriften auf europäischer Ebene reichen hierfür nicht aus. 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 <sup>(3)</sup> findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß Titel VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich.

<sup>(1)</sup> ABl. C 125 E vom 22.5.2008, S 154.

<sup>(2)</sup> ABl. C 198 vom 12.8.2005, S. 1.

<sup>(3)</sup> ABl. L 281 vom 23.11.1995, S. 31.

- (6) Dieser Rahmenbeschluss gilt nur für Daten, die von zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen erhoben oder verarbeitet werden. Dieser Rahmenbeschluss sollte es den Mitgliedstaaten überlassen, auf nationaler Ebene näher zu bestimmen, welche anderen Zwecke als unvereinbar mit dem Zweck gelten, für die die personenbezogenen Daten ursprünglich erhoben wurden. Eine Weiterverarbeitung zu historischen, statistischen oder wissenschaftlichen Zwecken sollte im Allgemeinen nicht als unvereinbar mit dem ursprünglichen Zweck der Verarbeitung angesehen werden.
- (7) Der Anwendungsbereich dieses Rahmenbeschlusses beschränkt sich auf die Verarbeitung personenbezogener Daten, die zwischen Mitgliedstaaten weitergegeben oder bereitgestellt werden. Aus dieser Beschränkung sollten keine Schlüsse hinsichtlich der Zuständigkeit der Union für die Annahme von Rechtsakten über die Erhebung und Verarbeitung personenbezogener Daten auf nationaler Ebene bzw. hinsichtlich der Frage gezogen werden, ob die Union künftig derartige Rechtsakte annehmen sollte.
- (8) Die Mitgliedstaaten beabsichtigen, zur Erleichterung des Datenaustauschs in der Union, sicherzustellen, dass bei der Datenverarbeitung im innerstaatlichen Bereich ein Datenschutzstandard gewährleistet wird, der dem in diesem Rahmenbeschluss festgelegten Datenschutzstandard entspricht. Was die nationale Datenverarbeitung angeht, so hindert dieser Rahmenbeschluss die Mitgliedstaaten nicht daran, Bestimmungen zum Schutz personenbezogener Daten zu erlassen, die strenger sind als die Bestimmungen dieses Rahmenbeschlusses.
- (9) Dieser Rahmenbeschluss sollte nicht für personenbezogene Daten gelten, die ein Mitgliedstaat im Anwendungsbereich dieses Rahmenbeschlusses erlangt hat und die aus diesem Mitgliedstaat stammen.
- (10) Die Angleichung der Rechtsvorschriften der Mitgliedstaaten sollte nicht zu einer Lockerung des Datenschutzes in diesen Ländern führen, sondern vielmehr auf ein hohes Maß an Schutz in der gesamten Union abstellen.
- (11) Es ist erforderlich, die Ziele des Datenschutzes im Rahmen der polizeilichen und justiziellen Tätigkeiten sowie Bestimmungen über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten festzulegen, um sicherzustellen, dass alle ausgetauschten Informationen auch rechtmäßig und nach den für die Datenqualität geltenden Grundsätzen verarbeitet wurden. Gleichzeitig dürfen die rechtmäßigen Tätigkeiten der Polizei-, Zoll-, Justiz- und sonstigen zuständigen Behörden in keiner Weise behindert werden.
- (12) Der Grundsatz der sachlichen Richtigkeit der Daten ist unter Berücksichtigung von Art und Zweck der jeweiligen Verarbeitung anzuwenden. So basieren insbesondere in einem Gerichtsverfahren Daten auf der subjektiven Wahrnehmung von Personen und sind in einigen Fällen in keiner Weise nachprüfbar. Infolgedessen kann sich die Vorschrift der sachlichen Richtigkeit nicht auf die Richtigkeit einer Aussage beziehen, sondern lediglich auf die Tatsache, dass eine bestimmte Aussage gemacht worden ist.
- (13) Eine Archivierung in einem gesonderten Datenbestand sollte erst dann zulässig sein, wenn die Daten nicht mehr für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen benötigt und verwendet werden. Eine Archivierung in einem gesonderten Datenbestand ist auch dann zulässig, wenn die archivierten Daten in einer Datenbank mit anderen Daten so gespeichert werden, dass sie nicht mehr für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen verwendet werden können. Die Angemessenheit des Zeitraums der Archivierung sollte sich nach den Zwecken der Archivierung und den legitimen Interessen der Betroffenen richten. Bei einer Archivierung zu historischen Zwecken kann ein sehr langer Zeitraum in Betracht kommen.
- (14) Daten können auch dadurch gelöscht werden, dass der Datenträger vernichtet wird.
- (15) Bei unrichtigen, unvollständigen oder nicht mehr aktuellen Daten, die einem anderen Mitgliedstaat übermittelt oder bereitgestellt wurden und von Behörden mit justizähnlichem Charakter, d. h. von Behörden, die rechtsverbindliche Beschlüsse erlassen dürfen, weiterverarbeitet werden, sollte die Berichtigung, Löschung oder Sperrung dieser Daten nach nationalem Recht erfolgen.
- (16) Die Gewährleistung eines hohen Schutzes der personenbezogenen Daten von natürlichen Personen setzt gemeinsame Bestimmungen über die Rechtmäßigkeit und die Qualität der von den zuständigen Behörden in anderen Mitgliedstaaten verarbeiteten Daten voraus.
- (17) Es sollte auf europäischer Ebene festgelegt werden, unter welchen Bedingungen die zuständigen Behörden der Mitgliedstaaten personenbezogene Daten, die sie von anderen Mitgliedstaaten erhalten haben, öffentlichen und nicht-öffentlichen Stellen in den Mitgliedstaaten übermitteln und zur Verfügung stellen dürfen. In vielen Fällen ist es erforderlich, dass die Justiz, die Polizei oder die Zollbehörden personenbezogene Daten an nicht-öffentliche Stellen übermitteln, um eine Straftat zu verfolgen oder eine unmittelbare und schwerwiegende Gefährdung der öffentlichen Sicherheit oder eine schwerwiegende Beeinträchtigung der Rechte natürlicher Personen zu verhüten, z. B. indem sie Warnmeldungen zu gefälschten Wertpapieren an Banken und Kreditinstitute senden oder im Bereich der Kfz-Kriminalität personenbezogene Daten an Versicherungsunternehmen weiterleiten, um einen ungesetzlichen Handel mit gestohlenen Kraftfahrzeugen zu verhindern oder um bessere Bedingungen für die Rückholung gestohlener Fahrzeuge aus dem Ausland zu schaffen. Dies ist nicht gleichzusetzen mit der Übertragung polizeilicher oder justizieller Aufgaben an nicht-öffentliche Stellen.

- (18) Die Vorschriften dieses Rahmenbeschlusses bezüglich der Übermittlung personenbezogener Daten durch die Justiz, die Polizei oder die Zollbehörden an nicht-öffentliche Stellen sind auf die Freigabe von Daten für Private (wie Strafverteidiger und Opfer) im Zusammenhang mit Strafverfahren nicht anwendbar.
- (19) Die Weiterverarbeitung der von der zuständigen Behörde eines anderen Mitgliedstaats übermittelten oder zur Verfügung gestellten Daten, insbesondere die Weitergabe oder Bereitstellung dieser Daten, sollte durch gemeinsame Bestimmungen auf europäischer Ebene geregelt werden.
- (20) Dürfen personenbezogene Daten weiterverarbeitet werden, nachdem der Staat, der sie übermittelt hat, dem zugestimmt hat, so sollten die Mitgliedstaaten selbst die Modalitäten einer solchen Zustimmung festlegen können, z. B. in Form einer allgemeinen Zustimmung für Informations- oder Weiterverarbeitungs-kategorien.
- (21) Dürfen personenbezogene Daten für Verwaltungsverfahren weiterverarbeitet werden, so fallen unter diese Verfahren auch die Tätigkeiten von Regulierungs- oder Aufsichtsbehörden.
- (22) Die rechtmäßigen Tätigkeiten der Polizei-, Zoll- und Gerichtsbehörden und anderer zuständiger Behörden können es erfordern, dass Daten an Behörden in Drittländern oder an internationale Einrichtungen übermittelt werden, die zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen verpflichtet sind.
- (23) Personenbezogene Daten, die von einem Mitgliedstaat an Drittstaaten oder internationale Stellen übermittelt werden, sollten grundsätzlich angemessen geschützt werden.
- (24) Werden personenbezogene Daten von einem Mitgliedstaat an Drittstaaten oder internationale Stellen weitergeleitet, so sollte die Weiterleitung grundsätzlich erst dann erfolgen, wenn der Mitgliedstaat, von dem die Daten übermittelt wurden, der Weiterleitung zugestimmt hat. Jeder Mitgliedstaat sollte die Modalitäten für diese Zustimmung festlegen können, die beispielsweise im Wege einer allgemeinen Zustimmung für Kategorien von Informationen oder für bestimmte Drittstaaten erteilt werden kann.
- (25) Ist die Bedrohung der öffentlichen Sicherheit eines Mitgliedstaats oder eines Drittstaats so akut, dass die vorherige Zustimmung nicht rechtzeitig eingeholt werden kann, so ist es im Interesse einer effizienten Zusammenarbeit bei der Strafverfolgung geboten, dass die zuständige Behörde die relevanten personenbezogenen Daten ohne vorherige Zustimmung an den betreffenden Drittstaat übermitteln können sollte. Dies könnte auch gelten, wenn andere wesentliche Interessen eines Mitgliedstaats von gleicher Bedeutung auf dem Spiel stehen, beispielsweise wenn die kritische Infrastruktur eines Mitgliedstaats unmittelbar und ernsthaft bedroht oder das Finanzsystem eines Mitgliedstaats erheblich gestört werden könnte.
- (26) Die Information der betroffenen Personen über die Verarbeitung ihrer Daten kann insbesondere bei besonders schwerwiegenden Eingriffen in ihre Rechte durch Maßnahmen der heimlichen Datenerhebung geboten sein, um diesen Personen die Möglichkeit eines effektiven Rechtsschutzes zu gewährleisten.
- (27) Die Mitgliedstaaten sollten dafür sorgen, dass die betroffene Person darüber informiert wird, dass personenbezogene Daten zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen erhoben, verarbeitet oder an einen anderen Mitgliedstaat übermittelt werden oder werden könnten. Die Modalitäten des Rechts der betroffenen Person auf Unterrichtung und die Ausnahmen hierzu sollten nach einzelstaatlichem Recht festgelegt werden. Dies kann in allgemeiner Form, z. B. durch Rechtsvorschriften oder durch Veröffentlichung einer Liste der Verarbeitungen, erfolgen.
- (28) Um den Schutz personenbezogener Daten ohne Beeinträchtigung der Interessen strafrechtlicher Untersuchungen zu gewährleisten, ist es erforderlich, die Rechte der betroffenen Personen festzulegen.
- (29) Einige Mitgliedstaaten haben das Zugangsrecht der betroffenen Person in Strafsachen durch ein System vorgesehen, bei dem die nationale Aufsichtsbehörde anstelle der betroffenen Person uneingeschränkter Zugang zu allen diese Person betreffenden personenbezogenen Daten hat und zudem unrichtige Daten berichtigen, löschen oder aktualisieren darf. Im Fall eines solchen indirekten Zugangs kann im nationalen Recht dieser Mitgliedstaaten vorgesehen werden, dass die nationale Aufsichtsbehörde der betroffenen Person nur mitteilt, dass alle erforderlichen Überprüfungen durchgeführt wurden. Allerdings sehen diese Mitgliedstaaten in bestimmten Fällen auch direkte Zugangsmöglichkeiten für die betroffene Person vor, wie den Zugang zu Justizdokumenten, um einen eigenen Strafregisterauszug oder Kopien von Dokumenten in Zusammenhang mit eigenen polizeilichen Vernehmungen zu erhalten.
- (30) Es sollten gemeinsame Bestimmungen über die Vertraulichkeit und die Sicherheit der Verarbeitung, über die Haftung und über Sanktionen bei unrechtmäßiger Verwendung der Daten durch die zuständigen Behörden sowie die den Betroffenen zur Verfügung stehenden Rechtsbehelfe festgelegt werden. Es ist jedoch Sache jedes Mitgliedstaats, die Art seiner schadenersatzrechtlichen Vorschriften und der Sanktionen für Verstöße gegen innerstaatliche Datenschutzbestimmungen festzulegen.
- (31) Dieser Rahmenbeschluss erlaubt bei der Umsetzung der mit ihm festgelegten Grundsätze die Berücksichtigung des Grundsatzes des öffentlichen Zugangs zu amtlichen Dokumenten.

- (32) Sind personenbezogene Daten im Zusammenhang mit einer Verarbeitung zu schützen, bei der aufgrund des Umfangs oder der Art der Verarbeitung spezifische Risiken für die Grundrechte und -freiheiten bestehen, z. B. bei der Verarbeitung mit Hilfe neuer Technologien, Mechanismen oder Verfahren, so sollte sichergestellt werden, dass die zuständigen nationalen Aufsichtsbehörden vor der Festlegung der Dateien, mit dem diese Daten verarbeitet werden sollen, konsultiert werden.
- (33) Die Einrichtung völlig unabhängiger Kontrollstellen in den Mitgliedstaaten ist ein wesentliches Element des Schutzes personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit zwischen den Mitgliedstaaten in Strafsachen verarbeitet werden.
- (34) Die nach der Richtlinie 95/46/EG in den Mitgliedstaaten bereits errichteten Kontrollstellen sollten auch die Aufgaben der nach diesem Rahmenbeschluss zu errichtenden nationalen Kontrollstellen übernehmen können.
- (35) Diese Kontrollstellen sind mit den notwendigen Mitteln für die Erfüllung dieser Aufgabe auszustatten, d. h. mit Untersuchungs- und Einwirkungsbefugnissen, insbesondere bei Beschwerden einzelner Personen, bzw. mit einem Klagerecht. Die Kontrollstellen haben zur Transparenz der Verarbeitungen in den Mitgliedstaaten beizutragen, denen sie unterstehen. Ihre Befugnisse dürfen jedoch weder die speziellen Vorschriften für Strafverfahren noch die Unabhängigkeit der Gerichte berühren.
- (36) Artikel 47 des Vertrags über die Europäische Union besagt, dass dieser Vertrag die Verträge zur Gründung der Europäischen Gemeinschaften sowie die nachfolgenden Verträge und Akte zu ihrer Änderung oder Ergänzung unberührt lässt. Dementsprechend berührt dieser Rahmenbeschluss nicht den Schutz personenbezogener Daten im Rahmen des Gemeinschaftsrechts und insbesondere der Richtlinie 95/46/EG, der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr<sup>(1)</sup> und der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)<sup>(2)</sup>.
- (37) Dieser Rahmenbeschluss lässt die den rechtswidrigen Datenzugriff betreffenden Bestimmungen des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme<sup>(3)</sup> unberührt.
- (38) Dieser Rahmenbeschluss lässt bestehende Verpflichtungen und Zusagen der Mitgliedstaaten oder der Union aufgrund bestehender bilateraler und/oder multilateraler Übereinkünfte mit Drittstaaten unberührt. Bei künftigen Übereinkünften sollten die Regelungen über den Austausch mit Drittstaaten beachtet werden.
- (39) Verschiedene auf der Grundlage von Titel VI des Vertrags über die Europäische Union erlassene Rechtsakte enthalten spezifische Vorschriften über den Schutz personenbezogener Daten, die gemäß den Bestimmungen dieser Rechtsakte ausgetauscht oder anderweitig verarbeitet werden. Diese Vorschriften bilden in einigen Fällen ein vollständiges, in sich geschlossenes Regelwerk, das alle relevanten Datenschutzaspekte (Grundsätze der Datenqualität, Vorschriften über Datensicherheit, Regelung der Rechte und Garantien für die betroffenen Personen, Ausgestaltung der Überwachung und Haftung) erfasst, und regeln diese Fragen ausführlicher als dieser Rahmenbeschluss. Die einschlägigen Datenschutzvorschriften dieser Rechtsakte, insbesondere solche, die die Arbeitsweise von Europol, Eurojust, des Schengener Informationssystems (SIS) und des Zollinformationssystems (ZIS) regeln, sowie diejenigen, die den direkten Zugriff der Behörden der Mitgliedstaaten auf bestimmte Datensysteme anderer Mitgliedstaaten einführen, bleiben von dem vorliegenden Rahmenbeschluss unberührt. 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<sup>(4)</sup>, regeln.
- (40) In anderen Fällen sind die Datenschutzvorschriften in auf der Grundlage von Titel VI des Vertrags über die Europäische Union erlassenen Rechtsakten stärker begrenzt. Häufig legen sie für den Mitgliedstaat, der Informationen mit personenbezogenen Daten von einem anderen Mitgliedstaat empfängt, spezielle Bedingungen für die Verwendungszwecke dieser Daten fest, verweisen bei anderen Datenschutzaspekten jedoch auf das Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten oder aber auf innerstaatliches Recht. Soweit die Vorschriften jener Rechtsakte, die für Empfängermitgliedstaaten Auflagen hinsichtlich der Verwendung oder Weiterleitung von personenbezogenen Daten vorsehen, strenger sind als die entsprechenden Bestimmungen dieses Rahmenbeschlusses, sollten diese unberührt bleiben. Für alle anderen Aspekte sollten jedoch die in diesem Rahmenbeschluss festgelegten Regelungen gelten.
- (41) Dieser Rahmenbeschluss berührt nicht das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, das Zusatzprotokoll vom 8. November 2001 zu diesem Übereinkommen sowie die Übereinkommen des Europarates über die justizielle Zusammenarbeit in Strafsachen.

<sup>(1)</sup> ABl. L 8 vom 12.1.2001, S. 1.

<sup>(2)</sup> ABl. L 201 vom 31.7.2002, S. 37.

<sup>(3)</sup> ABl. L 69 vom 16.3.2005, S. 67.

<sup>(4)</sup> ABl. L 210 vom 6.8.2008, S. 1.

- (42) Da die Ziele dieses Rahmenbeschlusses, nämlich die Festlegung gemeinsamer Vorschriften über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, auf Ebene der Mitgliedstaaten nicht ausreichend verwirklicht werden können und daher wegen des Umfangs und der Wirkung der Maßnahme besser auf Ebene der Union zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags zur Gründung der Europäischen Gemeinschaft niedergelegten Subsidiaritätsprinzip, auf das in Artikel 2 des Vertrags über die Europäische Union Bezug genommen wird, tätig werden. Entsprechend dem in Artikel 5 des Vertrags zur Gründung der Europäischen Gemeinschaft genannten Grundsatz der Verhältnismäßigkeit geht dieser Rahmenbeschluss nicht über das zur Erreichung dieses Ziels erforderliche Maß hinaus.
- (43) Das Vereinigte Königreich beteiligt sich an diesem Rahmenbeschluss nach Artikel 5 des dem Vertrag über die Europäische Union und dem Vertrag zur Gründung der Europäischen Gemeinschaft beigefügten Protokolls zur Einbeziehung des Schengen-Besitzstands in den Rahmen der Europäischen Union und nach Artikel 8 Absatz 2 des Beschlusses 2000/365/EG des Rates vom 29. Mai 2000 zum Antrag des Vereinigten Königreichs Großbritannien und Nordirland, einzelne Bestimmungen des Schengen-Besitzstands auf sie anzuwenden <sup>(1)</sup>.
- (44) Irland beteiligt sich an diesem Rahmenbeschluss nach Artikel 5 des dem Vertrag über die Europäische Union und dem Vertrag zur Gründung der Europäischen Gemeinschaft beigefügten Protokolls zur Einbeziehung des Schengen-Besitzstands in den Rahmen der Europäischen Union und nach Artikel 6 Absatz 2 des Beschlusses 2002/192/EG des Rates vom 28. Februar 2002 zum Antrag Irlands auf Anwendung einzelner Bestimmungen des Schengen-Besitzstands auf Irland <sup>(2)</sup>.
- (45) Für Island und Norwegen stellt dieser Rahmenbeschluss eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union und der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands <sup>(3)</sup> dar, die zu dem Bereich nach Artikel 1 Buchstaben H und I des Beschlusses 1999/437/EG des Rates <sup>(4)</sup> zum Erlass bestimmter Durchführungsvorschriften zu dem Übereinkommen gehören.
- (46) Für die Schweiz stellt dieser Rahmenbeschluss eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung

der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands <sup>(5)</sup> dar, die in den in Artikel 1 Buchstaben H und I des Beschlusses 1999/437/EG in Verbindung mit Artikel 3 des Beschlusses 2008/149/JI des Rates <sup>(6)</sup> über die Unterzeichnung des Abkommens im Namen der Europäischen Union genannten Bereich fallen.

- (47) Für Lichtenstein stellt dieser Rahmenbeschluss eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein unterzeichneten Protokolls über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar, die in den in Artikel 1 Buchstaben H und I des Beschlusses 1999/437/EG in Verbindung mit Artikel 3 des Beschlusses 2008/262/JI des Rates <sup>(7)</sup> über die Unterzeichnung des Protokolls im Namen der Europäischen Union genannten Bereich fallen.
- (48) Dieser Rahmenbeschluss steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union <sup>(8)</sup> anerkannt wurden. Dieser Rahmenbeschluss stellt auf die vollständige Wahrung des Rechtes auf Schutz der Privatsphäre und des Rechtes auf Schutz personenbezogener Daten im Sinne der Artikel 7 und 8 der Charta ab —

HAT FOLGENDEN RAHMENBESCHLUSS ANGENOMMEN:

#### Artikel 1

##### Zweck und Anwendungsbereich

- (1) Zweck dieses Rahmenbeschlusses ist es, einen hohen Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihres Rechts auf Privatsphäre hinsichtlich der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen gemäß Titel VI des Vertrags über die Europäische Union sowie gleichzeitig ein hohes Maß an öffentlicher Sicherheit zu gewährleisten.
- (2) Gemäß diesem Rahmenbeschluss schützen die Mitgliedstaaten die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Privatsphäre, wenn personenbezogene Daten zum Zweck der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen
- a) zwischen Mitgliedstaaten übermittelt oder bereitgestellt werden oder wurden;

<sup>(1)</sup> ABl. L 131 vom 1.6.2000, S. 43.

<sup>(2)</sup> ABl. L 64 vom 7.3.2002, S. 20.

<sup>(3)</sup> ABl. L 176 vom 10.7.1999, S. 36.

<sup>(4)</sup> ABl. L 176 vom 10.7.1999, S. 31.

<sup>(5)</sup> ABl. L 53 vom 27.2.2008, S. 52.

<sup>(6)</sup> ABl. L 53 vom 27.2.2008, S. 50.

<sup>(7)</sup> ABl. L 83 vom 26.3.2008, S. 5.

<sup>(8)</sup> ABl. C 303 vom 14.12.2007, S. 1.

- b) von Mitgliedstaaten an Behörden oder an Informationssysteme, die aufgrund von Titel VI des Vertrags über die Europäische Union errichtet worden sind, übermittelt oder ihnen bereitgestellt werden oder wurden;
- c) von Behörden oder Informationssystemen, die aufgrund des Vertrags über die Europäische Union oder des Vertrags zur Gründung der Europäischen Gemeinschaft errichtet worden sind, an die zuständigen Behörden der Mitgliedstaaten übermittelt oder ihnen bereitgestellt werden oder wurden.

(3) Dieser Rahmenbeschluss gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

(4) Dieser Rahmenbeschluss lässt die wesentlichen nationalen Sicherheitsinteressen und spezifische nachrichtendienstliche Tätigkeiten, die die innere Sicherheit betreffen, unberührt.

(5) Dieser Rahmenbeschluss hindert die Mitgliedstaaten nicht daran, zum Schutz personenbezogener Daten, die auf nationaler Ebene erhoben oder verarbeitet werden, Bestimmungen zu erlassen, die strenger sind als die Bestimmungen dieses Rahmenbeschlusses.

#### Artikel 2

##### Begriffsbestimmungen

Im Sinne dieses Rahmenbeschlusses bezeichnet der Ausdruck

- a) „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;
- b) „Verarbeitung personenbezogener Daten“ und „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe 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;
- c) „Sperrung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
- d) „Datei mit personenbezogenen Daten“ und „Datei“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, gleichgültig, ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geografischen Gesichtspunkten aufgeteilt geführt wird;
- e) „Auftragsverarbeiter“ jede Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;
- f) „Empfänger“ jede Stelle, die Daten erhält;
- g) „Einwilligung der betroffenen Person“ jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass die sie betreffenden personenbezogenen Daten verarbeitet werden;
- h) „zuständige Behörden“ durch Rechtsakte, die der Rat gemäß Titel VI des Vertrags über die Europäische Union erlassen hat, errichtete Agenturen oder Einrichtungen sowie Polizei-, Zoll-, Justiz- oder sonstige zuständige Behörden der Mitgliedstaaten, die nach innerstaatlichem Recht ermächtigt sind, personenbezogene Daten im Anwendungsbereich dieses Rahmenbeschlusses zu verarbeiten;
- i) „für die Verarbeitung Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
- j) „Kennzeichnung“ die Markierung gespeicherter personenbezogener Daten, ohne dass damit das Ziel verfolgt wird, ihre künftige Verarbeitung einzuschränken;
- k) „Anonymisieren“ das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.

#### Artikel 3

##### Grundsatz der Rechtmäßigkeit, Verhältnismäßigkeit und der Zweckbindung

(1) Personenbezogene Daten dürfen von den zuständigen Behörden nur zu festgelegten, eindeutigen und rechtmäßigen Zwecken im Rahmen ihrer Aufgaben erhoben und nur zu dem Zweck verarbeitet werden, zu dem die Daten erhoben worden sind. Die Verarbeitung der Daten muss rechtmäßig sein und den Zwecken entsprechen, für die sie erhoben werden, dafür erheblich sein und darf nicht darüber hinausgehen.

(2) Die Weiterverarbeitung zu einem anderen Zweck ist zulässig, soweit

- a) diese Verarbeitung mit den Zwecken, zu denen die Daten erhoben worden sind, nicht unvereinbar ist;
- b) die zuständigen Behörden nach den für sie geltenden Rechtsvorschriften zur Verarbeitung solcher Daten zu einem anderen Zweck befugt sind und
- c) diese Verarbeitung zu diesem anderen Zweck notwendig und verhältnismäßig ist.

Darüber hinaus dürfen die übermittelten personenbezogenen Daten durch die zuständigen Behörden für historische, statistische oder wissenschaftliche Zwecke weiter verarbeitet werden, sofern die Mitgliedstaaten geeignete Garantien vorsehen, wie die Anonymisierung der Daten.

#### Artikel 4

##### **Berichtigung, Löschung und Sperrung**

- (1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind, und, sofern dies möglich und nötig ist, zu vollständigen oder auf den neuesten Stand zu bringen.
- (2) Personenbezogene Daten sind zu löschen oder zu anonymisieren, wenn sie für die Zwecke, für die sie rechtmäßig erhoben worden sind oder rechtmäßig weiter verarbeitet werden, nicht mehr erforderlich sind. Eine Archivierung dieser Daten in einem gesonderten Datenbestand über einen angemessenen Zeitraum nach Maßgabe des innerstaatlichen Rechts bleibt hiervon unberührt.
- (3) Besteht berechtigter Grund zu der Annahme, dass eine Löschung die schutzwürdigen Interessen der betroffenen Person beeinträchtigen würde, so werden die personenbezogenen Daten nicht gelöscht, sondern lediglich gesperrt. Gesperrte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand.
- (4) Sind die personenbezogenen Daten in einem Gerichtsbeschluss oder einem Gerichtsdokument enthalten, das mit dem Erlass eines Gerichtsbeschlusses in Verbindung steht, so erfolgt die Berichtigung, Löschung oder Sperrung im Einklang mit der nationalen Prozessordnung.

#### Artikel 5

##### **Festlegung von Löschungs- und Prüffristen**

Für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung sind angemessene Fristen vorzusehen. Durch verfahrensrechtliche Vorkehrungen ist sicherzustellen, dass diese Fristen eingehalten werden.

#### Artikel 6

##### **Verarbeitung besonderer Kategorien personenbezogener Daten**

Die Verarbeitung personenbezogener Daten, aus denen die rassistische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben ist nur zulässig, wenn dies unbedingt notwendig ist und das innerstaatliche Recht einen angemessenen Schutz gewährleistet.

#### Artikel 7

##### **Automatisierte Einzelentscheidungen**

Eine Entscheidung, die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt und die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, ist nur zulässig, wenn dies durch ein Gesetz vorgesehen ist, das Garantien zur Wahrung der schutzwürdigen Interessen der betroffenen Person festlegt.

#### Artikel 8

##### **Überprüfung der Qualität der übermittelten oder bereitgestellten Daten**

- (1) Die zuständigen Behörden ergreifen alle angemessenen Maßnahmen, um dafür zu sorgen, dass personenbezogene Da-

ten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Zu diesem Zweck überprüfen die zuständigen Behörden, soweit dies praktisch möglich ist, die Qualität der personenbezogenen Daten vor ihrer Übermittlung oder Bereitstellung. Bei jeder Übermittlung von Daten werden nach Möglichkeit Informationen beigefügt, die es dem Empfängermitgliedstaat gestatten, die Richtigkeit, Vollständigkeit, Aktualität und die Zuverlässigkeit der Daten zu beurteilen. Werden personenbezogene Daten ohne vorheriges Ersuchen übermittelt, so prüft die empfangende Behörde unverzüglich, ob die Daten für den Zweck, für den sie übermittelt wurden, benötigt werden.

- (2) Wird festgestellt, dass unrichtige Daten übermittelt worden sind oder Daten unrechtmäßig übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. Er ist verpflichtet, die Daten unverzüglich gemäß Artikel 4 zu berichtigen, zu löschen oder zu sperren.

#### Artikel 9

##### **Fristen**

- (1) Die übermittelnde Behörde kann bei der Übermittlung oder Bereitstellung der Daten im Einklang mit innerstaatlichem Recht und in Übereinstimmung mit den Artikeln 4 und 6 Fristen für die Aufbewahrung der Daten angeben, nach deren Ablauf auch der Empfänger die Daten zu löschen, zu sperren oder zu prüfen hat, ob sie noch benötigt werden. Diese Verpflichtung besteht nicht, wenn die Daten zum Zeitpunkt des Ablaufs dieser Fristen für eine laufende Ermittlung, Verfolgung von Straftaten oder Vollstreckung strafrechtlicher Sanktionen benötigt werden.

- (2) Hat die übermittelnde Stelle keine Frist nach Absatz 1 angegeben, so gelten für die Aufbewahrung der Daten im Einklang mit den Artikeln 4 und 5 die nach dem innerstaatlichen Recht des Empfängermitgliedstaats vorgesehenen Fristen.

#### Artikel 10

##### **Protokollierung und Dokumentierung**

- (1) Jede Übermittlung personenbezogener Daten ist zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung und der Sicherstellung der Integrität und Sicherheit der Daten zu protokollieren oder zu dokumentieren.

- (2) Die Protokolle oder Dokumentationen nach Absatz 1 werden der für den Datenschutz zuständigen Kontrollstelle auf Anforderung zur Datenschutzkontrolle übermittelt. Die zuständige Kontrollstelle verwendet diese Informationen nur zur Datenschutzkontrolle und zur Sicherstellung der ordnungsgemäßen Verarbeitung sowie der Integrität und Sicherheit der Daten.

#### Artikel 11

##### **Verarbeitung personenbezogener Daten die von einem anderen Mitgliedstaat übermittelt oder bereitgestellt wurden**

Personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übermittelt oder bereitgestellt wurden, dürfen unter den Voraussetzungen des Artikels 3 Absatz 2 nur für folgende andere Zwecke als diejenigen, für die sie übermittelt oder bereitgestellt wurden, weiter verarbeitet werden:

- a) die Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder Vollstreckung von strafrechtlichen Sanktionen, bei denen es sich nicht um die Straftaten oder Sanktionen handelt, für die sie übermittelt oder bereitgestellt wurden;
- b) andere justizielle und verwaltungsbehördliche Verfahren, die mit der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder Vollstreckung von strafrechtlichen Sanktionen unmittelbar zusammenhängen;
- c) die Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit; oder
- d) jeden anderen Zweck nur mit der vorherigen Zustimmung des übermittelnden Mitgliedstaats oder mit Einwilligung der betroffenen Person, die sie im Einklang mit dem innerstaatlichen Recht erteilt hat.

Darüber hinaus dürfen die übermittelten personenbezogenen Daten durch die zuständigen Behörden für historische, statistische oder wissenschaftliche Zwecke weiter verarbeitet werden, sofern die Mitgliedstaaten geeignete Garantien vorsehen, wie z. B. die Anonymisierung der Daten.

#### Artikel 12

##### **Wahrung von innerstaatlichen Verarbeitungsbeschränkungen**

(1) Gelten nach dem innerstaatlichen Recht des übermittelnden Mitgliedstaats unter besonderen Umständen besondere Verarbeitungsbeschränkungen für den Datenaustausch zwischen den zuständigen Behörden innerhalb dieses Mitgliedstaats, so weist die übermittelnde Behörde den Empfänger auf diese besonderen Beschränkungen hin. Der Empfänger stellt sicher, dass diese Verarbeitungsbeschränkungen eingehalten werden.

(2) Bei der Anwendung von Absatz 1 wenden die Mitgliedstaaten für Datenübermittlungen an andere Mitgliedstaaten oder an nach Titel VI des Vertrags über die Europäische Union errichtete Agenturen oder Einrichtungen nur solche Beschränkungen an, die auch für entsprechende innerstaatliche Datenübermittlungen gelten.

#### Artikel 13

##### **Weiterleitung an die zuständigen Behörden in Drittstaaten oder an internationale Einrichtungen**

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übermittelt oder bereitgestellt wurden, an Drittstaaten oder internationale Einrichtungen, nur dann weitergeleitet werden, wenn:

- a) dies zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen erforderlich ist;
- b) die empfangende Stelle in dem Drittstaat oder die empfangende internationale Einrichtung für die Verhütung, Ermitt-

lung, Feststellung oder Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen zuständig ist;

- c) der Mitgliedstaat, von dem er die Daten erhalten hat, der Weiterleitung unter Beachtung seines innerstaatlichen Rechts zugestimmt hat; und
- d) dieser Drittstaat oder diese internationale Einrichtung ein angemessenes Schutzniveau für die beabsichtigte Datenverarbeitung gewährleistet.

(2) Eine Weiterleitung ohne vorherige Zustimmung nach Absatz 1 Buchstabe c ist nur zulässig, wenn die Weiterleitung der Daten zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittstaats oder für die wesentlichen Interessen eines Mitgliedstaats unerlässlich ist und die vorherige Zustimmung nicht rechtzeitig eingeholt werden kann. Die für die Erteilung der Zustimmung zuständige Behörde wird unverzüglich unterrichtet.

(3) Abweichend von Absatz 1 Buchstabe d dürfen personenbezogene Daten weitergeleitet werden, wenn

- a) dies im innerstaatlichen Recht des Mitgliedstaats, der die Daten weiterleitet, vorgesehen ist
  - i) wegen überwiegender schutzwürdiger Interessen der betroffenen Person oder
  - ii) wegen überwiegender berechtigter Interessen, insbesondere wichtiger öffentlicher Interessen, oder

b) der Drittstaat oder die empfangende internationale Einrichtung Garantien bietet und diese vom betreffenden Mitgliedstaat in Übereinstimmung mit ihrem jeweiligen innerstaatlichen Recht für angemessen befunden werden.

(4) Die Angemessenheit des Schutzniveaus nach Absatz 1 Buchstabe d wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, der Herkunftsstaat und der Staat oder die internationale Einrichtung, für welche die Daten am Ende bestimmt sind, die in dem betreffenden Drittstaat oder der betreffenden internationalen Einrichtung geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standardsregeln und Sicherheitsmaßnahmen berücksichtigt.

#### Artikel 14

##### **Übermittlung von Daten an nicht-öffentliche Stellen in Mitgliedstaaten**

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übermittelt oder bereitgestellt wurden, an nicht-öffentliche Stellen nur dann weitergeleitet werden, wenn

- a) die zuständige Behörde des Mitgliedstaats, von dem er die Daten erhalten hat, der Weiterleitung unter Beachtung ihres innerstaatlichen Rechts zugestimmt hat;
- b) überwiegende schutzwürdige Interessen der betroffenen Person nicht entgegenstehen und
- c) die Weiterleitung im Einzelfall für die zuständige Behörde, die die Daten an eine nicht-öffentliche Stelle weiterleitet, unerlässlich ist:
  - i) für die Erfüllung einer ihr rechtmäßig zugewiesenen Aufgabe,
  - ii) zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung von strafrechtlichen Sanktionen,
  - iii) zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit oder
  - iv) zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner.

(2) Die zuständige Behörde, die die Daten an eine nicht-öffentliche Stelle weiterleitet, weist diese darauf hin, zu welchen Zwecken die Daten ausschließlich verwendet werden dürfen.

#### Artikel 15

##### Unterrichtung auf Antrag der zuständigen Behörde

Der Empfänger unterrichtet auf Ersuchen die zuständige Behörde, die die personenbezogenen Daten übermittelt oder bereitgestellt hat, über die Verarbeitung der Daten.

#### Artikel 16

##### Information der betroffenen Person

(1) Die Mitgliedstaaten stellen sicher, dass die betroffene Person im Einklang mit dem innerstaatlichen Recht über die Erhebung oder Verarbeitung personenbezogener Daten durch ihre zuständigen Behörden informiert wird.

(2) Wurden personenbezogene Daten zwischen Mitgliedstaaten übermittelt oder bereitgestellt, so kann jeder Mitgliedstaat nach Maßgabe seines innerstaatlichen Rechts gemäß Absatz 1 darum ersuchen, dass der andere Mitgliedstaat die betroffene Person nicht informiert. In diesem Fall informiert der letztgenannte Mitgliedstaat die betroffene Person nicht ohne die vorherige Zustimmung des anderen Mitgliedstaats.

#### Artikel 17

##### Recht auf Auskunft

(1) Jede betroffene Person hat das Recht, auf in angemessenen Abständen gestellten Antrag frei und ungehindert und ohne unzumutbare Verzögerung oder übermäßig hohe Kosten folgende Auskunft zu erhalten:

- a) zumindest die Bestätigung von dem für die Verarbeitung Verantwortlichen oder von der nationalen Kontrollstelle,

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; oder

- b) zumindest die Bestätigung von der nationalen Kontrollstelle, dass alle erforderlichen Überprüfungen durchgeführt wurden.

(2) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die das Recht auf Auskunft nach Absatz 1 Buchstabe a beschränken, sofern eine solche Beschränkung unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Person notwendig und verhältnismäßig ist, um

- a) behördliche oder gerichtliche Ermittlungen, Untersuchungen oder Verfahren nicht zu behindern;
- b) die Verhütung, Feststellung, Ermittlung oder Verfolgung von Straftaten nicht zu beeinträchtigen oder um strafrechtliche Sanktionen zu vollstrecken;
- c) die öffentliche Sicherheit zu schützen;
- d) die Sicherheit des Staates zu schützen;
- e) die betroffene Person und die Rechte und Freiheiten anderer zu schützen.

(3) Eine Verweigerung oder Einschränkung der Auskunft ist schriftlich mitzuteilen. Dabei sind die tatsächlichen oder rechtlichen Gründe, auf die die Entscheidung gestützt wird, mitzuteilen. Eine solche Mitteilung kann unterbleiben, sofern ein Grund nach Absatz 2 Buchstaben a bis e vorliegt. In allen diesen Fällen ist die betroffene Person darauf hinzuweisen, dass sie bei der zuständigen nationalen Kontrollstelle, bei einer Justizbehörde oder vor Gericht Beschwerde einlegen kann.

#### Artikel 18

##### Recht auf Berichtigung, Löschung oder Sperrung

(1) Die betroffene Person hat ein Recht darauf, dass der für die Verarbeitung Verantwortliche seinen Pflichten nach den Artikeln 4, 8 und 9 zur Berichtigung, Löschung oder Sperrung personenbezogener Daten, die sich aus diesem Rahmenbeschluss ergeben, nachkommt. Die Mitgliedstaaten legen fest, ob die betroffene Person dieses Recht direkt gegenüber dem für die Verarbeitung Verantwortlichen oder über die zuständige nationale Kontrollstelle geltend machen kann. Lehnt der für die Verarbeitung Verantwortliche die Berichtigung, Löschung oder Sperrung ab, so ist dies der betroffenen Person schriftlich mitzuteilen und sie auf die nach innerstaatlichem Recht vorgesehenen Möglichkeiten einer Beschwerde oder eines Rechtsbehelfs hinzuweisen. Bei der Prüfung der Beschwerde oder des Rechtsbehelfs wird die betroffene Person davon in Kenntnis gesetzt, ob der für die Verarbeitung Verantwortliche ordnungsgemäß gehandelt hat oder nicht. Die Mitgliedstaaten können auch vorsehen, dass der betroffenen Person durch die zuständige nationale Kontrollstelle mitgeteilt wird, dass eine Überprüfung stattgefunden hat.

(2) Wird die Richtigkeit eines personenbezogenen Datums von der betroffenen Person bestritten und kann nicht ermittelt werden, ob dieses richtig ist oder nicht, kann eine Kennzeichnung dieses Datums erfolgen.

#### Artikel 19

##### Recht auf Schadenersatz

(1) Jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen mit den innerstaatlichen Vorschriften zur Umsetzung dieses Rahmenbeschlusses nicht zu vereinbarenden Handlung ein Schaden entsteht, hat Anspruch auf Schadenersatz gegenüber dem für die Verarbeitung Verantwortlichen oder der sonst nach innerstaatlichem Recht zuständigen Stelle.

(2) Hat eine zuständige Behörde eines Mitgliedstaats personenbezogene Daten übermittelt, kann der Empfänger sich im Rahmen seiner Haftung nach Maßgabe des innerstaatlichen Rechts gegenüber dem Geschädigten zu seiner Entlastung nicht darauf berufen, dass die übermittelten Daten unrichtig gewesen sind. Leistet der Empfänger Schadenersatz wegen eines Schadens, der durch die Verwendung von unrichtig übermittelten Daten verursacht wurde, so erstattet die übermittelnde zuständige Behörde dem Empfänger den Betrag des geleisteten Schadensersatzes, wobei ein etwaiges Verschulden des Empfängers zu berücksichtigen ist.

#### Artikel 20

##### Rechtsbehelfe

Unbeschadet verwaltungsrechtlicher Beschwerdeverfahren, die vor Beschreiten des Rechtswegs eingeleitet werden können, hat die betroffene Person das Recht, im Falle der Verletzung der Rechte, die ihr nach innerstaatlichen Rechtsvorschriften garantiert sind, bei Gericht Rechtsbehelfe einzulegen.

#### Artikel 21

##### Vertraulichkeit der Verarbeitung

(1) Personen, die Zugang zu personenbezogenen Daten haben, die in den Anwendungsbereich dieses Rahmenbeschlusses fallen, dürfen diese nur als Angehörige oder auf Weisung der zuständigen Behörde verarbeiten, es sei denn, es bestehen dafür gesetzliche Verpflichtungen.

(2) Personen, die beauftragt werden, für eine zuständige Behörde eines Mitgliedstaats zu arbeiten, unterliegen sämtlichen Datenschutzbestimmungen, die für die jeweilige zuständige Behörde gelten.

#### Artikel 22

##### Sicherheit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass die zuständigen Behörden geeignete technische und organisatorische Maßnahmen ergreifen müssen, um die unbeabsichtigte oder unerlaubte Vernichtung, den unbeabsichtigten Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten

Zugang — insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übermittelt oder durch einen direkten automatischen Zugang zur Verfügung gestellt werden — und jede andere Form der unerlaubten Verarbeitung personenbezogener Daten zu verhindern; dabei sind insbesondere die von der Verarbeitung ausgehenden Risiken und die Art der zu schützenden Daten zu berücksichtigen. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(2) Jeder Mitgliedstaat trifft im Hinblick auf die automatisierte Datenverarbeitung Maßnahmen, die geeignet sind,

- a) Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle);
- b) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle);
- c) die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten zu verhindern (Speicherkontrolle);
- d) zu verhindern, dass automatisierte Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle);
- e) zu gewährleisten, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle);
- f) zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übermittlungskontrolle);
- g) zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle);
- h) zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);
- i) zu gewährleisten, dass eingesetzte Systeme im Störfalle wiederhergestellt werden können (Wiederherstellung) und
- j) zu gewährleisten, dass die Funktionen des Systems ablaufen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Daten nicht durch Fehlfunktionen des Systems verfälscht werden (Datenintegrität).

(3) Die Mitgliedstaaten sehen vor, dass zum Auftragsverarbeiter nur bestimmt werden darf, der Gewähr dafür bietet, dass er die erforderlichen technischen und organisatorischen Maßnahmen nach Absatz 1 trifft und Weisungen nach Artikel 21 beachtet. Die zuständige Behörde hat den Auftragsverarbeiter daraufhin zu überwachen.

(4) Personenbezogene Daten dürfen durch einen Auftragsverarbeiter nur auf der Grundlage eines Rechtsakts oder eines schriftlichen Vertrags verarbeitet werden.

#### Artikel 23

##### Vorabkonsultation

Die Mitgliedstaaten gewährleisten, dass die zuständigen nationalen Kontrollstellen vor der Verarbeitung personenbezogener Daten in neu zu errichtenden Dateien konsultiert werden, wenn

- a) besondere Kategorien von Daten nach Artikel 6 verarbeitet werden oder
- b) 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.

#### Artikel 24

##### Sanktionen

Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um die ordnungsgemäße Anwendung der Bestimmungen dieses Rahmenbeschlusses sicherzustellen, und legen insbesondere wirksame, angemessene und abschreckende Sanktionen fest, die bei Verstößen gegen die Vorschriften zur Umsetzung dieses Rahmenbeschlusses zu verhängen sind.

#### Artikel 25

##### Nationale Kontrollstellen

(1) Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, bei der Anwendung der von den Mitgliedstaaten zur Umsetzung dieses Rahmenbeschlusses erlassenen innerstaatlichen Vorschriften in ihrem Hoheitsgebiet zu beraten und die Anwendung dieser Vorschriften zu überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

(2) Jede Kontrollstelle verfügt insbesondere über:

- a) Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;
- b) wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Einrichtungen zu befragen;

chung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Einrichtungen zu befragen;

- c) das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die innerstaatlichen Vorschriften zur Umsetzung dieses Rahmenbeschlusses. Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.

(3) Jede Person kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten mit einer Eingabe an jede Kontrollstelle wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.

(4) Die Mitgliedstaaten sehen vor, dass die Mitglieder und Bediensteten der Kontrollstellen an die für die jeweilige zuständige Behörde geltenden Datenschutzbestimmungen gebunden sind und hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach ihrem Ausscheiden aus dem Dienst, unterliegen.

#### Artikel 26

##### Beziehung zu Übereinkünften mit Drittstaaten

Dieser Rahmenbeschluss berührt nicht die Verpflichtungen und Zusagen der Mitgliedstaaten oder der Union aufgrund bilateraler und/oder multilateraler Übereinkünfte mit Drittstaaten, die vor der Annahme dieses Rahmenbeschlusses abgeschlossen wurden.

Bei der Anwendung solcher Übereinkünfte erfolgt die Weiterleitung personenbezogener Daten, die von einem anderen Mitgliedstaat erhalten wurden, an einen Drittstaat unter Einhaltung von Artikel 13 Absatz 1 Buchstabe c oder gegebenenfalls Artikel 13 Absatz 2.

#### Artikel 27

##### Evaluierung

(1) Die Mitgliedstaaten berichten der Kommission bis zum 27. November 2013, welche innerstaatlichen Maßnahmen sie getroffen haben, um die umfassende Beachtung dieses Rahmenbeschlusses insbesondere im Hinblick auf die Regelungen sicherzustellen, die bereits bei der Erhebung der Daten zu beachten sind. Die Kommission prüft insbesondere die Auswirkungen der Bestimmungen über den Anwendungsbereich dieses Rahmenbeschlusses gemäß Artikel 1 Absatz 2.

(2) Die Kommission berichtet dem Europäischen Parlament und dem Rat binnen eines Jahres über die Ergebnisse der Evaluierung nach Absatz 1 und fügt dem Bericht gegebenenfalls geeignete Änderungsvorschläge für diesen Rahmenbeschluss bei.

*Artikel 28***Beziehung zu bereits früher angenommenen EU-Rechtsakten**

Enthalten Rechtsakte, die im Rahmen von Titel VI des Vertrags über die Europäische Union vor dem Inkrafttreten dieses Rahmenbeschlusses erlassen wurden und die den Austausch personenbezogener Daten zwischen Mitgliedstaaten oder den Zugang der von den Mitgliedstaaten bestimmten Behörden zu den gemäß dem Vertrag zur Gründung der Europäischen Gemeinschaft errichteten Informationssystemen regeln, spezifische Bestimmungen für die Verwendung dieser Daten durch den Empfängermitgliedstaat, so haben diese Bestimmungen Vorrang gegenüber den in diesem Rahmenbeschluss enthaltenen Bestimmungen über die Verwendung der von einem anderen Mitgliedstaat übermittelten oder zur Verfügung gestellten Daten.

*Artikel 29***Umsetzung**

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um den Vorschriften dieses Rahmenbeschlusses vor dem 27. November 2010 nachzukommen.

(2) Die Mitgliedstaaten übermitteln dem Generalsekretariat des Rates und der Kommission bis zu diesem Zeitpunkt den Wortlaut der Bestimmungen, mit denen sie die sich aus diesem Rahmenbeschluss ergebenden Verpflichtungen in ihr innerstaatliches Recht umgesetzt haben, sowie Angaben zu den in Artikel 25 genannten Kontrollstellen. Auf der Grundlage eines anhand dieser Angaben von der Kommission erstellten Berichts überprüft der Rat vor dem 27. November 2011, ob die Mitgliedstaaten den Bestimmungen dieses Rahmenbeschlusses nachgekommen sind.

*Artikel 30***Inkrafttreten**

Dieser Rahmenbeschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Geschehen zu Brüssel am 27. November 2008.

*Im Namen des Rates*

*Die Präsidentin*

M. ALLIOT-MARIE

---